

**paloalto**  
NETWORKS®

# PAN-OS Administrator's Guide

Version 7.0

## Contact Information

Corporate Headquarters:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-us](http://www.paloaltonetworks.com/company/contact-us)

## About this Guide

This guide takes you through the configuration and maintenance of your Palo Alto Networks next-generation firewall. For additional information, refer to the following resources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: <https://www.paloaltonetworks.com/documentation> or search the documentation.
- For access to the knowledge base and community forums, refer to <https://live.paloaltonetworks.com>.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to <https://www.paloaltonetworks.com/support/tabs/overview.html>.
- For the most current PAN-OS and Panorama 7.0 release notes, go to <https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os-release-notes.html>.

To provide feedback on the documentation, please write to us at: [documentation@paloaltonetworks.com](mailto:documentation@paloaltonetworks.com).

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2015–2016 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

Revision Date: July 22, 2016



# Table of Contents

---

---

<b>Getting Started . . . . .</b>	<b>15</b>
Integrate the Firewall into Your Management Network . . . . .	16
Determine Your Management Strategy . . . . .	17
Perform Initial Configuration . . . . .	18
Set Up Network Access for External Services . . . . .	22
Register the Firewall . . . . .	27
Activate Licenses and Subscriptions . . . . .	28
Manage Content Updates . . . . .	30
Install Software Updates . . . . .	33
Create the Security Perimeter . . . . .	34
Basic Interface Deployments . . . . .	35
About Security Policy . . . . .	37
Plan the Deployment . . . . .	40
Configure Interfaces and Zones . . . . .	41
Set Up Basic Security Policies . . . . .	43
Enable Basic Threat Prevention Features . . . . .	49
Enable WildFire . . . . .	50
Scan Traffic for Threats . . . . .	53
Control Access to Web Content . . . . .	58
Best Practices for Completing the Firewall Deployment . . . . .	61
<b>Device Management . . . . .</b>	<b>63</b>
Management Interfaces . . . . .	64
Use the Web Interface . . . . .	65
Use the Command Line Interface (CLI) . . . . .	72
Use the XML API . . . . .	74
Manage Firewall Administrators . . . . .	76
Administrative Roles . . . . .	77
Administrative Authentication . . . . .	79
Configure Administrative Accounts and Authentication . . . . .	80
Configure an Administrative Account . . . . .	81
Configure Kerberos SSO and External or Local Authentication for Administrators . . . . .	82
Configure Certificate-Based Administrator Authentication to the Web Interface . . . . .	84
Configure SSH Key-Based Administrator Authentication to the CLI . . . . .	85
Configure RADIUS Vendor-Specific Attributes for Administrator Authentication . . . . .	86
Reference: Web Interface Administrator Access . . . . .	88
Web Interface Access Privileges . . . . .	88
Panorama Web Interface Access . . . . .	129
Reference: Port Numbers Used by Palo Alto Networks Devices . . . . .	132
Ports Used for Management Functions . . . . .	132
Ports Used for HA . . . . .	133
Ports Used for Panorama . . . . .	134
Ports Used for GlobalProtect . . . . .	134
Ports Used for User-ID . . . . .	135
Reset the Firewall to Factory Default Settings . . . . .	137

<b>Authentication . . . . .</b>	<b>139</b>
Configure Kerberos Single Sign-On . . . . .	140
Configure External Authentication . . . . .	141
Configure Authentication Server Profiles . . . . .	142
Configure a RADIUS Server Profile . . . . .	143
RADIUS Vendor-Specific Attributes for Palo Alto Networks Devices . . . . .	144
Configure a TACACS+ Server Profile . . . . .	145
Configure an LDAP Server Profile . . . . .	146
Configure a Kerberos Server Profile . . . . .	147
Set CHAP and PAP Authentication for RADIUS and TACACS+ Servers . . . . .	148
Configure an Authentication Profile and Sequence . . . . .	149
Enable External Authentication for Users and Services . . . . .	152
Test Authentication Server Connectivity . . . . .	153
Run the Test Authentication Command . . . . .	154
Local Database Authentication Profile Use Case . . . . .	155
RADIUS Authentication Profile Use Case . . . . .	156
TACACS+ Authentication Profile Use Case . . . . .	158
LDAP Authentication Profile Use Case . . . . .	161
Kerberos Authentication Profile Use Case . . . . .	163
Troubleshoot Authentication Issues . . . . .	165
<b>Certificate Management . . . . .</b>	<b>167</b>
Keys and Certificates . . . . .	168
Certificate Revocation . . . . .	170
Certificate Revocation List (CRL) . . . . .	170
Online Certificate Status Protocol (OCSP) . . . . .	171
Certificate Deployment . . . . .	172
Set Up Verification for Certificate Revocation Status . . . . .	173
Configure an OCSP Responder . . . . .	173
Configure Revocation Status Verification of Certificates Used for User/Device Authentication . . . . .	174
Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption . . . . .	174
Configure the Master Key . . . . .	176
Obtain Certificates . . . . .	177
Create a Self-Signed Root CA Certificate . . . . .	178
Generate a Certificate on the Device . . . . .	179
Import a Certificate and Private Key . . . . .	181
Obtain a Certificate from an External CA . . . . .	182
Export a Certificate and Private Key . . . . .	184
Configure a Certificate Profile . . . . .	185
Configure an SSL/TLS Service Profile . . . . .	187
Configure the Key Size for SSL Forward Proxy Server Certificates . . . . .	188
Revoke and Renew Certificates . . . . .	189
Revoke a Certificate . . . . .	189
Renew a Certificate . . . . .	189

## Table of Contents

Secure Keys with a Hardware Security Module .....	190
Set up Connectivity with an HSM .....	191
Encrypt a Master Key Using an HSM .....	197
Store Private Keys on an HSM .....	199
Manage the HSM Deployment .....	200
<b>High Availability .....</b>	<b>201</b>
HA Overview .....	202
HA Concepts .....	203
HA Modes .....	203
HA Links and Backup Links .....	203
Device Priority and Preemption .....	206
Failover Triggers .....	206
HA Timers .....	207
Set Up Active/Passive HA .....	210
Prerequisites for Active/Passive HA .....	211
Configuration Guidelines for Active/Passive HA .....	212
Configure Active/Passive HA .....	214
Define HA Failover Conditions .....	220
Verify Failover .....	222
Reference: HA Synchronization .....	223
What Settings Don't Sync in Active/Passive HA? .....	223
What Settings Don't Sync in Active/Active HA? .....	225
Synchronization of System Runtime Information .....	227
HA Resources .....	229
<b>Monitoring .....</b>	<b>231</b>
Use the Dashboard .....	232
Use the Application Command Center .....	233
ACC—First Look .....	234
ACC Tabs .....	236
ACC Widgets .....	237
Widget Descriptions .....	239
ACC Filters .....	243
Interact with the ACC .....	245
Use Case: ACC—Path of Information Discovery .....	248
App Scope .....	254
Summary Report .....	255
Change Monitor Report .....	256
Threat Monitor Report .....	258
Threat Map Report .....	259
Network Monitor Report .....	260
Traffic Map Report .....	261
Use the Automated Correlation Engine .....	262
Automated Correlation Engine Concepts .....	263
View the Correlated Objects .....	264
Interpret Correlated Events .....	265
Use the Compromised Hosts Widget in the ACC .....	268

Take Packet Captures . . . . .	269
Disable Hardware Offload . . . . .	270
Take a Custom Packet Capture . . . . .	270
Take a Threat Packet Capture . . . . .	275
Take an Application Packet Capture . . . . .	276
Monitor Applications and Threats . . . . .	282
Monitor and Manage Logs . . . . .	283
View the Log Files . . . . .	284
Filter Log Data . . . . .	287
Configure Log Storage Quotas and Expiration Periods . . . . .	288
Log Severity Levels and WildFire Verdicts . . . . .	289
Schedule Log Exports to an SCP or FTP Server . . . . .	291
Manage Reporting . . . . .	292
Report Types . . . . .	293
View Reports . . . . .	294
Configure the Report Expiration Period . . . . .	295
Disable Predefined Reports . . . . .	296
Generate Custom Reports . . . . .	297
Generate Botnet Reports . . . . .	303
Manage PDF Summary Reports . . . . .	305
Generate User/Group Activity Reports . . . . .	307
Manage Report Groups . . . . .	309
Schedule Reports for Email Delivery . . . . .	310
Use External Services for Monitoring . . . . .	311
Configure Log Forwarding . . . . .	312
Configure Email Alerts . . . . .	315
Use Syslog for Monitoring . . . . .	316
Configure Syslog Monitoring . . . . .	317
Syslog Field Descriptions . . . . .	320
SNMP Monitoring and Traps . . . . .	337
SNMP for Palo Alto Networks Devices . . . . .	338
Use an SNMP Manager to Explore MIBs and Objects . . . . .	340
Enable SNMP Services for Firewall-Secured Network Elements . . . . .	344
Monitor Device Statistics Using SNMP . . . . .	345
Forward Traps to an SNMP Manager . . . . .	348
Supported MIBs . . . . .	350
NetFlow Monitoring . . . . .	358
Configure NetFlow Exports . . . . .	358
NetFlow Templates . . . . .	359
Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors . . . . .	363
<b>User-ID . . . . .</b>	<b>365</b>
User-ID Overview . . . . .	366
User-ID Concepts . . . . .	368
Group Mapping . . . . .	368
User Mapping . . . . .	369
Enable User-ID . . . . .	373

## Table of Contents

Map Users to Groups.....	374
Map IP Addresses to Users .....	377
Configure User Mapping Using the Windows User-ID Agent .....	378
Configure User Mapping Using the PAN-OS Integrated User-ID Agent.....	384
Configure User-ID to Receive User Mappings from a Syslog Sender.....	387
Map IP Addresses to Usernames Using Captive Portal .....	397
Configure User Mapping for Terminal Server Users .....	405
Send User Mappings to User-ID Using the XML API.....	413
Configure a Firewall to Share User Mapping Data with Other Firewalls .....	414
Enable User- and Group-Based Policy .....	416
Enable Policy for Users with Multiple Accounts .....	418
Verify the User-ID Configuration .....	420
Deploy User-ID in a Large-Scale Network.....	423
Windows Log Forwarding and Global Catalog Servers .....	423
Plan Your User-ID Implementation for a Large-Scale Network.....	424
Configure Windows Log Forwarding .....	425
Configure User-ID for a Large-Scale Network.....	425
<b>App-ID .....</b>	<b>429</b>
App-ID Overview .....	430
Manage Custom or Unknown Applications .....	431
Manage New App-IDs Introduced in Content Releases .....	433
Review New App-IDs .....	434
Review New App-IDs Since Last Content Version .....	435
Review New App-ID Impact on Existing Policy Rules .....	436
Disable or Enable App-IDs .....	437
Prepare Policy Updates For Pending App-IDs.....	438
Use Application Objects in Policy.....	440
Create an Application Group .....	440
Create an Application Filter .....	441
Create a Custom Application .....	442
Applications with Implicit Support .....	447
Application Level Gateways.....	450
Disable the SIP Application-level Gateway (ALG) .....	451
<b>Threat Prevention.....</b>	<b>453</b>
Set Up Security Profiles and Policies.....	454
Set Up Antivirus, Anti-Spyware, and Vulnerability Protection.....	455
Set Up Data Filtering .....	457
Set Up File Blocking.....	461
Prevent Brute Force Attacks .....	463
Customize the Action and Trigger Conditions for a Brute Force Signature .....	464
Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions .....	467
Enable Passive DNS Collection for Improved Threat Intelligence.....	470

Use DNS Queries to Identify Infected Hosts on the Network.....	471
DNS Sinkholing .....	472
Configure DNS Sinkholing .....	473
Identify Infected Hosts .....	477
Content Delivery Network Infrastructure for Dynamic Updates .....	479
Threat Prevention Resources .....	481
<b>Decryption.....</b>	<b>483</b>
Decryption Overview .....	484
Decryption Concepts.....	485
Keys and Certificates for Decryption Policies .....	486
SSL Forward Proxy .....	488
SSL Inbound Inspection .....	490
SSH Proxy.....	491
Decryption Exceptions .....	492
Decryption Mirroring.....	493
Configure SSL Forward Proxy .....	494
Configure SSL Inbound Inspection .....	499
Configure SSH Proxy.....	501
Configure Decryption Exceptions .....	502
Exclude Traffic from Decryption .....	502
Exclude a Server from Decryption .....	503
Enable Users to Opt Out of SSL Decryption .....	504
Configure Decryption Port Mirroring.....	506
Temporarily Disable SSL Decryption.....	508
<b>URL Filtering.....</b>	<b>509</b>
URL Filtering Overview .....	510
URL Filtering Vendors .....	511
Interaction Between App-ID and URL Categories .....	512
PAN-DB Private Cloud.....	513
URL Filtering Concepts.....	515
URL Categories .....	516
URL Filtering Profile .....	517
URL Filtering Profile Actions .....	518
Block and Allow Lists .....	519
Safe Search Enforcement.....	520
Container Pages .....	522
HTTP Header Logging .....	523
URL Filtering Response Pages .....	524
URL Category as Policy Match Criteria .....	526
PAN-DB Categorization .....	527
PAN-DB URL Categorization Components .....	527
PAN-DB URL Categorization Workflow.....	529

## Table of Contents

Enable a URL Filtering Vendor .....	530
Enable PAN-DB URL Filtering .....	531
Enable BrightCloud URL Filtering .....	532
Determine URL Filtering Policy Requirements .....	534
Monitor Web Activity .....	536
Monitor Web Activity of Network Users .....	537
View the User Activity Report .....	540
Configure Custom URL Filtering Reports .....	542
Configure URL Filtering .....	543
Customize the URL Filtering Response Pages .....	545
Configure URL Admin Override .....	546
Enable Safe Search Enforcement .....	548
Block Search Results that are not Using Strict Safe Search Settings .....	548
Enable Transparent Safe Search Enforcement .....	552
Set Up the PAN-DB Private Cloud .....	555
Set Up a PAN-DB Private Cloud .....	556
Configure the Firewalls to Access the PAN-DB Private Cloud .....	560
URL Filtering Use Case Examples .....	561
Use Case: Control Web Access .....	562
Use Case: Use URL Categories for Policy Matching .....	566
Troubleshoot URL Filtering .....	568
Problems Activating PAN-DB .....	568
PAN-DB Cloud Connectivity Issues .....	569
URLs Classified as Not-Resolved .....	570
Incorrect Categorization .....	571
URL Database Out of Date .....	572
<b>Quality of Service .....</b>	<b>573</b>
QoS Overview .....	574
QoS Concepts .....	576
QoS for Applications and Users .....	576
QoS Profile .....	577
QoS Classes .....	578
QoS Policy .....	579
QoS Egress Interface .....	580
QoS Clear Text and Tunneled Traffic .....	581
Configure QoS .....	582
Configure QoS for a Virtual System .....	587
Enforce QoS Based on DSCP Classification .....	594
QoS Use Cases .....	597
Use Case: QoS for a Single User .....	598
Use Case: QoS for Voice and Video Applications .....	601

<b>VPNs . . . . .</b>	<b>605</b>
VPN Deployments . . . . .	606
Site-to-Site VPN Overview . . . . .	607
Site-to-Site VPN Concepts . . . . .	608
IKE Gateway . . . . .	608
Tunnel Interface . . . . .	608
Tunnel Monitoring . . . . .	609
Internet Key Exchange (IKE) for VPN . . . . .	609
IKEv2 . . . . .	612
Set Up Site-to-Site VPN . . . . .	616
Set Up an IKE Gateway . . . . .	617
Define Cryptographic Profiles . . . . .	624
Set Up an IPSec Tunnel . . . . .	627
Set Up Tunnel Monitoring . . . . .	631
Enable/Disable, Refresh or Restart an IKE Gateway or IPSec Tunnel . . . . .	632
Test VPN Connectivity . . . . .	634
Interpret VPN Error Messages . . . . .	635
Site-to-Site VPN Quick Configs . . . . .	636
Site-to-Site VPN with Static Routing . . . . .	637
Site-to-Site VPN with OSPF . . . . .	642
Site-to-Site VPN with Static and Dynamic Routing . . . . .	648
 <b>Large Scale VPN (LSVPN) . . . . .</b>	 <b>655</b>
LSVPN Overview . . . . .	656
Create Interfaces and Zones for the LVPN . . . . .	657
Enable SSL Between GlobalProtect LVPN Components . . . . .	659
About Certificate Deployment . . . . .	659
Deploy Server Certificates to the GlobalProtect LVPN Components . . . . .	659
Configure the Portal to Authenticate Satellites . . . . .	663
Configure GlobalProtect Gateways for LVPN . . . . .	665
Prerequisite Tasks . . . . .	665
Configure the Gateway . . . . .	665
Configure the GlobalProtect Portal for LVPN . . . . .	668
Prerequisite Tasks . . . . .	668
Configure the Portal . . . . .	668
Define the Satellite Configurations . . . . .	669
Prepare the Satellite Device to Join the LVPN . . . . .	672
Verify the LVPN Configuration . . . . .	675
LVPN Quick Configs . . . . .	676
Basic LVPN Configuration with Static Routing . . . . .	677
Advanced LVPN Configuration with Dynamic Routing . . . . .	681

## Table of Contents

<b>Networking . . . . .</b>	<b>685</b>
Interface Deployments . . . . .	686
Virtual Wire Deployments . . . . .	686
Layer 2 Deployments . . . . .	689
Layer 3 Deployments . . . . .	689
Tap Mode Deployments . . . . .	690
Virtual Routers . . . . .	691
Static Routes . . . . .	693
RIP . . . . .	695
OSPF . . . . .	697
OSPF Concepts . . . . .	697
Configure OSPF . . . . .	700
Configure OSPFv3 . . . . .	705
Configure OSPF Graceful Restart . . . . .	708
Confirm OSPF Operation . . . . .	709
BGP . . . . .	712
Session Settings and Timeouts . . . . .	717
Transport Layer Sessions . . . . .	718
TCP . . . . .	719
UDP . . . . .	723
ICMP . . . . .	724
Configure Session Timeouts . . . . .	725
Configure Session Settings . . . . .	727
Prevent TCP Split Handshake Session Establishment . . . . .	729
DHCP . . . . .	730
DHCP Overview . . . . .	731
DHCP Messages . . . . .	732
DHCP Addressing . . . . .	733
DHCP Options . . . . .	735
Firewall as a DHCP Server and Client . . . . .	738
Configure an Interface as a DHCP Server . . . . .	739
Configure an Interface as a DHCP Client . . . . .	744
Configure an Interface as a DHCP Relay Agent . . . . .	746
Monitor and Troubleshoot DHCP . . . . .	747
NAT . . . . .	749
NAT Policy Rules . . . . .	750
Source NAT and Destination NAT . . . . .	753
NAT Rule Capacities . . . . .	755
Dynamic IP and Port NAT Oversubscription . . . . .	756
Dataplane NAT Memory Statistics . . . . .	758
Configure NAT . . . . .	759
NAT Configuration Examples . . . . .	769
NPTv6 . . . . .	777
NPTv6 Overview . . . . .	778
How NPTv6 Works . . . . .	780
NDP Proxy . . . . .	782
NPTv6 and NDP Proxy Example . . . . .	784
Create an NPTv6 Policy . . . . .	786

LACP .....	788
LACP Settings .....	788
Configure LACP.....	791
ECMP.....	794
ECMP Load-Balancing Algorithms.....	795
ECMP Platform, Interface, and IP Routing Support.....	797
HA Active/Active Failover Behavior with ECMP.....	798
Configure ECMP on a Virtual Router.....	799
Enable ECMP for Multiple BGP Autonomous Systems.....	801
Verify ECMP .....	803
LLDP .....	804
LLDP Overview.....	805
Supported TLVs in LLDP.....	806
LLDP Syslog Messages and SNMP Traps .....	808
Configure LLDP .....	809
View LLDP Settings and Status.....	811
Clear LLDP Statistics.....	814
<b>Policy.....</b>	<b>815</b>
Policy Types .....	816
Security Policy .....	817
Components of a Security Policy Rule .....	818
Security Policy Best Practices .....	821
Policy Objects .....	822
Security Profiles .....	823
Antivirus Profiles .....	824
Anti-Spyware Profiles.....	825
Vulnerability Protection Profiles .....	826
URL Filtering Profiles .....	827
Data Filtering Profiles .....	828
File Blocking Profiles .....	830
WildFire Analysis Profiles .....	831
DoS Protection Profiles .....	832
Zone Protection Profiles .....	833
Security Profile Group .....	834
Enumeration of Rules Within a Rulebase.....	838
Move or Clone a Policy Rule or Object to a Different Virtual System.....	840
Use Tags to Group and Visually Distinguish Objects .....	841
Create and Apply Tags .....	842
Modify Tags .....	843
Use the Tag Browser .....	844
Use a Dynamic Block List in Policy .....	848
View the IP Address Limit For Your Firewall Model .....	848
Formatting Guidelines for Dynamic Block Lists .....	849
Enforce Policy with a Dynamic Block List.....	849
View the List of IP addresses in the Dynamic Block List .....	850
Retrieve a Dynamic Block List from Web Server.....	851

## Table of Contents

Register IP Addresses and Tags Dynamically .....	852
Monitor Changes in the Virtual Environment .....	853
Enable VM Monitoring to Track Changes on the Virtual Network .....	854
Attributes Monitored in the AWS and VMware Environments.....	857
Use Dynamic Address Groups in Policy .....	858
CLI Commands for Dynamic IP Addresses and Tags .....	861
Identify Users Connected through a Proxy Server .....	863
Use XFF Values for Policies and Logging Source Users .....	863
Add XFF Values to URL Filtering Logs .....	864
Policy-Based Forwarding .....	865
PBF .....	866
Create a Policy-Based Forwarding Rule.....	868
Use Case: PBF for Outbound Access with Dual ISPs .....	870
DoS Protection Against Flooding of New Sessions .....	878
DoS Protection Against Flooding of New Sessions .....	879
Configure DoS Protection Against Flooding of New Sessions .....	883
Use the CLI to End a Single Attacking Session .....	886
Identify Sessions That Use an Excessive Percentage of the Packet Buffer.....	887
Discard a Session Without a Commit .....	889
<b>Virtual Systems .....</b>	<b>891</b>
Virtual Systems Overview .....	892
Virtual System Components and Segmentation .....	892
Benefits of Virtual Systems.....	893
Use Cases for Virtual Systems .....	893
Platform Support and Licensing for Virtual Systems .....	894
Administrative Roles for Virtual Systems .....	894
Shared Objects for Virtual Systems .....	894
Communication Between Virtual Systems .....	895
Inter-VSYS Traffic That Must Leave the Firewall .....	896
Inter-VSYS Traffic That Remains Within the Firewall.....	897
Inter-VSYS Communication Uses Two Sessions .....	900
Shared Gateway .....	901
External Zones and Shared Gateway.....	901
Networking Considerations for a Shared Gateway.....	902
Service Routes for Virtual Systems .....	903
Use Cases for Service Routes for a Virtual System .....	904
PA-7000 Series Firewall LPC Support for Per-Virtual System Paths to Logging Servers.....	905
DNS Proxy Object .....	906
DNS Server Profile.....	907
Multi-Tenant DNS Deployments.....	908
Configure Virtual Systems .....	909
Configure Inter-Virtual System Communication within the Firewall .....	912
Configure a Shared Gateway .....	913

Customize Service Routes for a Virtual System . . . . .	914
Customize Service Routes to Services for Virtual Systems . . . . .	914
Configure a PA-7000 Series Firewall for Logging Per Virtual System . . . . .	916
Configure a DNS Proxy Object. . . . .	917
Configure a DNS Server Profile . . . . .	918
Configure Administrative Access Per Virtual System or Device . . . . .	920
DNS Resolution—Three Use Cases . . . . .	922
Use Case 1: Firewall Requires DNS Resolution for Management Purposes. . . . .	922
Use Case 2: ISP Tenant Uses DNS Proxy to Handle DNS Resolution for Security Policies, Reporting, and Services within its Virtual System	925
Use Case 3: Firewall Acts as DNS Proxy Between Client and Server . . . . .	929
Virtual System Functionality with Other Features . . . . .	931
<b>Certifications . . . . .</b>	<b>933</b>
Enable FIPS and Common Criteria Support . . . . .	934
CCEAL4 Security Functions . . . . .	935



# Getting Started

---

---

The following topics provide detailed steps to help you deploy a new Palo Alto Networks next-generation firewall. They provide details for integrating a new firewall into your network and configuring basic security policies and threat prevention features.

After you perform the basic configuration steps required to integrate the firewall into your network, you can use the rest of the topics in this guide to help you deploy the comprehensive enterprise security platform features as necessary to address your network security needs.

- ▲ [Integrate the Firewall into Your Management Network](#)
- ▲ [Create the Security Perimeter](#)
- ▲ [Enable Basic Threat Prevention Features](#)
- ▲ [Best Practices for Completing the Firewall Deployment](#)

# Integrate the Firewall into Your Management Network

All Palo Alto Networks firewalls provide an out-of-band management port (MGT) that you can use to perform the firewall administration functions. By using the MGT port, you separate the management functions of the firewall from the data processing functions, safeguarding access to the firewall and enhancing performance. When using the web interface, you must perform all initial configuration tasks from the MGT port even if you plan to use an in-band port for managing your device going forward.

Some management tasks, such as retrieving licenses and updating the threat and application signatures on the firewall require access to the Internet. If you do not want to enable external access to your MGT port, you will need to either set up a data port to provide access to required external services or plan to manually upload updates regularly.

The following topics describe how to perform the initial configuration steps that are necessary to integrate a new firewall into the management network and deploy it in a basic security configuration.

- ▲ [Determine Your Management Strategy](#)
- ▲ [Perform Initial Configuration](#)
- ▲ [Set Up Network Access for External Services](#)
- ▲ [Register the Firewall](#)
- ▲ [Activate Licenses and Subscriptions](#)
- ▲ [Manage Content Updates](#)
- ▲ [Install Software Updates](#)



The following topics describe how to integrate a single Palo Alto Networks next-generation firewall into your network. However, for redundancy, consider deploying a pair of firewalls in a [High Availability](#) configuration.

## Determine Your Management Strategy

The Palo Alto Networks firewall can be configured and managed locally or it can be managed centrally using [Panorama](#), the Palo Alto Networks centralized security management system. If you have six or more firewalls deployed in your network, use Panorama to achieve the following benefits:

- Reduce the complexity and administrative overhead in managing configuration, policies, software and dynamic content updates. Using device groups and templates on Panorama, you can effectively manage device specific configuration locally on a device and enforce shared policies across all devices or device groups.
- Aggregate data from all managed firewalls and gain visibility across all the traffic on your network. The Application Command Center (ACC) on Panorama provides a single glass pane for unified reporting across all the firewalls, allowing you to centrally analyze, investigate and report on network traffic, security incidents and administrative modifications.

The procedures that follow describe how to manage the firewall using the local web interface. If you want to use Panorama for centralized management, first [Perform Initial Configuration](#) and verify that the firewall can establish a connection to Panorama. From that point on you can use [Panorama](#) to configure your firewall centrally.

## Perform Initial Configuration

By default, the firewall has an IP address of 192.168.1.1 and a username/password of admin/admin. For security reasons, you must change these settings before continuing with other firewall configuration tasks. You must perform these initial configuration tasks either from the MGT interface, even if you do not plan to use this interface for your firewall management, or using a direct serial connection to the console port on the device.

Set Up Network Access to the Firewall	
<b>Step 1</b>	Gather the required information from your network administrator. <ul style="list-style-type: none"><li>• IP address for MGT port</li><li>• Netmask</li><li>• Default gateway</li><li>• DNS server address</li></ul>
<b>Step 2</b>	Connect your computer to the firewall. <p>You can connect to the firewall in one of the following ways:</p> <ul style="list-style-type: none"><li>• Connect a serial cable from your computer to the Console port and connect to the firewall using terminal emulation software (9600-8-N-1). Wait a few minutes for the boot-up sequence to complete; when the device is ready, the prompt changes to the name of the firewall, for example PA-500 login.</li><li>• Connect an RJ-45 Ethernet cable from your computer to the MGT port on the firewall. From a browser, go to <a href="https://192.168.1.1">https://192.168.1.1</a>. Note that you may need to change the IP address on your computer to an address in the 192.168.1.0 network, such as 192.168.1.2, in order to access this URL.</li></ul>
<b>Step 3</b>	When prompted, log in to the firewall. <p>You must log in using the default username and password (admin/admin). The firewall will begin to initialize.</p>
<b>Step 4</b>	Configure the MGT interface. <ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Management</b> and then edit the Management Interface Settings.</li><li>2. Enter the <b>IP Address</b>, <b>Netmask</b>, and <b>Default Gateway</b>.<p> To prevent unauthorized access to the management interface, it is a best practice to <b>Add the Permitted IP Addresses</b> from which an administrator can access the MGT interface.</p></li><li>3. Set the <b>Speed</b> to <b>auto-negotiate</b>.</li><li>4. Select which management services to allow on the interface.<p> Make sure <b>Telnet</b> and <b>HTTP</b> are not selected because these services use plaintext and are not as secure as the other services and could compromise administrator credentials.</p></li><li>5. Click <b>OK</b>.</li></ol>

**Set Up Network Access to the Firewall (Continued)**

<p><b>Step 5</b> Configure general firewall settings as needed.</p> <p> As a best practice, add a login banner that indicates that access to the firewall is restricted to prevent unauthorized users from accessing the management functions. It is a good idea to avoid using welcoming verbiage and to run your messaging by your legal department to ensure that you are providing adequate warning that unauthorized access is prohibited.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Management</b> and edit the General Settings.</li><li>2. Enter a <b>Hostname</b> for the firewall and enter your network <b>Domain</b> name. The domain name is just a label; it will not be used to join the domain.</li><li>3. Enter <b>Login Banner</b> text that informs users who are attempting to log in that they must have authorization to access the firewall management functions.</li><li>4. Enter the <b>Latitude</b> and <b>Longitude</b> to enable accurate placement of the firewall on the world map.</li><li>5. Click <b>OK</b>.</li></ol>
<p><b>Step 6</b> Configure DNS, update server, and proxy server settings.</p> <p> You must manually configure at least one DNS server on the firewall or it will not be able to resolve hostnames; it will not use DNS server settings from another source, such as an ISP.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Services</b>.<ul style="list-style-type: none"><li>• For multi-virtual system platforms, select <b>Global</b> and edit the Services section.</li><li>• For single virtual system platforms, edit the Services section.</li></ul></li><li>2. On the <b>Services</b> tab, for <b>DNS</b>, click one of the following:<ul style="list-style-type: none"><li>• <b>Servers</b>—Enter the <b>Primary DNS Server</b> address and <b>Secondary DNS Server</b> address.</li><li>• <b>DNS Proxy Object</b>—From the drop-down, select the <b>DNS Proxy</b> that you want to use to configure global DNS services, or click <b>DNS Proxy</b> to configure a new <b>DNS proxy object</b>.</li></ul></li><li>3. (Optional) For <b>Update Server</b>, enter the IP address or host name of the server from which to download updates from Palo Alto Networks. The current value is <code>updates.paloaltonetworks.com</code>. Do not change the Update Server unless instructed by Technical Support.</li><li>4. (Optional) Click <b>Verify Update Server Identity</b> for an extra level of validation. The firewall will check the update server's SSL certificate to ensure that it was signed by a trusted authority.</li><li>5. (Optional) If the firewall needs to use a proxy server to reach Palo Alto Networks update services, in the <b>Proxy Server</b> window, enter:<ul style="list-style-type: none"><li>• <b>Server</b>—IP address or host name of the proxy server.</li><li>• <b>Port</b>—Port for the proxy server. Range: 1-65535.</li><li>• <b>User</b>—Username to access the server.</li><li>• <b>Password</b>—Password for the user to access the proxy server. Re-enter the password at <b>Confirm Password</b>.</li></ul></li><li>6. Click <b>OK</b>.</li></ol>

## Set Up Network Access to the Firewall (Continued)

<p><b>Step 7</b> Configure date and time (NTP) settings.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Services</b>.           <ul style="list-style-type: none"> <li>• For multi-virtual system platforms, select <b>Global</b> and edit the Services section.</li> <li>• For single virtual system platforms, edit the Services section.</li> </ul> </li> <li>2. On the <b>NTP</b> tab, to use the virtual cluster of time servers on the Internet, enter the hostname <b>pool.ntp.org</b> as the <b>Primary NTP Server</b> or enter the IP address of your primary NTP server.</li> <li>3. (Optional) Enter a <b>Secondary NTP Server</b> address.</li> <li>4. (Optional) To authenticate time updates from the NTP server(s), for <b>Authentication Type</b>, select one of the following for each server:           <ul style="list-style-type: none"> <li>• <b>None</b>—(Default) Disables NTP authentication.</li> <li>• <b>Symmetric Key</b>—Firewall uses symmetric key exchange (shared secrets) to authenticate time updates.               <ul style="list-style-type: none"> <li>– <b>Key ID</b>—Enter the Key ID (1-65534).</li> <li>– <b>Algorithm</b>—Select the algorithm to use in NTP authentication (<b>MD5</b> or <b>SHA1</b>).</li> </ul> </li> <li>• <b>Autokey</b>—Firewall uses autokey (public key cryptography) to authenticate time updates.</li> </ul> </li> <li>5. Click <b>OK</b>.</li> </ol>
<p><b>Step 8</b> Set a secure password for the admin account.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Administrators</b>.</li> <li>2. Select the <b>admin</b> role.</li> <li>3. Enter the current default password and the new password.</li> <li>4. Click <b>OK</b> to save your settings.</li> </ol>
<p><b>Step 9</b> Commit your changes.</p> <p> When the configuration changes are saved, you will lose connectivity to the web interface because the IP address will have changed.</p>	<p>Click <b>Commit</b>. The device may take up to 90 seconds to save your changes.</p> 
<p><b>Step 10</b> Connect the firewall to your network.</p>	<ol style="list-style-type: none"> <li>1. Disconnect the firewall from your computer.</li> <li>2. Connect the MGT port to a switch port on your management network using an RJ-45 Ethernet cable. Make sure that the switch port you cable the firewall to is configured for auto-negotiation.</li> </ol>
<p><b>Step 11</b> Open an SSH management session to the firewall.</p>	<p>Using a terminal emulation software, such as PuTTY, launch an SSH session to the firewall using the new IP address you assigned to it.</p>

### Set Up Network Access to the Firewall (Continued)

**Step 12** Verify network access to external services required for firewall management, such as the Palo Alto Networks Update Server.

You can do this in one of the following ways:

- If you do not want to allow external network access to the MGT interface, you will need to set up a data port to retrieve required service updates. Continue to [Set Up Network Access for External Services](#).
- If you do plan to allow external network access to the MGT interface, verify that you have connectivity and then proceed to [Register the Firewall](#) and [Activate Licenses and Subscriptions](#).

1. Use the ping utility to verify network connectivity to the Palo Alto Networks Update server as shown in the following example. Verify that DNS resolution occurs and the response includes the IP address for the Update server; the update server does not respond to a ping request.

```
admin@PA-200 > ping host
updates.paloaltonetworks.com
PING updates.paloaltonetworks.com (10.101.16.13)
56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host
Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host
Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host
Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host
Unreachable
```

 After verifying DNS resolution, press Ctrl+C to stop the ping request.

2. Use the following CLI command to retrieve information on the support entitlement for the firewall from the Palo Alto Networks update server:

```
request support check
```

If you have connectivity, the update server will respond with the support status for your firewall. Because your firewall is not registered, the update server will return the following message:

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```

## Set Up Network Access for External Services

By default, the firewall uses the MGT interface to access remote services, such as DNS servers, content updates, and license retrieval. If you do not want to enable external network access to your management network, you must set up a data port to provide access to these required external services.



This task requires familiarity with firewall interfaces, zones, and policies. For more information on these topics, see [Create the Security Perimeter](#).

For information on setting up network access to external services on a virtual system basis rather than a global basis, see [Per-Virtual System Service Routes](#).

### Set Up a Data Port for Access to External Services

Step 1	Decide which port you want to use for access to external services and connect it to your switch or router port.	The interface you use must have a static IP address.
Step 2	Log in to the web interface.	Using a secure connection ( <a href="https://&lt;IP address&gt;">https://&lt;IP address&gt;</a> ) from your web browser, log in using the new IP address and password you assigned during initial configuration ( <a href="https://&lt;IP address&gt;">https://&lt;IP address&gt;</a> ). You will see a certificate warning; that is okay. Continue to the web page.
Step 3	(Optional) The firewall comes preconfigured with a default virtual wire interface between ports Ethernet 1/1 and Ethernet 1/2 (and a corresponding default security policy and zones). If you do not plan to use this virtual wire configuration, you must manually delete the configuration to prevent it from interfering with other interface settings you define.	You must delete the configuration in the following order: <ol style="list-style-type: none"><li>To delete the default security policy, select <b>Policies &gt; Security</b>, select the rule, and click <b>Delete</b>.</li><li>Next, delete the default virtual wire by selecting <b>Network &gt; Virtual Wires</b>, selecting the virtual wire and clicking <b>Delete</b>.</li><li>To delete the default trust and untrust zones, select <b>Network &gt; Zones</b>, select each zone and click <b>Delete</b>.</li><li>Finally, delete the interface configurations by selecting <b>Network &gt; Interfaces</b> and then select each interface (ethernet1/1 and ethernet1/2) and click <b>Delete</b>.</li><li><b>Commit</b> the changes.</li></ol>

**Set Up a Data Port for Access to External Services (Continued)**

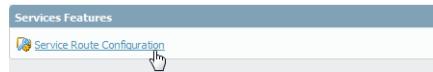
**Step 4** Configure the interface.

1. Select **Network > Interfaces** and select the interface that corresponds to the port you cabled in Step 1.
2. Select the **Interface Type**. Although your choice here depends on your network topology, this example shows the steps for **Layer3**.
3. On the **Config** tab, expand the **Security Zone** drop-down and select **New Zone**.
4. In the Zone dialog, define a **Name** for new zone, for example L3-trust, and then click **OK**.
5. Select the **IPv4** tab, select the **Static** radio button, and click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.1.254/24.
6. Select **Advanced > Other Info**, expand the **Management Profile** drop-down, and select **New Management Profile**.
7. Enter a **Name** for the profile, such as allow\_ping, and then select the services you want to allow on the interface. For the purposes of allowing access to the external services, you probably only need to enable **Ping** and then click **OK**.  
 These services provide management access to the device, so only select the services that correspond to the management activities you want to allow on this interface. For example, if you plan to use the MGT interface for device configuration tasks through the web interface or CLI, you would not want to enable HTTP, HTTPS, SSH, or Telnet so that you could prevent unauthorized access through this interface (and if you did allow those services, you should limit access to a specific set of **Permitted IP Addresses**).
8. To save the interface configuration, click **OK**.

## Set Up a Data Port for Access to External Services (Continued)

**Step 5** Because the firewall uses the MGT interface by default to access the external services it requires, you must change the interface the firewall uses to send these requests by editing the service routes.

1. Select **Device > Setup > Services > Service Route Configuration.**



 For the purposes of activating your licenses and getting the most recent content and software updates, you will want to change the service route for **DNS**, **Palo Alto Updates**, **URL Updates**, and **WildFire**.

2. Click the **Customize** radio button, and select one of the following:
  - For a predefined service, select **IPv4** or **IPv6** and click the link for the service for which you want to modify the **Source Interface** and select the interface you just configured.  
If more than one IP address is configured for the selected interface, the **Source Address** drop-down allows you select an IP address.
  - To create a service route for a custom destination, select **Destination**, and click **Add**. Enter a **Destination** name and select a **Source Interface**. If more than one IP address is configured for the selected interface, the **Source Address** drop-down allows you select an IP address.
3. Click **OK** to save the settings.
4. Repeat steps 2-3 above for each service route you want to modify.
5. **Commit** your changes.

### Set Up a Data Port for Access to External Services (Continued)

**Step 6** Configure an external-facing interface and an associated zone and then create security and NAT policy rules to allow the firewall to send service requests from the internal zone to the external zone.

1. Select **Network > Interfaces** and then select your external-facing interface. Select **Layer3** as the **Interface Type**, **Add** the IP address (on the **IPv4** or **IPv6** tab), and create the associated **Security Zone** (on the **Config** tab), such as l3-untrust. You do not need to set up management services on this interface.

2. To set up a security rule that allows traffic from your internal network to the Palo Alto Networks update server, select **Policies > Security** and click **Add**. For the purposes of initial configuration, you can create a simple rule that allows all traffic from l3-trust to l3-untrust as follows:

Name	Tag	Zone	Source			Dest
			Address	User	HTTP Profile	Zone
rule1	none	l3-trust	any	any	any	l3-untrust

3. If you are using a private IP address on the internal-facing interface, you will need to create a source NAT rule to translate the address to a publicly routable address. Select **Policies > NAT** and then click **Add**. At a minimum you must define a name for the rule (**General** tab), specify a source and destination zone, l3-trust to l3-untrust in this case (**Original Packet** tab), and define the source address translation settings (**Translated Packet** tab) and then click **OK**.

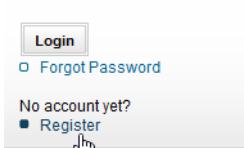
Original Packet							
Name	Tag	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service
source NAT	none	l3-trust	l3-untrust	any	any	any	any

4. **Commit** your changes.

## Set Up a Data Port for Access to External Services (Continued)

<p><b>Step 7</b> Verify that you have connectivity from the data port to the external services, including the default gateway, and the Palo Alto Networks Update Server.</p> <p>After you verify you have the required network connectivity, continue to <a href="#">Register the Firewall</a> and <a href="#">Activate Licenses and Subscriptions</a>.</p>	<ol style="list-style-type: none"><li>1. Use the ping utility to verify network connectivity to the Palo Alto Networks Update server as shown in the following example. Verify that DNS resolution occurs and the response includes the IP address for the Update server; the update server does not respond to a ping request.<pre>admin@PA-200 &gt; ping host updates.paloaltonetworks.com PING updates.paloaltonetworks.com (10.101.16.13) 56(84) bytes of data. From 192.168.1.1 icmp_seq=1 Destination Host Unreachable From 192.168.1.1 icmp_seq=2 Destination Host Unreachable From 192.168.1.1 icmp_seq=3 Destination Host Unreachable From 192.168.1.1 icmp_seq=4 Destination Host Unreachable</pre> After verifying DNS resolution, press Ctrl+C to stop the ping request.</li><li>2. Use the following CLI command to retrieve information on the support entitlement for the firewall from the Palo Alto Networks update server: <code>request support check</code> If you have connectivity, the update server will respond with the support status for your firewall. Because your firewall is not registered, the update server will return the following message: <code>Contact Us https://www.paloaltonetworks.com/company/contact-us.html Support Home https://www.paloaltonetworks.com/support/tabs/overview.html Device not found on this update server</code></li></ol>
---	---

## Register the Firewall

<b>Register the Firewall</b>	
<b>Step 1</b> Log in to the web interface.	Using a secure connection ( <a href="https://">&gt;https&lt;/&gt;</a> ) from your web browser, log in using the new IP address and password you assigned during initial configuration ( <a href="https://&lt;IP address&gt;">https://&lt;IP address&gt;</a> ). You will see a certificate warning; that is okay. Continue to the web page.
<b>Step 2</b> Locate your serial number and copy it to the clipboard.	On the <b>Dashboard</b> , locate your <b>Serial Number</b> in the General Information section of the screen.
<b>Step 3</b> Go to the Palo Alto Networks Support site.	In a new browser tab or window, go to <a href="https://support.paloaltonetworks.com">https://support.paloaltonetworks.com</a> .
<b>Step 4</b> Register the device. The way you register depends on whether you already have a login to the support site.	<ul style="list-style-type: none"> <li>If this is the first Palo Alto Networks device you are registering and you do not yet have a login, click <b>Register</b> on the right side of the page. To register, you must provide your sales order number or customer ID, and the serial number of your firewall (which you can paste from your clipboard) or the authorization code you received with your order. You will also be prompted to set up a username and password for access to the Palo Alto Networks support community.</li> </ul>  <ul style="list-style-type: none"> <li>If you already have a support account, log in and then click <b>My Devices</b>. Scroll down to Register Device section at the bottom of the screen and enter the serial number of your firewall (which you can paste from your clipboard), your city and postal code and then click <b>Register Device</b>.</li> </ul>

## Activate Licenses and Subscriptions

Before you can start using your firewall to secure the traffic on your network, you must activate the licenses for each of the services you purchased. Available licenses and subscriptions include the following:

- **Threat Prevention**—Provides antivirus, anti-spyware, and vulnerability protection.
- **Decryption Mirroring**—Provides the ability to create a copy of decrypted traffic from a firewall and send it to a traffic collection tool that is capable of receiving raw packet captures—such as NetWitness or Solera—for archiving and analysis.
- **URL Filtering**—Allows you create security policy to enforce web access based on dynamic URL categories. You must purchase and install a subscription for one of the supported URL filtering databases: PAN-DB or BrightCloud. With PAN-DB, you can set up access to the PAN-DB public cloud or to the PAN-DB private cloud. For more information about URL filtering, see [Control Access to Web Content](#).
- **Virtual Systems**—This license is required to enable support for multiple virtual systems on PA-2000 and PA-3000 Series firewalls. In addition, you must purchase a Virtual Systems license if you want to increase the number of virtual systems beyond the base number provided by default on PA-4000 Series, PA-5000 Series, and PA-7000 Series firewalls (the base number varies by platform). The PA-500, PA-200, and VM-Series firewalls do not support virtual systems.
- **WildFire**—Although basic WildFire support is included as part of the Threat Prevention license, the WildFire subscription service provides enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding (APK, PDF, Microsoft Office, and Java Applet), as well as the ability to upload files using the WildFire API. A WildFire subscription is also required if your firewalls will be forwarding files to a WF-500 appliance.
- **GlobalProtect**—Provides mobility solutions and/or large-scale VPN capabilities. By default, you can deploy GlobalProtect portals and gateways (without HIP checks) without a license. If you want to use HIP checks, you will also need gateway licenses (subscription) for each gateway.

### Activate Licenses

<b>Step 1</b>	Locate the activation codes for the licenses you purchased.	When you purchased your subscriptions you should have received an email from Palo Alto Networks customer service listing the activation code associated with each subscription. If you cannot locate this email, contact customer support to obtain your activation codes before you proceed.
<b>Step 2</b>	Launch the web interface and go to the license page.	Select <b>Device &gt; Licenses</b> .

<b>Activate Licenses (Continued)</b>							
<b>Step 3</b> Activate each license you purchased.	<p>After purchasing your licenses/subscriptions activate them in one of the following ways:</p> <ul style="list-style-type: none"> <li>• <b>Retrieve license keys from license server</b>—Use this option if you activated your license on the support portal.</li> <li>• <b>Activate feature using authorization code</b>—Use this option to enable purchased subscriptions using an authorization code for licenses that have not been previously activated on the support portal. When prompted, enter the <b>Authorization Code</b> and then click <b>OK</b>.</li> <li>• <b>Manually upload license key</b>—Use this option if your device does not have connectivity to the Palo Alto Networks support site. In this case, you must download a license key file from the support site on an Internet connected computer and then upload to the device.</li> </ul>						
<b>Step 4</b> Verify that the license was successfully activated	<p>On the <b>Device &gt; Licenses</b> page, verify that the license was successfully activated. For example, after activating the WildFire license, you should see that the license is valid:</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>WildFire License</b></p> <table> <tr> <td>Date Issued</td> <td>September 11, 2012</td> </tr> <tr> <td>Date Expires</td> <td>September 11, 2015</td> </tr> <tr> <td>Description</td> <td>WildFire License</td> </tr> </table> </div>	Date Issued	September 11, 2012	Date Expires	September 11, 2015	Description	WildFire License
Date Issued	September 11, 2012						
Date Expires	September 11, 2015						
Description	WildFire License						
<b>Step 5</b> <i>(WildFire subscriptions only)</i> Perform a commit to complete WildFire subscription activation.	<p>After activating a WildFire subscription, a commit is required for the firewall to begin forwarding advanced file types:</p> <ul style="list-style-type: none"> <li>• Commit any pending changes.</li> <li>• Make a minor change and perform a commit. For example, update a rule description and commit the change.</li> </ul> <p> Check that the <b>WildFire Analysis profile rules</b> include the advanced file types that are now supported with the WildFire subscription. If no change to any of the rules is required, make a minor edit to a rule description and perform a commit.</p>						

## Manage Content Updates

In order to stay ahead of the changing threat and application landscape, Palo Alto Networks maintains a Content Delivery Network (CDN) infrastructure for delivering content updates to the Palo Alto Networks devices. The devices access the web resources in the CDN to perform various App-ID and Content-ID functions. By default, the devices use the management port to access the CDN infrastructure for application updates, threat and antivirus signature updates, BrightCloud and PAN-DB database updates and lookups, and access to the Palo Alto Networks WildFire cloud. To ensure that you are always protected from the latest threats (including those that have not yet been discovered), you must ensure that you keep your devices up-to-date with the latest updates published by Palo Alto Networks.

The following content updates are available, depending on which subscriptions you have:



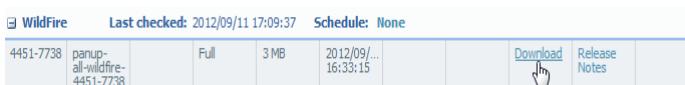
Although you can manually download and install content updates at any time, as a best practice you should [Schedule each update](#). Scheduled updates occur automatically.

- **Antivirus**—Includes new and updated antivirus signatures, including signatures discovered by the WildFire cloud service. You must have a Threat Prevention subscription to get these updates. New antivirus signatures are published daily.
- **Applications**—Includes new and updated application signatures. This update does not require any additional subscriptions, but it does require a valid maintenance/support contract. New application updates are published weekly. To review the policy impact of new application updates, see [Manage New App-IDs Introduced in Content Releases](#).
- **Applications and Threats**—Includes new and updated application and threat signatures. This update is available if you have a Threat Prevention subscription (and you get it instead of the Applications update). New Applications and Threats updates are published weekly.
- **GlobalProtect Data File**—Contains the vendor-specific information for defining and evaluating host information profile (HIP) data returned by GlobalProtect agents. You must have a GlobalProtect gateway license and create an update schedule in order to receive these updates.
- **BrightCloud URL Filtering**—Provides updates to the BrightCloud URL Filtering database only. You must have a BrightCloud subscription to get these updates. New BrightCloud URL database updates are published daily. If you have a PAN-DB license, scheduled updates are not required as devices remain in-sync with the servers automatically.
- **WildFire**—Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire cloud service. Without the subscription, you must wait 24 to 48 hours for the signatures to roll into the Applications and Threat update.

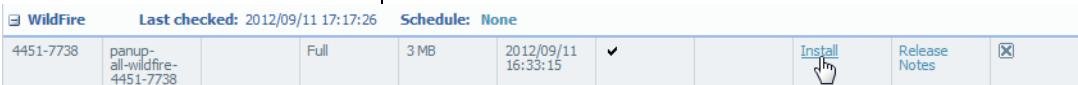


If your firewall does not have Internet access from the management port, you can download content updates from the [Palo Alto Networks Support](#) portal and then Upload them to your firewall.

If your firewall is deployed behind existing firewalls or proxy servers, access to these external resources might be restricted using access control lists that allow the firewall to only access a hostname or an IP address. In such cases, to allow access to the CDN, set the update server address to use the hostname `staticupdates.paloaltonetworks.com` or the IP address `199.167.52.15`. For details on setting up CDN access, see [Content Delivery Network Infrastructure for Dynamic Updates](#).

<b>Update Content</b>	
<b>Step 1</b> Verify that the firewall points to the <a href="#">CDN infrastructure</a> .	Select <b>Device &gt; Setup &gt; Services</b> . <ul style="list-style-type: none"> <li>As a best practice, set the <b>Update Server</b> to access <code>updates.paloaltonetworks.com</code>. This allows the firewall to receive content updates from the server to which it is closest in the CDN infrastructure.</li> <li>(Optional) If the firewall has restricted access to the Internet, set the update server address to use the hostname <code>staticupdates.paloaltonetworks.com</code> or the IP address <code>199.167.52.15</code>.</li> <li>For additional security, select <b>Verify Update Server Identity</b>. The firewall verifies that the server from which the software or content package is download has an SSL certificate signed by a trusted authority.</li> </ul>
<b>Step 2</b> Launch the web interface and go to the Dynamic Updates page.	Select <b>Device &gt; Dynamic Updates</b> .
<b>Step 3</b> Check for the latest updates.	<p>Click <b>Check Now</b> (located in the lower left-hand corner of the window) to check for the latest updates. The link in the <b>Action</b> column indicates whether an update is available:</p> <ul style="list-style-type: none"> <li><b>Download</b>—Indicates that a new update file is available. Click the link to begin downloading the file directly to the firewall. After successful download, the link in the <b>Action</b> column changes from <b>Download</b> to <b>Install</b>.</li> </ul>  <p> You cannot download the antivirus database until you have installed the Application and Threats database.</p> <ul style="list-style-type: none"> <li><b>Upgrade</b>—Indicates that there is a new version of the BrightCloud database available. Click the link to begin the download and installation of the database. The database upgrade begins in the background; when completed a check mark displays in the <b>Currently Installed</b> column. Note that if you are using PAN-DB as your URL filtering database you will not see an upgrade link because the PAN-DB database automatically stays in sync with the server.</li> </ul>  <p> To check the status of an action, click <b>Tasks</b> (on the lower right-hand corner of the window).</p> <ul style="list-style-type: none"> <li><b>Revert</b>—Indicates that a previously installed version of the content or software version is available. You can choose to revert to the previously installed version.</li> </ul>

## Update Content (Continued)

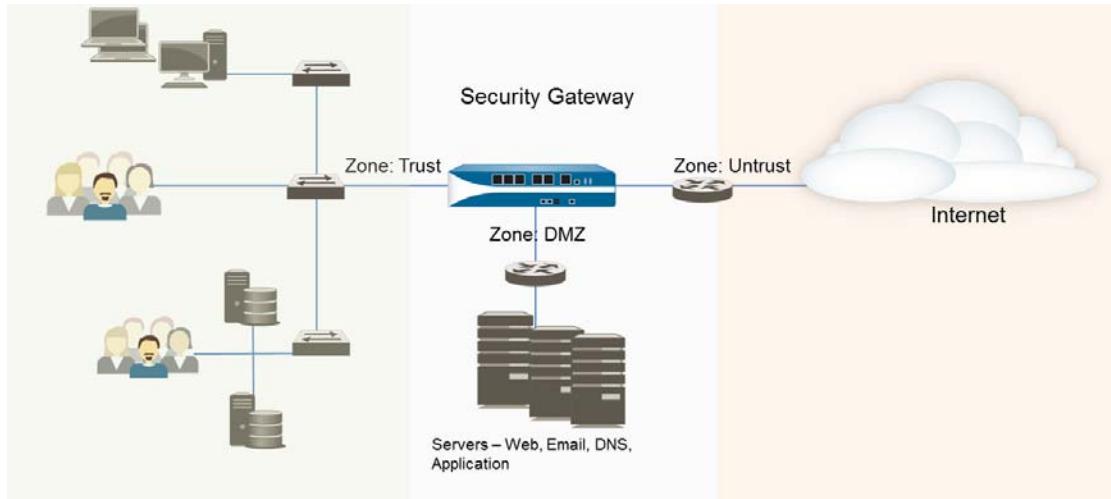
<p><b>Step 4</b> Install the updates.</p> <p> Installation can take up to 20 minutes on a PA-200, PA-500, or PA-2000 Series device and up to two minutes on a PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, or VM-Series firewall.</p>	<p>Click the <b>Install</b> link in the <b>Action</b> column. When the installation completes, a check mark displays in the <b>Currently Installed</b> column.</p>
	
<p><b>Step 5</b> Schedule each update.</p> <p>Repeat this step for each update you want to schedule.</p> <p> Stagger the update schedules because the firewall can only download one update at a time. If you schedule the updates to download during the same time interval, only the first download will succeed.</p>	<ol style="list-style-type: none"> <li>Set the schedule of each update type by clicking the <b>None</b> link.</li>  <li>Specify how often you want the updates to occur by selecting a value from the <b>Recurrence</b> drop-down. The available values vary by content type (WildFire updates are available <b>Every 15 minutes</b>, <b>Every 30 minutes</b> or <b>Every Hour</b> whereas all other content types can be scheduled for <b>Daily</b> or <b>Weekly</b> update).</li> <li>Specify the <b>Time</b> and (or, minutes past the hour in the case of WildFire), if applicable depending on the <b>Recurrence</b> value you selected, <b>Day</b> of the week that you want the updates to occur.</li> <li>Specify whether you want the system to <b>Download Only</b> or, as a best practice, <b>Download And Install</b> the update.</li> <li>In rare instances, errors in content updates may be found. For this reason, you may want to delay installing new updates until they have been released for a certain number of hours. You can specify how long after a release to wait before performing a content update by entering the number of hours to wait in the <b>Threshold (Hours)</b> field.</li> <li>Click <b>OK</b> to save the schedule settings.</li> <li>Click <b>Commit</b> to save the settings to the running configuration.</li> </ol>

## Install Software Updates

When installing a new firewall, it is a good idea to [upgrade to the latest software](#) update (or to the update version that your reseller or Palo Alto Networks Systems Engineer recommends) to take advantage of the latest fixes and security enhancements. Before updating the software, make sure you have the latest content updates as detailed in [Manage Content Updates](#) (the [Release Notes](#) for a software update specify the minimum content release version supported in the release).

# Create the Security Perimeter

Traffic must pass through the firewall in order for the firewall to manage and control it. Physically, traffic enters and exits the firewall through *interfaces*. The firewall determines how to act on a packet based on whether the packet matches a *security policy rule*. At the most basic level, each security policy rule must identify where the traffic came from and where it is going. On a Palo Alto Networks next-generation firewall, security policy rules are applied between zones. A *zone* is a grouping of interfaces (physical or virtual) that provides an abstraction for an area of trust for simplified policy enforcement. For example, in the following topology diagram, there are three zones: Trust, Untrust, and DMZ. Traffic can flow freely within a zone, but traffic will not be able to flow between zones until you define a security policy rule that allows it.



The following topics describe the components of the security perimeter and provide steps for configuring the firewall interfaces, defining zones, and setting up a basic security policy that allows traffic from your internal zone to the Internet and to the DMZ. By initially creating a basic security policy rulebase like this, you will be able to analyze the traffic running through your network and use this information to define more granular policies for safely enabling applications while preventing threats.

- ▲ [Basic Interface Deployments](#)
- ▲ [About Security Policy](#)
- ▲ [Plan the Deployment](#)
- ▲ [Configure Interfaces and Zones](#)
- ▲ [Set Up Basic Security Policies](#)

If you use private IP addresses in your internal networks, you will also need to configure network address translation ([NAT](#)).

## Basic Interface Deployments

All Palo Alto Networks next-generation firewalls provide a flexible networking architecture that includes support for dynamic routing, switching, and VPN connectivity, enabling you to deploy the firewall into nearly any networking environment. When configuring the Ethernet ports on your firewall, you can choose from virtual wire, Layer 2, or Layer 3 interface deployments. In addition, to allow you to integrate into a variety of network segments, you can configure different types of interfaces on different ports. The following sections provide basic information on each type of deployment.

- ▲ [Virtual Wire Deployments](#)
- ▲ [Layer 2 Deployments](#)
- ▲ [Layer 3 Deployments](#)

For more detailed deployment information, refer to [Designing Networks with Palo Alto Networks Firewalls](#).

### Virtual Wire Deployments

In a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together. By using a virtual wire, you can install the firewall in any network environment without reconfiguring adjacent devices. If necessary, a virtual wire can block or allow traffic based on the virtual LAN (VLAN) tag values. You can also create multiple subinterfaces and classify traffic according to an IP Address (address, range, or subnet), VLAN, or a combination of the two.

By default, the virtual wire (named **default-vwire**) binds Ethernet ports 1 and 2 and allows all untagged traffic. Choose this deployment to simplify installation and configuration and/or avoid configuration changes to surrounding network devices.

A virtual wire is the default configuration, and should be used only when no switching or routing is needed. If you do not plan to use the default virtual wire, you should manually delete the configuration before proceeding with interface configuration to prevent it from interfering with other interface settings you define. For instructions on how to delete the default virtual wire and its associated security policy and zones, see [Step 3 in Set Up a Data Port for Access to External Services](#).

### Layer 2 Deployments

In a Layer 2 deployment, the firewall provides switching between two or more interfaces. Each group of interfaces must be assigned to a VLAN object in order for the firewall to switch between them. The firewall will perform VLAN tag switching when Layer 2 subinterfaces are attached to a common VLAN object. Choose this option when switching is required.

For more information on Layer 2 deployments, refer to the [Layer 2 Networking Tech Note](#) and/or the [Securing Inter VLAN Traffic Tech Note](#).

## Layer 3 Deployments

In a Layer 3 deployment, the firewall routes traffic between ports. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing is required.

You must assign an IP address to each physical Layer 3 interface you configure. You can also create logical subinterfaces for each physical Layer 3 interface that allows you to segregate the traffic on the interface based on VLAN tag (when VLAN trunking is in use) or by IP address, for example for multi-tenancy.

In addition, because the firewall must route traffic in a Layer 3 deployment, you must configure a virtual router. You can configure the virtual router to participate with dynamic routing protocols ([BGP](#), [OSPF](#), or [RIP](#)) as well as adding static routes. You can also create multiple virtual routers, each maintaining a separate set of routes that are not shared between virtual routers, enabling you to configure different routing behaviors for different interfaces. For more information on routing integrations on the firewall, see the [PAN-OS Admin Guide](#).

The configuration example in this chapter illustrates how to integrate the firewall into your Layer 3 network using static routes.

## About Security Policy

[Security Policy](#) protects network assets from threats and disruptions and aids in optimally allocating network resources for enhancing productivity and efficiency in business processes. On the Palo Alto Networks firewall, security policy rules determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

For traffic that doesn't match any defined rules, the default rules apply. The default rules—displayed at the bottom of the security rulebase—are predefined to allow all intrazone (within the zone) traffic and deny all interzone (between zones) traffic. Although these rules are part of the pre-defined configuration and are read-only by default, you can override them and change a limited number of settings, including the tags, action (allow or deny), log settings, and security profiles.

Security policies rules are evaluated left to right and from top to bottom. A packet is matched against the first rule that meets the defined criteria; after a match is triggered the subsequent rules are not evaluated. Therefore, the more specific rules must precede more generic ones in order to enforce the best match criteria. Traffic that matches a rule generates a log entry at the end of the session in the traffic log, if logging is enabled for that rule. The logging options are configurable for each rule, and can for example be configured to log at the start of a session instead of, or in addition to, logging at the end of a session.

- ▲ [Actions in Security Policy](#)
- ▲ [About Policy Objects](#)
- ▲ [About Security Profiles](#)

## Actions in Security Policy

For traffic that matches the attributes defined in a security policy, you can apply the following actions:

Action	Description
<b>Allow</b> (default action)	Allows the traffic.
<b>Deny</b>	Blocks traffic, and enforces the default <i>Deny Action</i> defined for the application that is being denied. To view the deny action defined by default for an application, view the application details in <b>Objects &gt; Applications</b> or check the application details in <a href="#">Applipedia</a> .
<b>Drop</b>	Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset is not sent to the host/application.  For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: <b>Drop</b> and enable the <b>Send ICMP Unreachable</b> check box. When enabled, the firewall sends the ICMP code for <i>communication with the destination is administratively prohibited</i> —ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.
<b>Reset client</b>	Sends a TCP reset to the client-side device.
<b>Reset server</b>	Sends a TCP reset to the server-side device.
<b>Reset both</b>	Sends a TCP reset to both the client-side and server-side devices.



A reset is sent only after a session is formed. If the session is blocked before a 3-way handshake is completed, the firewall will not send the reset.

For a TCP session with a reset action, the firewall does not send an ICMP Unreachable response.

For a UDP session with a drop or reset action, if the **ICMP Unreachable** check box is selected, the firewall sends an ICMP message to the client.

## About Policy Objects

A *policy object* is a single object or a collective unit that groups discrete identities such as IP addresses, URLs, applications, or users. With [Policy Objects](#) that are a collective unit, you can reference the object in security policy instead of manually selecting multiple objects one at a time. Typically, when creating a policy object, you group objects that require similar permissions in policy. For example, if your organization uses a set of server IP addresses for authenticating users, you can group the set of server IP addresses as an *address group* policy object and reference the address group in the security policy. By grouping objects, you can significantly reduce the administrative overhead in creating policies.

Some examples of address and application policy objects are shown in the security policies that are included in [Create Security Rules](#). For information on the other policy objects, see [Enable Basic Threat Prevention Features](#).

## About Security Profiles

While security policies enable you to allow or deny traffic on your network, security profiles help you define an *allow but scan* rule, which scan allowed applications for threats. When traffic matches the allow rule defined in the security policy, the [Security Profiles](#) that are attached to the rule are applied for further content inspection rules such as antivirus checks and data filtering.



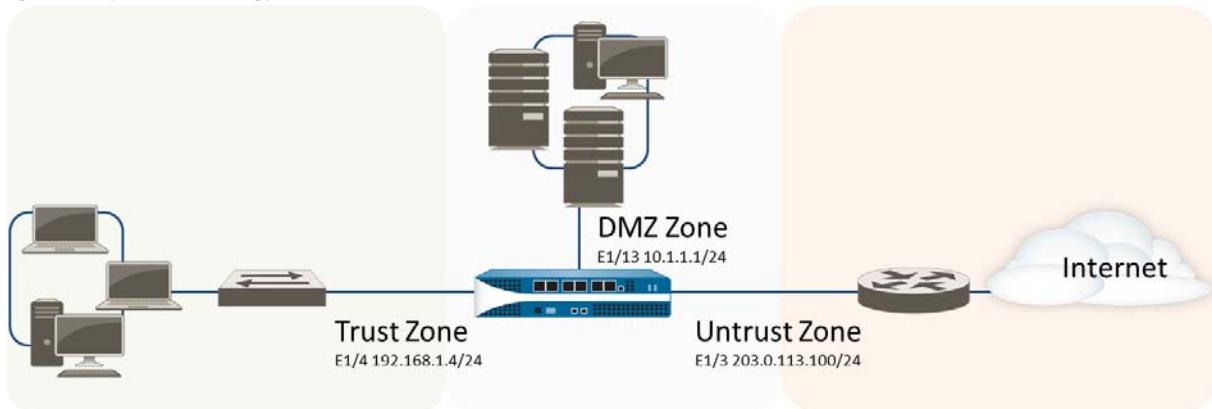
Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.

The different types of security profiles that can be attached to security policies are: Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, and Data Filtering. The firewall provides default security profiles that you can use out of the box to begin protecting your network from threats. See [Create Security Rules](#) for information on using the default profiles in your security policy. As you get a better understanding about the security needs on your network, you can create custom profiles. See [Scan Traffic for Threats](#) for more information.

## Plan the Deployment

Before you begin configuring interfaces and zones, take some time to plan the zones you will need based on the different usage requirements within your organization. In addition, you should gather all of the configuration information you will need ahead of time. At a basic level, you should plan which interfaces will belong to which zones. For Layer 3 deployments you'll also need to obtain the required IP addresses and network configuration information from your network administrator, including information on how to configure the routing protocol or static routes required for the virtual router configuration. The example in this chapter will be based on the following topology:

**Figure: Layer 3 Topology Example**



The following table shows the information we will use to configure the Layer 3 interfaces and their corresponding zones as shown in the sample topology.

Zone	Deployment Type	Interface(s)	Configuration Settings
Untrust	L3	Ethernet1/3	<b>IP address:</b> 203.0.113.100/24 <b>Virtual router:</b> default <b>Default route:</b> 0.0.0.0/0 <b>Next hop:</b> 203.0.113.1
Trust	L3	Ethernet1/4	<b>IP address:</b> 192.168.1.4/24 <b>Virtual router:</b> default
DMZ	L3	Ethernet1/13	<b>IP address:</b> 10.1.1.1/24 <b>Virtual router:</b> default

## Configure Interfaces and Zones

After you plan your zones and the corresponding interfaces, you can configure them on the device. The way you configure each interface depends on your network topology.

The following procedure shows how to configure a Layer 3 deployment as depicted in [Figure: Layer 3 Topology Example](#).



The firewall comes preconfigured with a default virtual wire interface between ports Ethernet 1/1 and Ethernet 1/2 (and a corresponding default security policy and virtual router). If you do not plan to use the default virtual wire, you must manually delete the configuration and commit the change before proceeding to prevent it from interfering with other settings you define. For instructions on how to delete the default virtual wire and its associated security policy and zones, see Step 3 in [Set Up a Data Port for Access to External Services](#).

### Set Up Interfaces and Zones

<p><b>Step 1</b> Configure a default route to your Internet router.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Virtual Router</b> and then select the <b>default</b> link to open the Virtual Router dialog.</li><li>2. Select the <b>Static Routes</b> tab and click <b>Add</b>. Enter a <b>Name</b> for the route and enter the route in the <b>Destination</b> field (for example, 0.0.0.0/0).</li><li>3. Select the <b>IP Address</b> radio button in the <b>Next Hop</b> field and then enter the IP address and netmask for your Internet gateway (for example, 203.00.113.1).</li><li>4. Click <b>OK</b> twice to save the virtual router configuration.</li></ol>
<p><b>Step 2</b> Configure the external interface (the interface that connects to the Internet).</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces</b> and then select the interface you want to configure. In this example, we are configuring Ethernet1/3 as the external interface.</li><li>2. Select the <b>Interface Type</b>. Although your choice here depends on your network topology, this example shows the steps for <b>Layer3</b>.</li><li>3. On the <b>Config</b> tab, select <b>New Zone</b> from the <b>Security Zone</b> drop-down. In the Zone dialog, define a <b>Name</b> for new zone, for example Untrust, and then click <b>OK</b>.</li><li>4. In the <b>Virtual Router</b> drop-down, select <b>default</b>.</li><li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 208.80.56.100/24.</li><li>6. To enable you to ping the interface, select <b>Advanced &gt; Other Info</b>, expand the <b>Management Profile</b> drop-down, and select <b>New Management Profile</b>. Enter a <b>Name</b> for the profile, select <b>Ping</b> and then click <b>OK</b>.</li><li>7. To save the interface configuration, click <b>OK</b>.</li></ol>

## Set Up Interfaces and Zones (Continued)

<p><b>Step 3</b> Configure the interface that connects to your internal network.</p> <p> In this example, the interface connects to a network segment that uses private IP addresses. Because private IP addresses cannot be routed externally, you will have to configure <b>NAT</b>.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces</b> and select the interface you want to configure. In this example, we are configuring Ethernet1/4 as the internal interface.</li> <li>2. Select <b>Layer3</b> from the <b>Interface Type</b> drop-down.</li> <li>3. On the <b>Config</b> tab, expand the <b>Security Zone</b> drop-down and select <b>New Zone</b>. In the Zone dialog, define a <b>Name</b> for new zone, for example Trust, and then click <b>OK</b>.</li> <li>4. Select the same Virtual Router you used in <b>Step 2</b>, default in this example.</li> <li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.1.4/24.</li> <li>6. To enable you to ping the interface, select the management profile that you created in <b>Step 2-6</b>.</li> <li>7. To save the interface configuration, click <b>OK</b>.</li> </ol>
<p><b>Step 4</b> Configure the interface that connects to the DMZ.</p>	<ol style="list-style-type: none"> <li>1. Select the interface you want to configure.</li> <li>2. Select <b>Layer3</b> from the <b>Interface Type</b> drop-down. In this example, we are configuring Ethernet1/13 as the DMZ interface.</li> <li>3. On the <b>Config</b> tab, expand the <b>Security Zone</b> drop-down and select <b>New Zone</b>. In the Zone dialog, define a <b>Name</b> for new zone, for example DMZ, and then click <b>OK</b>.</li> <li>4. Select the Virtual Router you used in <b>Step 2</b>, default in this example.</li> <li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 10.1.1.1/24.</li> <li>6. To enable you to ping the interface, select the management profile that you created in <b>Step 2-6</b>.</li> <li>7. To save the interface configuration, click <b>OK</b>.</li> </ol>
<p><b>Step 5</b> Save the interface configuration.</p>	Click <b>Commit</b> .
<p><b>Step 6</b> Cable the firewall.</p>	Attach straight through cables from the interfaces you configured to the corresponding switch or router on each network segment.
<p><b>Step 7</b> Verify that the interfaces are active.</p>	From the web interface, select <b>Network &gt; Interfaces</b> and verify that icon in the Link State column is green. You can also monitor link state from the <b>Interfaces</b> widget on the <b>Dashboard</b> . 

## Set Up Basic Security Policies

Policies allow you to enforce rules and take action. The different types of policy rules that you can create on the firewall are: Security, NAT, Quality of Service (QoS), Policy Based Forwarding (PBF), Decryption, Application Override, Captive Portal, Denial of Service, and Zone protection policies. All these different policies work together to allow, deny, prioritize, forward, encrypt, decrypt, make exceptions, authenticate access, and reset connections as needed to help secure your network. This section covers basic security policies and the default security profiles:

- ▲ [Create Security Rules](#)
- ▲ [Test Your Security Policies](#)
- ▲ [Monitor Network Traffic](#)

### Create Security Rules

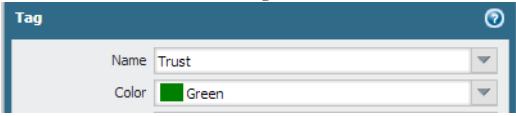
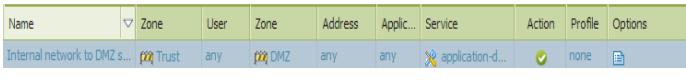
Security policies reference security zones and enable you to allow, restrict, and track traffic on your network. Because each zone implies a level of trust, the implicit rule for passing traffic between two different zones is deny, and the traffic within a zone is permitted. To allow traffic between two different zones, you must create a security rule that allows traffic to flow between them.

While setting up the basic framework for securing the enterprise perimeter, it's good idea to start with a simple security policy that allows traffic between the different zones without being too restrictive. As illustrated in the following section, our objective is to minimize the likelihood of breaking applications that users on the network need access to, while providing visibility into the applications and the potential threats for your network.



When defining policies make sure that you do not create a policy that denies all traffic from *any* source zone to *any* destination zone as this will break intra-zone traffic that is implicitly allowed. By default, intra-zone traffic is permitted because the source and destination zones are the same and therefore share the same level of trust.

## Define Basic Security Rules

<p><b>Step 1</b> Permit Internet access for all users on the enterprise network.</p> <p>Zone: Trust to Untrust</p> <p> By default, the firewall includes a security rule named <i>rule1</i> that allows all traffic from Trust zone to Untrust zone. You can either delete the rule or modify the rule to reflect your zone-naming convention.</p>	<p>To safely enable applications that are required for day-to-day business operations we will create a simple rule that allows access to the Internet. To provide basic threat protection, we will attach the default security profiles available on the firewall.</p> <ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b> and click <b>Add</b>.</li> <li>2. Give the rule a descriptive name in the <b>General</b> tab.</li> <li>3. In the <b>Source</b> tab, set the <b>Source Zone</b> to Trust.</li> <li>4. In the <b>Destination</b> tab, Set the <b>Destination Zone</b> to Untrust.</li> <li>5. To scan policy rules and visually identify the zones on each rule, create a tag with the same name as the zone. For example, to color code the Trust zone as green, select <b>Objects &gt; Tags</b>, click <b>Add</b> and <b>Name</b> the tag Trust, and select the <b>Color</b> green.</li>  <li>6. In the <b>Service/ URL Category</b> tab, select service-http and service-https.</li> <li>7. In the <b>Actions</b> tab, complete these tasks:       <ol style="list-style-type: none"> <li>a. Set the <b>Action Setting</b> to <b>Allow</b>.</li> <li>b. Attach the default profiles for antivirus, anti-spyware, vulnerability protection and URL filtering, under <b>Profile Setting</b>.</li> </ol> </li> <li>8. Verify that logging is enabled at the end of a session under <b>Options</b>. Only traffic that matches a security rule will be logged.</li>  </ol>
<p><b>Step 2</b> Permit users on the internal network to access the servers in the DMZ.</p> <p>Zone: Trust to DMZ</p> <p> If using IP addresses for configuring access to the servers in the DMZ, make sure to always refer to the original IP addresses in the packet (i.e. the pre-NAT addresses), and the post-NAT zone.</p>	<ol style="list-style-type: none"> <li>1. Click <b>Add</b> in the <b>Policies &gt; Security</b> section.</li> <li>2. Give the rule a descriptive name in the <b>General</b> tab.</li> <li>3. In the <b>Source</b> tab, set the <b>Source Zone</b> to Trust.</li> <li>4. In the <b>Destination</b> tab, set the <b>Destination Zone</b> to DMZ.</li> <li>5. In the <b>Service/ URL Category</b> tab, make sure the <b>Service</b> is set to <b>application-default</b>.</li> <li>6. In the <b>Actions</b> tab, set the <b>Action Setting</b> to Allow.</li> <li>7. Leave all the other options at the default values.</li>  </ol>

### Define Basic Security Rules (Continued)

**Step 3** Restrict access from the Internet to the servers on the DMZ to specific server IP addresses only.

For example, you might only allow users to access the webmail servers from outside.

Zone: Untrust to DMZ

To restrict inbound access to the DMZ from the Internet, configure a rule that allows access only to specific servers IP addresses and on the default ports that the applications use.

1. Click **Add** to add a new rule, and give it a descriptive name.
2. In the **Source** tab, set the **Source Zone** to Untrust.
3. In the **Destination** tab, set the **Destination Zone** to DMZ.
4. Set the **Destination Address** to the **Public web server** address object you created earlier. The public web server address object references the public IP address—208.80.56.11/24—of the web server that is accessible on the DMZ.
5. Select the webmail application in the **Application** tab.



The **Service** is set to **application-default** by default.

Name	Zone	Address	Zone	Address	Application	Service	Action	Profile
Internet to DMZ	untrust	any	DMZ	Public web server	outlook-web	application-default	Allow	none

6. Set the **Action Setting** to **Allow**.

**Step 4** Allow access from the DMZ to your internal network (Trust zone). To minimize risk, you will allow traffic only between specific servers and destination addresses. For example, if you have an application server on the DMZ that needs to communicate with a specific database server in your Trust zone, create a rule to allow traffic between a specific source to a specific destination.

Zone: DMZ to Trust

1. Click **Add** to add a new rule, and give it a descriptive name.
2. Set the **Source Zone** to DMZ.
3. Set the **Destination Zone** to Trust.
4. Create a an address object that specifies the server(s) on your Trust zone that can be accessed from the DMZ.

**Address**

Name	Database servers accessible from DMZ
Description	
Type	IP Range
Enter an IP address range (Ex. 10.0.0.1-10.0.0.4). Each of the IP addresses in the range can also be in an IPv6 form (Ex. 2001:db8:123:1::1-2001:db8:123:1::11)	
192.168.1.200-192.168.1.202	

5. In the **Destination** tab on the Security Policy rule, set the **Destination Address** to the Address object you created above.
6. In the **Actions** tab, complete these tasks:
  - a. Set the **Action Setting** to **Allow**.
  - b. Attach the default profiles for antivirus, anti-spyware, vulnerability protection, under **Profile Setting**.
  - c. In the Other Settings section, select the option to **Disable Server Response Inspection**. This setting disables the antivirus and anti-spyware scanning on the server-side responses, and thus reduces the load on the firewall.

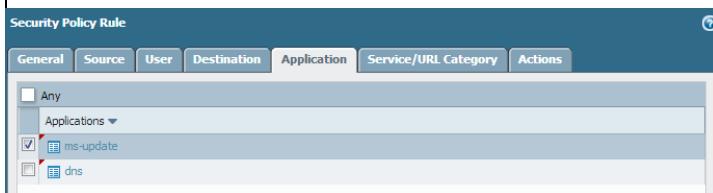
Name	Zone	Address	Zone	Address	Application	Service	Action
Internal network to D...	DMZ	any	untrust	Database acc...	any	any	Allow

### Define Basic Security Rules (Continued)

**Step 5** Enable the servers on the DMZ to obtain updates and hot fixes from the Internet. Say, for example, you would like to allow the Microsoft Update service.

Zone: DMZ to Untrust

1. Add a new rule and give it a descriptive label.
2. Set the **Source Zone** to DMZ.
3. Set the **Destination Zone** to Untrust.
4. Create an application group to specify the applications that you would like to allow. In this example, we allow Microsoft updates (ms-updates) and dns.



The **Service** is set to **application-default** by default. This allows the firewall to permit the applications only when they use the standard ports associated with these applications.

5. Set the **Action Setting** to **Allow**.
6. Attach the default profiles for antivirus, anti-spyware, and vulnerability protection, under **Profiles**.

Name	Zone	User	Zone	Address	Application	Service	Action	Profile	Options
Updates-DMZ to Internet	DMZ	any	Untrust	any	dns	application-d...	Allow	AV, AS, DV	

**Step 6** Save your policies to the running configuration on the device.

Click **Commit**.

## Test Your Security Policies

To verify that you have set up your basic policies effectively, test whether your security policies are being evaluated and determine which security rule applies to a traffic flow.

### Verify Policy Match Against a Flow

To verify the policy rule that matches a flow, use the following CLI command:

```
test security-policy-match source <IP_address> destination <IP_address>
destination port <port_number> protocol <protocol_number>
```

The output displays the best rule that matches the source and destination IP address specified in the CLI command.

For example, to verify the policy rule that will be applied for a server on the DMZ with the IP address 208.90.56.11 when it accesses the Microsoft update server, you will try the following command:

```
test security-policy-match source 208.80.56.11
destination 176.9.45.70 destination-port 80
protocol 6
```

```
"Updates-DMZ to Internet" {
    from dmz;
    source any;
    source-region any;
    to untrust;
    destination any;
    destination-region any;
    user any;
    category any;
    application/service[dns/tcp/any/53
dns/udp/any/53 dns/udp/any/5353
ms-update/tcp/any/80 ms-update/tcp/any/443];
    action allow;
    terminal yes;
```

## Monitor Network Traffic

Now that you have a basic security policy, you can review the statistics and data in the Application Command Center (ACC), traffic logs, and the threat logs to observe trends on your network, to identify where you need to create more granular policies.

### Monitor Network Traffic

- Use the Application Command Center and [Use the Automated Correlation Engine](#).

In the ACC, review the most used applications and the high-risk applications on your network. The ACC graphically summarizes the log information to highlight the applications traversing the network, who is using them (with [User-ID](#) enabled), and the potential security impact of the content to help you identify what is happening on the network in real time. You can then use this information to create appropriate security policy rules that block unwanted applications, while allowing and enabling applications in a secure manner.

The Compromised Hosts widget in **ACC > Threat Activity** displays potentially compromised hosts on your network and the logs and match evidence that corroborates the events.

<b>Monitor Network Traffic</b>	
<ul style="list-style-type: none"> <li>Determine what updates/modifications are required for your network security policy rules and implement the changes.</li> </ul>	<p>For example:</p> <ul style="list-style-type: none"> <li>Evaluate whether to allow content based on schedule, users, or groups.</li> <li>Allow or control certain applications or functions within an application.</li> <li>Decrypt and inspect content.</li> <li>Allow but scan for threats and exploits.</li> </ul> <p>For information on refining your security policies and for attaching custom security profiles, see <a href="#">Enable Basic Threat Prevention Features</a>.</p>
<ul style="list-style-type: none"> <li><a href="#">View the Log Files</a>.</li> </ul>	<p>Specifically, view the traffic and threat logs (<b>Monitor &gt; Logs</b>).</p>  <p>Traffic logs are dependent on how your security policies are defined and set up to log traffic. The Application Usage widget in the <b>ACC</b>, however, records applications and statistics regardless of policy configuration; it shows all traffic that is allowed on your network, therefore it includes the inter-zone traffic that is allowed by policy and the same zone traffic that is allowed implicitly</p>
<ul style="list-style-type: none"> <li><a href="#">Monitor Web Activity of Network Users</a>.</li> </ul>	<p>Review the URL filtering logs to scan through alerts, denied categories/URLs. URL logs are generated when a traffic matches a security rule that has a URL filtering profile attached with an action of alert, continue, override or block.</p>

## Enable Basic Threat Prevention Features

The Palo Alto Networks next-generation firewall has unique threat prevention capabilities that allow it to protect your network from attack despite evasive, tunneled, or circumvention techniques. The threat prevention features on the firewall include the WildFire service, the Security Profiles that support Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking and Data Filtering capabilities and the Denial of Service (DoS) and Zone protection functionality.



Before you can apply threat prevention features, you must first configure zones—to identify one or more source or destination interfaces—and security policy rules. To configure interfaces, zones, and the policies that are needed to apply threat prevention features, see [Configure Interfaces and Zones](#) and [Set Up Basic Security Policies](#).

To begin protecting your network from threats start here:

- ▲ [Enable WildFire](#)
- ▲ [Scan Traffic for Threats](#)
- ▲ [Control Access to Web Content](#)

## Enable WildFire

The [WildFire](#) service is included as part of the base product. The WildFire service enables the firewall to forward attachments to a sandbox environment where applications are run to detect any malicious activity. As new malware is detected by the WildFire service, malware signatures are automatically generated and are made available within 24-48 hours in the antivirus daily downloads. Your threat prevention subscription entitles you to antivirus signature updates that include signatures discovered by WildFire.

Consider purchasing the WildFire subscription service for these additional benefits:

- Sub-hourly (as often as every 15 minutes) WildFire signature updates.
- Advanced file type forwarding for APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. Portable Executable (PE) files can be forwarded for WildFire analysis both with and without a WildFire subscription.
- Ability to upload files using the WildFire API.
- Ability to forward files to a private WF-500 WildFire appliance. When using a WildFire appliance, you can also set up a WildFire hybrid cloud, enabling the WildFire appliance to analyze sensitive file types locally, while other less sensitive file types (such as PEs) or file types not supported for WildFire appliance analysis (such as APKs) can be forwarded to the WildFire cloud.

### Enable WildFire

Step 1	Confirm that your device is registered and that you have a valid support account as well as any subscriptions you require.	<ol style="list-style-type: none"><li>1. Go to the <a href="#">Palo Alto Networks Support Site</a>, log in, and select <b>My Devices</b>.</li><li>2. Verify that the firewall is listed. If it is not listed, see <a href="#">Register the Firewall</a>.</li><li>3. (Optional) <a href="#">Activate Licenses and Subscriptions</a>.</li></ol>
--------	--	---

<b>Enable WildFire (Continued)</b>	
<p><b>Step 2</b> Set the WildFire forwarding options.</p> <p> If you do not have a WildFire subscription you can only forward PEs.</p>	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; WildFire</b> and edit the General Settings.</li> <li>(Optional) Specify the WildFire cloud or WildFire appliance (or both) to which the firewall will forward files for analysis. By default, the firewall will forward files to the public WildFire cloud hosted in the United States (wildfire.paloaltonetworks.com). To forward files to the WildFire cloud hosted in Japan or to enable file-forwarding to a WildFire appliance, update the following fields:           <ul style="list-style-type: none"> <li><b>WildFire Public Cloud</b>—To forward files to the public WildFire cloud running in Japan, enter <code>wildfire.paloaltonetworks.jp</code>.</li> <li><b>WildFire Private Cloud</b>—To forward files to a private WildFire cloud, enter the IP address or FQDN of your WF-500 WildFire appliance.</li> </ul> </li> <li>Review the maximum file size that the firewall can forward for a specific type of file.           <p> It is a <a href="#">WildFire best practice</a> to set the <b>File Size</b> limit for PEs to the maximum file size supported: 10 MB.</p> </li> <li>Click <b>OK</b> to save WildFire settings.</li> </ol>
<p><b>Step 3</b> Enable the firewall to forward decrypted SSL traffic for WildFire analysis.</p> <p> This is a <a href="#">WildFire best practice</a>.</p>	<p><b>On a firewall with no virtual systems configured:</b></p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; Content-ID</b>.</li> <li>Edit the Content-ID settings and <b>Allow Forwarding of Decrypted Content</b>.</li> <li>Click <b>OK</b> to save the changes.</li> </ol> <p><b>On a firewall with multiple virtual systems configured:</b></p> <p>Select <b>Device &gt; Virtual Systems</b>, select the virtual system you want to modify, and <b>Allow Forwarding of Decrypted Content</b>.</p>
<p><b>Step 4</b> Set up a WildFire Analysis profile to forward files to WildFire.</p>	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Security Profiles &gt; WildFire Analysis</b> and click <b>Add</b>.</li> <li>Enter a <b>Name</b> and optionally a <b>Description</b> for the profile.</li> <li>Click <b>Add</b> to create a forwarding rule and enter a name.</li> <li>Define traffic to be forwarded to the WildFire service based on <b>Applications, File Types</b>, or transmission <b>Direction</b>.</li> <li>In the <b>Analysis</b> column, select <b>public-cloud</b> to forward the defined files to the WildFire cloud or select <b>private-cloud</b> to forward files to the WildFire appliance.</li> <li>(Optional) Add additional forwarding rules as necessary.</li> <li>Click <b>OK</b> to save the profile.</li> </ol>

Enable WildFire (Continued)	
Step 5	Attach the WildFire Analysis profile to the security policies that allow access to the Internet.
	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b> and either select an existing policy or create a new policy as described in <a href="#">Create Security Rules</a>.</li><li>2. Click the <b>Actions</b> tab within the security policy.</li><li>3. In the Profile Settings section, click the drop-down and select the WildFire Analysis profile you created for WildFire forwarding. (If you don't see a drop-down for selecting a profile, select <b>Profiles</b> from the <b>Profile Type</b> drop-down.)</li></ol>
Step 6	Save the configuration.
Step 7	Verify that the firewall is forwarding files to the WildFire cloud or the WildFire appliance.
	<ol style="list-style-type: none"><li>1. Select <b>Monitor &gt; Logs &gt; WildFire Submissions</b> to WildFire logs. For each log entry displayed, the firewall has successfully forwarded the file to WildFire and WildFire has returned a file analysis report.</li><li>2. Check the <b>WildFire Cloud</b> column to view if a file was forwarded to the WildFire cloud or the WildFire appliance for analysis.</li></ol>

## Scan Traffic for Threats

Security Profiles provide threat protection in security policies. For example, you can apply an antivirus profile to a security policy and all traffic that matches the security policy will be scanned for viruses.

The following sections provide steps for setting up a basic threat prevention configuration:

- ▲ [Set Up Antivirus, Anti-Spyware, and Vulnerability Protection](#)
- ▲ [Set Up File Blocking](#)

### Set Up Antivirus, Anti-Spyware, and Vulnerability Protection

Every Palo Alto Networks next-generation firewall comes with predefined Antivirus, Anti-Spyware, and Vulnerability Protection profiles that you can attach to security policies. There is one predefined Antivirus profile, **default**, which uses the default action for each protocol (block HTTP, FTP, and SMB traffic and alert on SMTP, IMAP, and POP3 traffic). There are two predefined Anti-Spyware and Zone Protection profiles:

- **default**—Applies the default action to all client and server critical, high, and medium severity spyware/vulnerability protection events. It does not detect low and informational events.
- **strict**—Applies the block response to all client and server critical, high and medium severity spyware/vulnerability protection events and uses the default action for low and informational events.

To ensure that the traffic entering your network is free from threats, attach the predefined profiles to your basic web access policies. As you monitor the traffic on your network and expand your policy rulebase, you can then design more granular profiles to address your specific security needs.

#### Set up Antivirus/Anti-Spyware/Vulnerability Protection

Step 1 Verify that you have a Threat Prevention license.	<ul style="list-style-type: none"><li>• The Threat Prevention license bundles the Antivirus, Anti-Spyware, and the Vulnerability Protection features in one license.</li><li>• Select <b>Device &gt; Licenses</b> to verify that the <b>Threat Prevention</b> license is installed and valid (check the expiration date).</li></ul>
Step 2 Download the latest antivirus threat signatures.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Dynamic Updates</b> and click <b>Check Now</b> at the bottom of the page to retrieve the latest signatures.</li><li>2. In the <b>Actions</b> column, click <b>Download</b> to install the latest Antivirus, and Applications and Threats signatures.</li></ol>

## Set up Antivirus/Anti-Spyware/Vulnerability Protection (Continued)

### Step 3 Schedule signature updates.



Perform a **download-and-install** on a daily basis for antivirus updates and weekly for applications and threats updates.

1. From **Device > Dynamic Updates**, click the text to the right of **Schedule** to automatically retrieve signature updates for **Antivirus** and **Applications and Threats**.
2. Specify the frequency and timing for the updates and whether the update will be downloaded and installed or only downloaded. If you select **Download Only**, you would need to manually go in and click the **Install** link in the **Action** column to install the signature. When you click **OK**, the update is scheduled. No commit is required.
3. (Optional) You can also enter the number of hours in the **Threshold** field to indicate the minimum age of a signature before a download will occur. For example, if you entered **10**, the signature must be at least 10 hours old before it will be downloaded, regardless of the schedule.
4. In an HA configuration, you can also click the **Sync To Peer** option to synchronize the content update with the HA peer after download/install. This will not push the schedule settings to the peer device, you need to configure the schedule on each device.

### Recommendations for HA Configurations:

- **Active/Passive HA**—If the MGT port is used for antivirus signature downloads, you should configure a schedule on both devices and both devices will download/install independently. If you are using a data port for downloads, the passive device will not perform downloads while it is in the passive state. In this case you would set a schedule on both devices and then select the **Sync To Peer** option. This will ensure that whichever device is active, the updates will occur and will then push to the passive device.
- **Active/Active HA**—If the MGT port is used for antivirus signature downloads on both devices, then schedule the download/install on both devices, but do not select the **Sync To Peer** option. If you are using a data port, schedule the signature downloads on both devices and select **Sync To Peer**. This will ensure that if one device in the active/active configuration goes into the active-secondary state, the active device will download/install the signature and will then push it to the active-secondary device.

### Set up Antivirus/Anti-Spyware/Vulnerability Protection (Continued)

**Step 4** Attach the security profiles to a security policy.



Attach a clone of a predefined security profile to your basic security policies. That way, if you want to customize the profile you can do so without deleting the read-only predefined **strict** or **default** profile and attaching a customized profile.

1. Select **Policies > Security**, select the desired policy to modify it and then click the **Actions** tab.

2. In **Profile Settings**, click the drop-down next to each security profile you would like to enable. In this example we choose default for **Antivirus**, **Vulnerability Protection**, and **Anti-Spyware**.



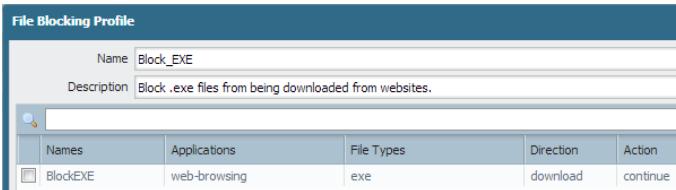
If you don't see drop-downs for selecting profiles, select **Profiles** from the **Profile Type** drop-down.

**Step 5** Save the configuration.

Click **Commit**.

## Set Up File Blocking

[File Blocking Profiles](#) allow you to identify specific file types that you want to want to block or monitor. The following workflow shows how to set up a basic file blocking profile that prevents users from downloading executable files from the Internet.

Configure File Blocking	
Step 1 Create the file blocking profile.	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Security Profiles &gt; File Blocking</b> and click <b>Add</b>.</li> <li>Enter a <b>Name</b> for the file blocking profile, for example <b>Block_EXE</b>.</li> <li>Optionally enter a <b>Description</b>, such as <b>Block users from downloading exe files from websites</b>.</li> </ol>
Step 2 Configure the file blocking options.	<ol style="list-style-type: none"> <li>Click <b>Add</b> to define the profile settings.</li> <li>Enter a <b>Name</b>, such as <b>BlockEXE</b>.</li> <li>Set the <b>Applications</b> to which to apply file blocking, or leave it set to <b>any</b>.</li> <li>Set <b>File Types</b> to block. For example, to block download of executables, you would select <b>exe</b>.</li> <li>Specify the <b>Direction</b> in which to block files: <b>download, upload, or both</b>.</li> <li>Set the <b>Action</b> to one of the following: <ul style="list-style-type: none"> <li>• <b>continue</b>—(web traffic only) Files matching the selected criteria will trigger a customizable response page that requires users to click <b>Continue</b> in order to proceed with the download/upload. You must enable response pages on the associated interfaces if you plan to use this option (<a href="#">Step 4</a>).</li> <li>• <b>block</b>—Files matching the selected criteria will be blocked from download/upload.</li> <li>• <b>alert</b>—Files matching the selected criteria will be allowed, but will generate a log entry in the data filtering log.</li> </ul> </li> </ol> 
Step 3 Attach the file blocking profile to the security policies that allow access to content.	<ol style="list-style-type: none"> <li>Click <b>OK</b> to save the profile.</li> </ol> <ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and either select an existing policy or create a new policy as described in <a href="#">Create Security Rules</a>.</li> <li>Click the <b>Actions</b> tab within the security policy.</li> <li>In the Profile Settings section, click the drop-down and select the file blocking profile you created.</li> </ol> <p> If you don't see drop-downs for selecting profiles, select <b>Profiles</b> from the <b>Profile Type</b> drop-down.</p>

Configure File Blocking (Continued)	
<p><b>Step 4</b> Enable response pages in the management profile for each interface on which you are attaching file blocking profile with a <b>continue</b> action.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b> and then select an interface profile to edit or click <b>Add</b> to create a new profile.</li><li>2. Select <b>Response Pages</b>, as well as any other management services required on the interface.</li><li>3. Click <b>OK</b> to save the interface management profile.</li><li>4. Select <b>Network &gt; Interfaces</b> and select the interface to which to attach the profile.</li><li>5. On the <b>Advanced &gt; Other Info</b> tab, select the interface management profile you just created.</li><li>6. Click <b>OK</b> to save the interface settings.</li></ol>
<p><b>Step 5</b> Test the file blocking configuration.</p>	<p>Access a client PC in the trust zone of the firewall and attempt to download an.exe file from a website in the untrust zone. Make sure the file is blocked as expected based on the action you defined in the file blocking profile:</p> <ul style="list-style-type: none"><li>• If you selected <b>alert</b> as the action, check the data filtering log to make sure you see a log entry for the request.</li><li>• If you selected <b>block</b> as the action, the File Blocking Block Page response page should display.</li><li>• If you selected the <b>continue</b> action, the File Blocking Continue Page response page should display. Click <b>Continue</b> to download the file. The following shows the default File Blocking Continue Page.</li></ul>

### File Download Blocked

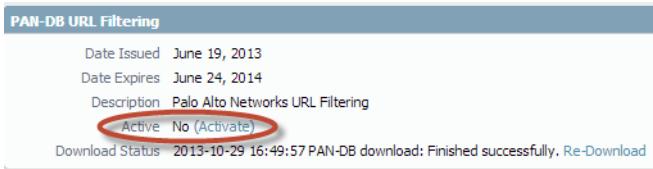
Access to the file you were trying to download has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

**File name:** Support\_services\_ds1.pdf

Please click **Continue** to download/upload the file.

## Control Access to Web Content

[URL Filtering](#) provides visibility and control over web traffic on your network. With URL filtering enabled, the firewall can categorize web traffic into one or more (from approximately 60) categories. You can then create policies that specify whether to allow, block, or log (alert) traffic based on the category to which it belongs. The following workflow shows how to enable PAN-DB for URL filtering, create security profiles, and attach them to security policies to enforce a basic URL filtering policy.

Configure URL Filtering	
Step 1 Confirm license information for URL Filtering.	<ol style="list-style-type: none"> <li>1. Obtain and install a URL Filtering license. See <a href="#">Activate Licenses and Subscriptions</a> for details.</li> <li>2. Select <b>Device &gt; Licenses</b> and verify that the URL Filtering license is valid.</li> </ol> 
Step 2 Download the seed database and activate the license.	<ol style="list-style-type: none"> <li>1. To download the seed database, click <b>Download</b> next to <b>Download Status</b> in the PAN-DB URL Filtering section of the Licenses page.</li> <li>2. Choose a region (North America, Europe, APAC, Japan) and then click <b>OK</b> to start the download.</li> <li>3. After the download completes, click <b>Activate</b>.</li> </ol> 
Step 3 Create a URL filtering profile.   Because the default URL filtering profile blocks risky and threat-prone content, clone this profile when creating a new profile in order to preserve the default settings.	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li> <li>2. Select the default profile and then click <b>Clone</b>. The new profile will be named default-1.</li> <li>3. Select the new profile and rename it.</li> </ol>

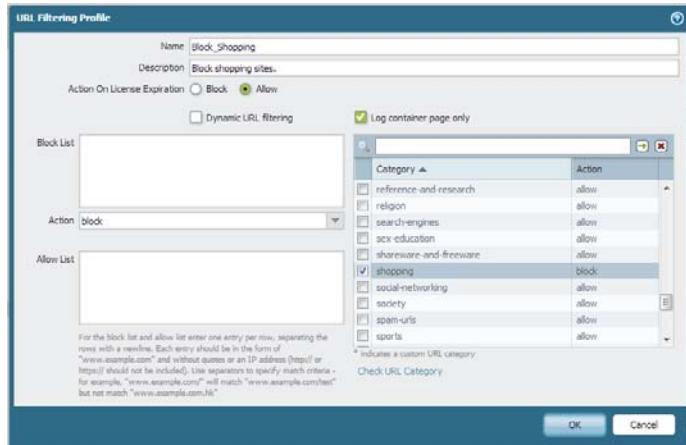
### Configure URL Filtering (Continued)

- Step 4** Define how to control access to web content.

If you are not sure what traffic you want to control, consider setting the categories (except for those blocked by default) to alert. You can then use the visibility tools on the firewall, such as the ACC and App Scope, to determine which web categories to restrict to specific groups or to block entirely. You can then go back and modify the profile to block and allow categories as desired.

You can also define specific sites to always allow or always block regardless of category and enable the safe search option to filter search results when defining the [URL Filtering](#) profile.

- For each category that you want visibility into or control over, select a value from the **Action** column as follows:
  - If you do not care about traffic to a particular category (that is you neither want to block it nor log it), select **allow**.
  - For visibility into traffic to sites in a category, select **alert**.
  - To present a response page to users attempting to access a particular category to alert them to the fact that the content they are accessing might not be work appropriate, select **continue**.
  - To prevent access to traffic that matches the associated policy, select **block** (this also generates a log entry).



- Click **OK** to save the URL filtering profile.

- Step 5** Attach the URL filtering profile to a security policy.

- Select **Policies > Security**.
- Select the desired policy to modify it and then click the **Actions** tab.
- If this is the first time you are defining a security profile, select **Profiles** from the **Profile Type** drop-down.
- In the **Profile Settings** list, select the profile you just created from the **URL Filtering** drop-down. (If you don't see drop-downs for selecting profiles, select **Profiles** from the **Profile Type** drop-down.)
- Click **OK** to save the profile.
- Commit** the configuration.

<b>Configure URL Filtering (Continued)</b>	
<b>Step 6</b> Enable Response Pages in the management profile for each interface on which you are filtering web traffic.	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b> and then select an interface profile to edit or click <b>Add</b> to create a new profile.</li> <li>Select <b>Response Pages</b>, as well as any other management services required on the interface.</li> <li>Click <b>OK</b> to save the interface management profile.</li> <li>Select <b>Network &gt; Interfaces</b> and select the interface to which to attach the profile.</li> <li>On the <b>Advanced &gt; Other Info</b> tab, select the interface management profile you just created.</li> <li>Click <b>OK</b> to save the interface settings.</li> </ol>
<b>Step 7</b> Save the configuration.	Click <b>Commit</b> .
<b>Step 8</b> Test the URL filtering configuration.	<p>Access a client PC in the trust zone of the firewall and attempt to access a site in a blocked category. Make sure URL filtering is applied based on the action you defined in the URL filtering profile:</p> <ul style="list-style-type: none"> <li>If you selected <b>alert</b> as the action, check the data filtering log to make sure you see a log entry for the request.</li> <li>If you selected the <b>continue</b> action, the URL Filtering Continue and Override Page response page should display <b>Continue</b> to the site.</li> <li>If you selected <b>block</b> as the action, the URL Filtering and Category Match Block Page response page should display as follows:</li> </ul> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>Web Page Blocked</b></p> <p>Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.</p> <p>User: 192.160.2.10 URL: amazon.com/ Category: shopping</p> </div>

## For More Information

For more detailed information on how to protect your enterprise from threats, see [Threat Prevention](#). For details on how to scan encrypted (SSH or SSL) traffic for threats, see [Decryption](#).

For information about the threats and applications that Palo Alto Networks products can identify, visit the following links:

- [Applipedia](#)—Provides details on the applications that Palo Alto Networks can identify.
- [Threat Vault](#)—Lists threats that Palo Alto Networks products can identify. You can search by Vulnerability, Spyware, or Virus. Click the Details icon next to the ID number for more information about a threat.

## Best Practices for Completing the Firewall Deployment

Now that you have integrated the firewall into your network and enabled the basic security features, you can begin configuring more advanced features. Here are some things to consider next:

- Learn about the different [Management Interfaces](#) that are available to you and how to access and use them.
- Set up [High Availability](#)—High availability (HA) is a configuration in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point to failure on your network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up the firewalls in a two-device cluster provides redundancy and allows you to ensure business continuity.
- [Configure the Master Key](#)—Every Palo Alto Networks firewall has a default master key that encrypts private keys that are used to authenticate administrators when they access management interfaces on the firewall. As a best practice to safeguard the keys, configure the master key on each firewall to be unique.
- [Manage Firewall Administrators](#)—Every Palo Alto Networks firewall and appliance is preconfigured with a default administrative account (admin) that provides full read-write access (also known as superuser access) to the device. As a best practice, create a separate administrative account for each person who needs access to the administrative or reporting functions of the firewall. This allows you to better protect the device from unauthorized configuration (or modification) and to enable logging of the actions of each individual administrator.
- Enable User Identification ([User-ID](#))—User-ID is a Palo Alto Networks next-generation firewall feature that allows you to create policies and perform reporting based on users and groups rather than individual IP addresses.
- Enable [Decryption](#)—Palo Alto Networks firewalls provide the capability to decrypt and inspect traffic for visibility, control, and granular security. Use decryption on a firewall to prevent malicious content from entering your network or sensitive content from leaving your network concealed as encrypted or tunneled traffic.
- [Enable Passive DNS Collection for Improved Threat Intelligence](#)—Enable this opt-in feature to enable the firewall to act as a passive DNS sensor and send select DNS information to Palo Alto Networks for analysis in order to improve threat intelligence and threat prevention capabilities.
- Follow the [Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions](#).





# Device Management

---

---

Administrators can configure, manage, and monitor the Palo Alto Networks firewalls using the web interface, the CLI, and the API management interface. Role-based administrative access to the management interfaces can be customized in order to delegate specific tasks or permissions to certain administrators. See the following topics for information on device management options, including how to begin using the management interfaces and how to customize administrator roles:

- ▲ [Management Interfaces](#)
- ▲ [Manage Firewall Administrators](#)
- ▲ [Reference: Web Interface Administrator Access](#)
- ▲ [Reference: Port Numbers Used by Palo Alto Networks Devices](#)
- ▲ [Reset the Firewall to Factory Default Settings](#)

# Management Interfaces

PAN-OS firewalls and Panorama provide three user interfaces: a web interface, a command line interface (CLI), and a XML-based management API. See the following topics for how to access and begin using each of the device management interfaces:

- [Use the Web Interface](#) to complete administrative tasks and generate reports from the web interface with relative ease. This graphical interface allows you to access the firewall using HTTPS and it is the best way to perform administrative tasks.
- [Use the Command Line Interface \(CLI\)](#) to type through the commands in rapid succession to complete a series of tasks. The CLI is a no-frills interface that supports two command modes and each mode has its own hierarchy of commands and statements. When you get familiar with the nesting structure and the syntax of the commands, the CLI allows quick response times and offers administrative efficiency.
- [Use the XML API](#) to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is provided as a web service that is implemented using HTTP/HTTPS requests and responses.

## Use the Web Interface

The following topics describes how to begin using the firewall web interface. For detailed information about the tabs and fields that are available in the web interface, refer to the [Web Interface Reference Guide](#).

- ▲ [Launch the Web Interface](#)
- ▲ [Navigate the Web Interface](#)
- ▲ [Commit or Validate Changes](#)
- ▲ [Use Global Find](#)
- ▲ [Use Configuration Pages](#)
- ▲ [Identify Required Fields](#)
- ▲ [Lock Transactions](#)

### Launch the Web Interface

The following web browsers are supported for access to the web interface for PAN-OS firewalls and Panorama:

- Internet Explorer 7+
- Firefox 3.6+
- Safari 5+
- Chrome 11+

Launch an Internet browser and enter the firewall's IP address. Enter your user credentials. If logging in to the firewall for the first time, type the default **admin** into both the **Name** and **Password** fields.

To view information on how to use a specific page and an explanation of the fields and options on the page, click the **Help** icon  in the upper right area of the page to open the online help system. In addition to displaying context-sensitive help for a page, clicking the **Help** icon displays a help navigation pane with options to browse and search all help content.

### Navigate the Web Interface

The following conventions apply when using the web interface.

- To display the menu items for a general functional category, click the tab, such as **Objects** or **Device**, near the top of the browser window.



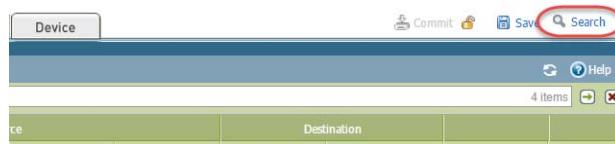
- Click an item on the side menu to display a panel.



- To display submenu items, click the icon to the left of an item. To hide submenu items, click the icon to the left of the item.



- To search the candidate configuration on a firewall or on Panorama for a particular string, click the **Search** icon to start a [Use Global Find](#) search.



- On most configuration pages, you can click **Add** to create a new item.



- To delete one or more items, select their check boxes and click **Delete**. In most cases, the system prompts you to confirm by clicking **OK** or to cancel the deletion by clicking **Cancel**.



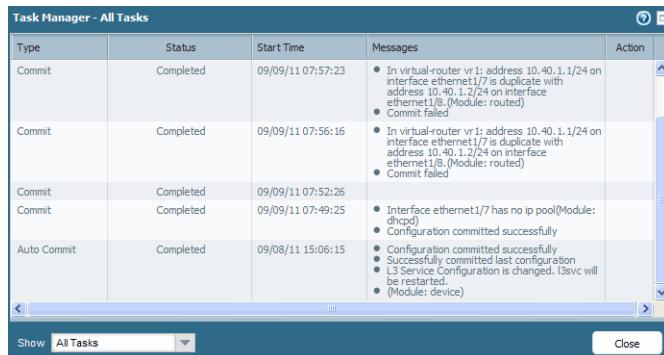
- On some configuration pages, you can select the check box for an item and click **Clone** to create a new item with the same information as the selected item.



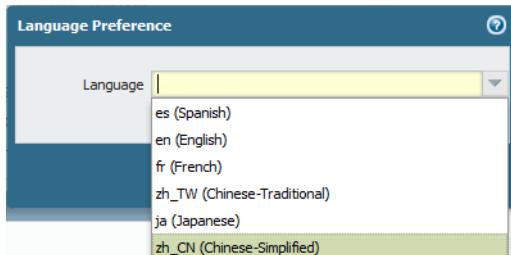
- To modify an item, click its underlined link.

Name	Location	Protocol
service-http	Predefined	TCP
<a href="#"><u>service-https</u></a>	Predefined	TCP

- To view the current list of tasks, click the **Tasks** icon in the lower right corner of the page. The Task Manager window opens to show the list of tasks, along with status, start times, associated messages, and actions. Use the **Show** drop-down to filter the list of tasks.



- The web interface language is controlled by the current language of the computer that is managing the device if a specific language preference has not been defined. For example, if the computer you use to manage the firewall has a locale of Spanish, when you log in to the firewall, the web interface will be in Spanish.
- To specify a language that will always be used for a given account regardless of the locale of the computer, click the **Language** icon in the lower right corner of the page and the Language Preference window opens. Click the drop-down to select the desired language and then click **OK** to save your change.



- On pages that list information you can modify (for example, the **Setup** page on the **Devices** tab), click the icon in the upper right corner of a section to edit the settings.



- After you configure settings, you must click **OK** or **Save** to store the changes. When you click **OK**, the current *candidate* configuration is updated.

## Commit or Validate Changes

Click **Commit** at the top of the web interface to open the Commit dialog box, which displays the following options. Certain options only display if you click **Advanced**.



If dependencies between the configuration changes you included and excluded cause a validation error, perform the commit with all the changes included. For example, if your changes introduce a new Log Forwarding profile (an object) that references a new Syslog server profile (a device setting), the commit must include both policy and object configurations and device and network configurations.

- **Include Device and Network configuration**—Include the device and network configuration changes in the commit operation.
- **Include Shared Object configuration**—(Multi-virtual system firewalls only) Include the shared object configuration changes in the commit operation.
- **Include Policy and Object configuration**—(Non-multi-virtual system firewalls only) Include the policy and object configuration changes in the commit operation.
- **Include Virtual System configuration**—Include all virtual systems or choose **Select one or more virtual systems**.
- **Preview Changes**—Click this button to display a two-pane window that shows proposed changes in the candidate configuration compared to the current running configuration. You can choose the number of lines of context to display, or show all lines. Changes are color coded based on items that you and other administrators added (green), modified (yellow), or deleted (red) since the last commit.



Because the preview results display in a new window, your browser must allow pop-ups. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-ups.

- **Validate Changes**—Click this button to perform a syntactic validation (of configuration syntax) and semantic validation (whether the configuration is complete and makes sense) of a firewall or Panorama candidate configuration before committing it. The results display all of the errors and warnings of a full commit or virtual system commit, including rule shadowing and application dependency warnings. Possible errors could be an invalid route destination or a missing account and password that are required to query a server. Such validation significantly reduces failures at commit time.

## Use Global Find

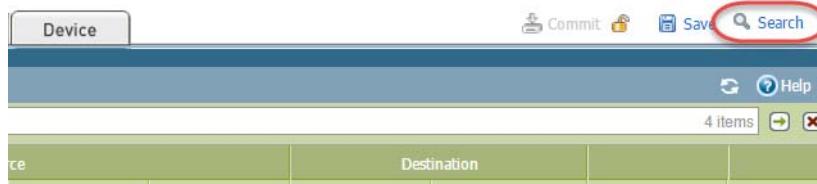
Global Find enables you to search the candidate configuration on a firewall or on Panorama for a particular string, such as an IP address, object name, policy rule name, threat ID, or application name. The search results are grouped by category and provide links to the configuration location in the web interface, so that you can easily find all of the places where the string is referenced. The search results also help you identify other objects that depend on or make reference to the search term or string. For example, when deprecating a security profile enter the profile name in Global Find to locate all instances of the profile and then click each instance to navigate to the configuration page and make the necessary change. After all references are removed, you can then delete the profile. You can do this for any configuration item that has dependencies.



Global Find will not search dynamic content (such as logs, address ranges, or allocated DHCP addresses). In the case of DHCP, you can search on a DHCP server attribute, such as the DNS entry, but you cannot search for individual addresses allocated to users. Global Find also does not search for individual user or group names identified by User-ID unless the user/group is defined in a policy. In general, you can only search content that the firewall writes to the configuration.

### Use Global Find

- Launch Global Find by clicking the **Search** icon located on the upper right of the web interface.



- To access the Global Find from within a configuration area, click the drop-down next to an item and click **Global Find** as follows:

Name	Tags	Type	Zone	Address	User
1 GF-Test	none	universal	I3-vlan-trust	Stu Local IP	any
2 rule1		universal	I3-vlan-trust	any	any
3 intrazone-default		intrazone	any	any	any
4 interzone-default		interzone	any	any	any

## Use Global Find (Continued)

For example, click **Global Find** on a zone named **l3-vlan-trust** to search the candidate configuration for each location where the zone is referenced. The following screen capture shows the search results for the zone **l3-vlan-trust**:

The screenshot shows the 'Policies' tab selected in the top navigation bar. A search bar at the top right contains the query "l3-vlan-trust". Below it, a table lists search results. A red callout box points to the search bar with the text: "Click here and select Global Find to perform a search on l3-vlan-trust..". Another red callout box points to the table with the text: "Search results appear here. Hover over an item to view details or click an item to navigate to the configuration page for the item." The table has columns for Name, Location Type, and Location.

Name	Location Type	Location
Security Rule (2)	VSYS	vsys1
rule1	VSYS	vsys1
GF-Test	VSYS	vsys1
NAT Rule (1)	VSYS	vsys1
access-corp	VSYS	vsys1
Decryption Rule (1)	VSYS	vsys1
Decrypt_All_Traffic	VSYS	vsys1
Zone (1)	VSYS	vsys1
<b>l3-vlan-trust</b>	VSYS	vsys1

When using global find, keep the following tips in mind:

- If you initiate a search on a firewall that has multiple virtual systems enabled or if custom [Administrative Roles](#) are defined, Global Find will only return results for areas of the firewall in which the administrator has permissions. The same applies to Panorama device groups.
- Spaces in search terms are handled as AND operations. For example, if you search on **corp policy**, the search results include instances where **corp** and **policy** exist in the configuration.
- To find an exact phrase, enclose the phrase in quotation marks.
- To rerun a previous search, click the Search icon located on the upper right of the web interface and a list of the last 20 searches will be displayed. Click an item in the list to rerun that search. The search history list is unique to each administrator account.

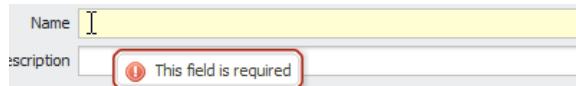
## Use Configuration Pages

The tables on configuration pages include sorting and column chooser options. Click a column header to sort on that column, and click again to change the sort order. Click the arrow to the right of any column and select check boxes to choose the columns to display.

The screenshot shows a table with columns: Direction, Default Action, and Comment. A context menu is open over the first row, specifically over the 'Direction' column header. The menu includes options for 'Sort Ascending' and 'Sort Descending'. A sub-menu for 'Columns' is also open, listing 'Location', 'Severity', 'Direction', 'Default Action', and 'Comment', each with a checked checkbox. A cursor is hovering over the 'Columns' option in the sub-menu.

## Identify Required Fields

Required fields are shown with a light yellow background. A message indicating that the field is required appears when you hover over or click in the field entry area.



## Lock Transactions

The web interface provides support for multiple administrators by allowing an administrator to lock a current set of transactions, thereby preventing configuration changes or commit operations by another administrator until the lock is removed. The following types of locks are supported:

- **Config lock**—Blocks other administrators from making changes to the configuration. This type of lock can be set globally or for a virtual system. It can be removed only by the administrator who set it or by a superuser on the system.
- **Commit Lock**—Blocks other administrators from committing changes until all of the locks have been released. This type of lock prevents collisions that can occur when two administrators are making changes at the same time and the first administrator finishes and commits changes before the second administrator has finished. The lock is released when the current changes are committed by the administrator who applied the lock, or it can be released manually.

Any administrator can open the lock window to view the current transactions that are locked, along with a time stamp for each.

To lock a transaction, click the unlocked icon on the top bar to open the Locks dialog box. Click **Take a Lock**, select the scope of the lock from the drop-down, and click **OK**. Add additional locks as needed, and then click **Close** to close the Lock dialog box.

The transaction is locked, and the icon on the top bar changes to a locked icon that shows the number of locked items in parentheses.

To unlock a transaction, click the locked icon on the top bar to open the Locks window. Click the icon for the lock that you want to remove, and click **Yes** to confirm. Click **Close** to close the Lock dialog box.

You can arrange to automatically acquire a commit lock by selecting the **Automatically acquire commit lock** check box in the Management area of the **Device Setup** page.

## Use the Command Line Interface (CLI)

The [PAN-OS CLI](#) allows you to access Firewall and Panorama devices, view status and configuration information, and modify configurations. Access to the PAN-OS CLI is provided through SSH, Telnet, or direct console access.

The following topics describe how to access and begin using the PAN-OS CLI:

- ▲ [Access the PAN-OS CLI](#)
- ▲ [Operational and Configuration Modes](#)

### Access the PAN-OS CLI

Use a terminal emulator, such as PuTTY, to connect to the CLI in one of the following ways:

- **SSH Connection**—If you [Perform Initial Configuration](#), you can establish a CLI connection over the network using a secure shell (SSH) connection.
- **Serial Connection**—If you have not yet completed initial configuration or if you chose not to enable SSH on the firewall, you can establish a direct serial connection from a serial interface on your management computer to the Console port on the firewall.

#### Access the PAN-OS CLI

**Step 1** Launch the terminal emulation software and select the type of connection (Serial or SSH).

- To establish an SSH connection, enter the hostname or IP address of the firewall or Panorama you want to connect to and set the port to 22.
- To establish a Serial connection, connect a serial interface on management computer to the Console port on the firewall. Configure the Serial connection settings in the terminal emulation software as follows:
  - Data rate: 9600
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: none

**Step 2** When prompted to log in, enter your administrative username.

The default superuser username is `admin`. To set up CLI access for other administrative users, [Configure an Administrative Account](#).

**Step 3** Enter the administrative password.

The default superuser password is `admin`. However, for security reasons you should immediately [change the admin password](#).

The CLI opens in Operational mode, and the CLI prompt is displayed:

```
username@hostname>
```

You can tell you are in Operational mode because the command prompt ends with a `>`.

## Operational and Configuration Modes

When you log in, the PAN-OS CLI opens in operational mode. You can move between operational and configuration modes at any time. Use operational mode to view the state of the system, navigate the PAN-OS CLI, and enter configuration mode. Use configuration mode to view and modify the configuration hierarchy.

- To enter configuration mode from operational mode, use the `configure` command:

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

- To leave configuration mode and return to operational mode, use the `quit` or `exit` command:

```
username@hostname# quit
Exiting configuration mode
username@hostname>
```

- To enter an operational mode command while in configuration mode, use the `run` command, for example:

```
username@hostname# run ping host 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data
...
username@hostname#
```

- To direct an Operational mode command to a particular VSYS, specify the target VSYS with the following command:

```
username@hostname# set system setting target-vsys <vsys_name>
```

## Use the XML API

Palo Alto Networks XML API uses standard HTTP requests to send and receive data, allowing access to several types of data on the device so the data can be easily integrated with and used in other systems. Use the XML-based Management API to view a firewall or Panorama's configuration, extract report data in XML format, and execute operational commands. API calls can be made directly from command line utilities such as curl or wget, or using any scripting or application framework that supports RESTful services. When using the API with command line tools, both HTTP GET and POST methods are supported.

You must generate an API key in order to use the XML API. The API key authenticates the user to the firewall, application, or Panorama. After you have generated an API key, you can use the key to perform device configuration and operational tasks, retrieve reports and logs, and import and export files. See [Generate an API Key](#) for steps to generate an API key.

The following table shows the URL structure for API requests:

PAN-OS Version	XML API URL Structure
Prior to PAN-OS 4.1.0	http(s)://hostname/esp/restapi.esp?request-parameters-values
PAN-OS 4.1.0 and later	http(s)://hostname/api/?request-parameters-values

URL structure item definitions:

- **hostname**—Device's IP address or Domain name.
- **request-parameters-values**—A series of multiple 'parameter=value' pairs separated by the ampersand character (&). These values can either be keywords or data-values in standard or XML format (response data is always in XML format).

There are APIs for PAN-OS, User-ID, and WildFire products. For more information on how to use the API interface, refer to the [PAN-OS XML API Usage Guide](#).

## Generate an API Key

In order to use the API to manage a firewall or application, an API key is required to authenticate all API calls. Admin account credentials are used to generate API keys.



As a best practice, create a separate admin account for XML-based administration.

### Generate an API key

Step 1 Create an administrator account.	<ol style="list-style-type: none"> <li>1. In the web interface, on the <b>Device &gt; Administrators</b> tab, click <b>Add</b>.</li> <li>2. Enter a login <b>Name</b> for the admin.</li> <li>3. Enter and confirm a <b>Password</b> for the admin.</li> <li>4. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
---	---

### Generate an API key (Continued)

<p><b>Step 2</b> Request an API key.</p> <p>For PAN-OS 4.1.0 and later releases, generating an API key using the same administrator account credentials returns unique API keys every time, and all of the keys are valid.</p> <p>You can choose to revoke and then change an API key associated with an administrator account by changing the password associated with the administrator account. Any API keys that were generated using the previous credentials would no longer be valid.</p>	<p>Replace the hostname, username and password parameters in the following URL with the appropriate values from your administrator account credentials:</p> <pre>http(s)://hostname/api/?type=keygen&amp;user=username&amp;password=password</pre> <p>The API key is displayed in an XML block. For example:</p> <pre>&lt;response status="success"&gt; &lt;result&gt; &lt;key&gt;0RgWc42Oi0vDx2WRUIUM6A&lt;/key&gt; &lt;/result&gt; &lt;/response&gt;</pre>
<p><b>Step 3</b> (Optional) Revoke or change an API key.</p> <p>On the <b>Device &gt; Administrators</b> tab, open the administrator account associated with the API key.</p> <p>Enter and confirm a new <b>Password</b> for the administrator account.</p> <p>Click <b>OK</b> and <b>Commit</b>. Any API keys associated with the admin account prior to the password change are revoked upon Commit.</p> <p>(Optional) Use the updated administrator account credentials to generate a new API key. See <a href="#">Step 2</a>.</p>	<ol style="list-style-type: none"> <li>1. On the <b>Device &gt; Administrators</b> tab, open the administrator account associated with the API key.</li> <li>2. Enter and confirm a new <b>Password</b> for the administrator account.</li> <li>3. Click <b>OK</b> and <b>Commit</b>. Any API keys associated with the admin account prior to the password change are revoked upon Commit.</li> <li>4. (Optional) Use the updated administrator account credentials to generate a new API key. See <a href="#">Step 2</a>.</li> </ol>

#### Example work flow using an API key:

Request an API key by entering the URL with the appropriate values in a web browser:

```
https://10.xx.10.50/esp/restapi.esp?type=keygen&user=admin&password=admin
```

Entering the URL displays an XML block that contains the API key:

```
<response status="success">
<result>
<key>0RgWc42Oi0vDx2WRUIUM6A</key>
</result>
</response>
```

Continue to use the API key to create API requests. For example, to generate a report:

```
https://10.xx.10.50/esp/restapi.esp?type=report&reporttype=dynamic&reportname=top-app-summary&period=last-hour&topn=5&key=0RgWc42Oi0vDx2WRUIUM6A=
```

# Manage Firewall Administrators

Administrative accounts specify roles and authentication methods for the administrators of Palo Alto Networks firewalls. Every Palo Alto Networks firewall has a predefined default administrative account (admin) that provides full read-write access (also known as superuser access) to the firewall.



As a best practice, create a separate administrative account for each person who needs access to the administrative or reporting functions of the firewall. This enables you to better protect the firewall from unauthorized configuration and enables logging of the actions of individual administrators.

- ▲ [Administrative Roles](#)
- ▲ [Administrative Authentication](#)
- ▲ [Configure Administrative Accounts and Authentication](#)

## Administrative Roles

A *role* defines the type of access that an administrator has to the firewall.

- ▲ [Administrative Role Types](#)
- ▲ [Configure an Admin Role Profile](#)

### Administrative Role Types

The role types are:

- **Dynamic Roles**—These are built-in roles that provide access to the firewall. When new features are added, the firewall automatically updates the definitions of dynamic roles; you never need to manually update them. The following table lists the access privileges associated with dynamic roles.

Dynamic Role	Privileges
Superuser	Full access to the firewall, including defining new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges.
Superuser (read-only)	Read-only access to the firewall.
Virtual system administrator	Full access to a selected virtual system (vsys) on the firewall.
Virtual system administrator (read-only)	Read-only access to a selected vsys on the firewall.
Device administrator	Full access to all firewall settings except for defining new accounts or virtual systems.
Device administrator (read-only)	Read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged in account is visible).

- **Admin Role Profiles**—Custom roles you can configure for more granular access control over the functional areas of the web interface, CLI, and XML API. For example, you can create an Admin Role profile for your operations staff that provides access to the firewall and network configuration areas of the web interface and a separate profile for your security administrators that provides access to security policy definitions, logs, and reports. On a multi-vsys firewall, you can select whether the role defines access for all virtual systems or for a specific vsys. When new features are added to the product, you must update the roles with corresponding access privileges: the firewall does not automatically add new features to custom role definitions. For details on the privileges you can configure for custom administrator roles, see [Reference: Web Interface Administrator Access](#).

## Configure an Admin Role Profile

Admin Role profiles enable you to define granular administrative access privileges to ensure protection for sensitive company information and privacy for end users. As a best practice, create Admin Role profiles that allow administrators to access only the areas of the management interfaces that they require to perform their jobs.

### Configure an Admin Role Profile

- Step 1 Select **Device > Admin Roles** and click **Add**.
- Step 2 Enter a **Name** to identify the role.
- Step 3 For the scope of the **Role**, select **Device** or **Virtual System**.
- Step 4 In the **Web UI** and **XML API** tabs, click the icon for each functional area to toggle it to the desired setting: Enable, Read Only, or Disable. For details on the **Web UI** options, see [Web Interface Access Privileges](#).
- Step 5 Select the **Command Line** tab and select a CLI access option. The **Role** scope controls the available options:
  - **Device** role—**superuser**, **superreader**, **deviceadmin**, **devicereader**, or **None**
  - **Virtual System** role—**vsysadmin**, **vsysreader**, or **None**
- Step 6 Click **OK** to save the profile.
- Step 7 Assign the role to an administrator. See [Configure an Administrative Account](#).

## Administrative Authentication

You can configure the following types of administrator authentication:

Account Type	Authentication Method	Description
Local	Local database	Both the administrator account credentials and the authentication mechanisms are local to the firewall. You can further secure a local administrator account by creating a password profile that defines a validity period for passwords and by setting firewall-wide password complexity settings. If your network supports <a href="#">Kerberos single sign-on (SSO)</a> , you can configure local authentication as a fallback in case SSO fails. For details, see <a href="#">Configure Kerberos SSO and External or Local Authentication for Administrators</a> .
Local	SSL-based	The administrator accounts are local to the firewall, but authentication is based on SSH certificates (for CLI access) or client certificates (for web interface access). For details, see <a href="#">Configure SSH Key-Based Administrator Authentication to the CLI</a> and <a href="#">Configure Certificate-Based Administrator Authentication to the Web Interface</a> .
Local	External service	The administrator accounts are local to the firewall, but <a href="#">external services</a> (LDAP, Kerberos, TACACS+, or RADIUS) handle the authentication functions. If your network supports <a href="#">Kerberos single sign-on (SSO)</a> , you can configure external authentication as a fallback in case SSO fails. For details, see <a href="#">Configure Kerberos SSO and External or Local Authentication for Administrators</a> .
External	External service	An external RADIUS server handles account management and authentication. You must define Vendor-Specific Attributes (VSAs) on your RADIUS server that map to the administrator role, access domain, user group (if applicable), and virtual system (if applicable). For details, see <a href="#">Configure RADIUS Vendor-Specific Attributes for Administrator Authentication</a> .

## Configure Administrative Accounts and Authentication

- ▲ Configure an Administrative Account
- ▲ Configure Kerberos SSO and External or Local Authentication for Administrators
- ▲ Configure Certificate-Based Administrator Authentication to the Web Interface
- ▲ Configure SSH Key-Based Administrator Authentication to the CLI
- ▲ Configure RADIUS Vendor-Specific Attributes for Administrator Authentication

## Configure an Administrative Account

Administrative accounts specify **roles** and **authentication methods** for the administrators of Palo Alto Networks firewalls.

### Configure an Administrative Account

**Step 1** Select **Device > Administrators** and click **Add**.

**Step 2** Enter a user **Name**.

**Step 3** Select an **Authentication Profile** or sequence if you **configured either** for the user. The default option **None** specifies that the firewall will locally manage and authenticate the account without a local database; you must enter and confirm the **Password**.

**Step 4** Select the **Administrator Type**. If you **configured a custom role** for the user, select **Role Based** and select the Admin Role **Profile**. Otherwise, select **Dynamic** (the default) and select a dynamic role. If the dynamic role is **virtual system administrator**, add one or more virtual systems that the virtual system administrator is allowed to manage.

**Step 5** Click **OK** and **Commit**.

## Configure Kerberos SSO and External or Local Authentication for Administrators

You can configure the firewall to first try [Kerberos single sign-on \(SSO\)](#) authentication and, if that fails, fall back to [External service](#) or [Local database](#) authentication.

<b>Configure Kerberos SSO and External or Local Authentication for Administrators</b>		
<b>Step 1</b>	Configure a Kerberos keytab for the firewall.  Required for Kerberos SSO authentication.	<a href="#">Create a Kerberos keytab.</a> A keytab is a file that contains Kerberos account information (principal name and hashed password) for the firewall.
<b>Step 2</b>	Configure an Admin Role profile.  Required if you are assigning a custom role to the administrator.	<a href="#">Configure an Admin Role Profile.</a>
<b>Step 3</b>	Create the local database.  Required for local database authentication.	<ol style="list-style-type: none"> <li>1. Add the user account:             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Local User Database &gt; Users</b> and click <b>Add</b>.</li> <li>b. Enter a user <b>Name</b> for the administrator.</li> <li>c. Enter a <b>Password</b> and <b>Confirm Password</b>.</li> <li>d. Be sure the <b>Enable</b> check box is selected and click <b>OK</b>.</li> </ol> </li> <li>2. (Optional) If the user is a member of a group, assign the user to that group:             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Local User Database &gt; User Groups</b> and click the Name of an existing group to edit it, or click <b>Add</b> to create a new group.</li> <li>b. Enter a <b>Name</b> to identify the group.</li> <li>c. Click <b>Add</b>, select the user you just created, and click <b>OK</b>.</li> </ol> </li> </ol>
<b>Step 4</b>	Configure access to an external authentication service.  Required for external authentication.	Configure a server profile for the authentication service type: <ul style="list-style-type: none"> <li>• <a href="#">Configure a RADIUS Server Profile</a>.</li> <li>• <a href="#">Configure a TACACS+ Server Profile</a>.</li> <li>• <a href="#">Configure an LDAP Server Profile</a>.</li> <li>• <a href="#">Configure a Kerberos Server Profile</a>.</li> </ul>
<b>Step 5</b>	Configure an authentication profile.   If your users are in multiple Kerberos realms, create an authentication profile for each realm and assign all the profiles to an authentication sequence. You can then assign the same authentication sequence to all user accounts ( <a href="#">Step 6</a> ).	<a href="#">Configure an Authentication Profile and Sequence.</a>

**Configure Kerberos SSO and External or Local Authentication for Administrators (Continued)**

**Step 6** Configure an administrator account.

[Configure an Administrative Account.](#)

- For local database authentication, specify the **Name** of the user you defined in [Step 3](#).
- Assign the **Authentication Profile** or sequence and the Admin Role **Profile** that you just created.

## Configure Certificate-Based Administrator Authentication to the Web Interface

As a more secure alternative to password-based authentication to the web interface of a Palo Alto Networks firewall, you can configure certificate-based authentication for administrator accounts that are local to the firewall. Certificate-based authentication involves the exchange and verification of a digital signature instead of a password.



Configuring certificate-based authentication for any administrator disables the username/password logins for all administrators on the firewall; administrators thereafter require the certificate to log in.

### Configure Certificate-Based Administrator Authentication to the Web Interface

<p><b>Step 1</b> Generate a certificate authority (CA) certificate on the firewall.  You will use this CA certificate to sign the client certificate of each administrator.</p>	<p><a href="#">Create a Self-Signed Root CA Certificate.</a>  Alternatively, you can <a href="#">Import a Certificate and Private Key</a> from your enterprise CA.</p>
<p><b>Step 2</b> Configure a certificate profile for securing access to the web interface.</p>	<p><a href="#">Configure a Certificate Profile.</a></p> <ul style="list-style-type: none"><li>Set the <b>Username Field</b> to <b>Subject</b>.</li><li>Select <b>Add</b> in the CA Certificates section and select the <b>CA Certificate</b> you just created or imported.</li></ul>
<p><b>Step 3</b> Configure the firewall to use the certificate profile for authenticating administrators.</p>	<ol style="list-style-type: none"><li>Select <b>Device &gt; Setup &gt; Management</b> and edit the Authentication Settings.</li><li>Select the <b>Certificate Profile</b> you just created and click <b>OK</b>.</li></ol>
<p><b>Step 4</b> Configure the administrator accounts to use client certificate authentication.</p>	<p>For each administrator who will access the firewall web interface, <a href="#">Configure an Administrative Account</a>. Select the <b>Use only client certificate authentication</b> check box.  If you have already deployed client certificates that your enterprise CA generated, skip to <b>Step 8</b>. Otherwise, go to <b>Step 5</b>.</p>
<p><b>Step 5</b> Generate a client certificate for each administrator.</p>	<p><a href="#">Generate a Certificate on the Device</a>. In the <b>Signed By</b> drop-down, select the CA certificate you created.</p>
<p><b>Step 6</b> Export the client certificate.</p>	<ol style="list-style-type: none"><li><a href="#">Export a Certificate and Private Key</a>.</li><li><b>Commit</b> your changes. The firewall restarts and terminates your login session. Thereafter, administrators can access the web interface only from client systems that have the client certificate you generated.</li></ol>
<p><b>Step 7</b> Import the client certificate into the client system of each administrator who will access the web interface.</p>	<p>Refer to your web browser documentation.</p>

### Configure Certificate-Based Administrator Authentication to the Web Interface (Continued)

<p><b>Step 8</b> Verify that administrators can access the web interface.</p>	<ol style="list-style-type: none"> <li>1. Open the firewall IP address in a browser on the computer that has the client certificate.</li> <li>2. When prompted, select the certificate you imported and click <b>OK</b>. The browser displays a certificate warning.</li> <li>3. Add the certificate to the browser exception list.</li> <li>4. Click <b>Login</b>. The web interface should appear without prompting you for a username or password.</li> </ol>
---	--

## Configure SSH Key-Based Administrator Authentication to the CLI

For administrators who use Secure Shell (SSH) to access the CLI of a Palo Alto Networks firewall, SSH keys provide a more secure authentication method than passwords. SSH keys almost eliminate the risk of brute-force attacks, provide the option for two-factor authentication (private key and passphrase), and don't send passwords over the network. SSH keys also enable automated scripts to access the CLI.

### Configure SSH Key-Based Administrator Authentication to the CLI

<p><b>Step 1</b> Use an SSH key generation tool to create an asymmetric keypair on the client system of the administrator.</p> <p>The supported key formats are IETF SECSH and Open SSH. The supported algorithms are DSA (1,024 bits) and RSA (768-4,096 bits).</p>	<p>For the commands to generate the keypair, refer to your SSH client documentation.</p> <p>The public key and private key are separate files. Save both to a location that the firewall can access. For added security, enter a passphrase to encrypt the private key. The firewall prompts the administrator for this passphrase during login.</p>
<p><b>Step 2</b> Configure the administrator account to use public key authentication.</p>	<ol style="list-style-type: none"> <li>1. <a href="#">Configure an Administrative Account</a>.           <ul style="list-style-type: none"> <li>Configure the authentication method to use as a fallback if SSH key authentication fails. If you configured an <b>Authentication Profile</b> for the administrator, select it in the drop-down. If you select <b>None</b>, you must enter a <b>Password</b> and <b>Confirm Password</b>.</li> <li>Select the <b>Use Public Key Authentication (SSH)</b> check box, click <b>Import Key</b>, <b>Browse</b> to the public key you just generated, and click <b>OK</b>.</li> </ul> </li> <li>2. <b>Commit</b> your changes.</li> </ol>
<p><b>Step 3</b> Configure the SSH client to use the private key to authenticate to the firewall.</p>	<p>Perform this task on the client system of the administrator. For the steps, refer to your SSH client documentation.</p>

**Configure SSH Key-Based Administrator Authentication to the CLI (Continued)**

<b>Step 4</b> Verify that the administrator can access the firewall CLI using SSH key authentication.	<ol style="list-style-type: none"><li>1. Use a browser on the client system of the administrator to go to the firewall IP address.</li><li>2. Log in to the firewall CLI as the administrator. After entering a username, you will see the following output (the key value is an example): <pre>Authenticating with public key "dsa-key-20130415"</pre></li><li>3. If prompted, enter the passphrase you defined when creating the keys.</li></ol>
---	--

## Configure RADIUS Vendor-Specific Attributes for Administrator Authentication

The following procedure provides an overview of the tasks required to use RADIUS Vendor-Specific Attributes (VSAs) for administrator authentication to Palo Alto Networks firewalls. For detailed instructions, refer to the following Knowledge Base articles:

- For Windows 2003 Server, Windows 2008 (and later), and Cisco ACS 4.0—[RADIUS Vendor-Specific Attributes \(VSAs\)](#)
- For Cisco ACS 5.2—[Configuring Cisco ACS 5.2 for use with Palo Alto VSA](#)

Before starting this procedure, you must:

- Create the administrative accounts in the directory service that your network uses (for example, Active Directory).
- Set up a RADIUS server that can communicate with that directory service.

Use RADIUS Vendor-Specific Attributes for Account Authentication	
Step 1 Configure the firewall.	<ol style="list-style-type: none"><li>1. <a href="#">Configure an Admin Role Profile</a> if the administrator will use a custom role.</li><li>2. Configure an access domain if the firewall has more than one virtual system (vsys):<ol style="list-style-type: none"><li>a. Select <b>Device &gt; Access Domain</b>, <b>Add</b> and access domain and enter a <b>Name</b> to identify it.</li><li>b. <b>Add</b> each vsys that the administrator will access, and then click <b>OK</b>.</li></ol></li><li>3. <a href="#">Configure a RADIUS Server Profile</a>.</li><li>4. <a href="#">Configure an authentication profile</a>. Set the authentication <b>Type</b> to <b>RADIUS</b> and assign the RADIUS <b>Server Profile</b>.</li><li>5. Configure the firewall to use the authentication profile for administrator access—Select <b>Device &gt; Setup &gt; Management</b>, edit the Authentication Settings, and select the <b>Authentication Profile</b>.</li><li>6. Click <b>OK</b> and <b>Commit</b>.</li></ol>
Step 2 Configure the RADIUS server.	<ol style="list-style-type: none"><li>1. Add the firewall IP address or hostname as the RADIUS client.</li><li>2. Define the VSAs for administrator authentication. You must specify the vendor code (25461 for Palo Alto Networks firewalls) and the VSA name, number, and value: see <a href="#">RADIUS Vendor-Specific Attributes for Palo Alto Networks Devices</a>.</li></ol>

# Reference: Web Interface Administrator Access

You can configure privileges for an entire device or for one or more virtual systems (on platforms that support multiple virtual systems). Within that **Device** or **Virtual System** designation, you can configure privileges for custom administrator roles, which are more granular than the fixed privileges associated with a dynamic administrator role.

Configuring privileges at a granular level ensures that lower level administrators cannot access certain information. You can create custom roles for firewall administrators (see [Configure an Administrative Account](#)), Panorama administrators, or Device Group and Template administrators (refer to the [Panorama Administrator's Guide](#)). You apply the admin role to a custom role-based administrator account where you can assign one or more virtual systems. The following topics describe the privileges you can configure for custom administrator roles.

- ▲ [Web Interface Access Privileges](#)
- ▲ [Panorama Web Interface Access](#)

## Web Interface Access Privileges

If you want to prevent a role-based administrator from accessing specific tabs on the web interface, you can disable the tab and the administrator will not even see it when logging in using the associated role-based administrative account. For example, you could create an Admin Role Profile for your operations staff that provides access to the **Device** and **Network** tabs only and a separate profile for your security administrators that provides access to the **Object**, **Policy**, and **Monitor** tabs.

An admin role can apply at the **Device** level or **Virtual System** level; the choice is made in the Admin Role Profile by clicking the **Device** or **Virtual System** radio button. If the **Virtual System** button is selected, the admin assigned this profile is restricted to the virtual system(s) he or she is assigned to. Furthermore, only the **Device > Setup > Services > Virtual Systems** tab is available to that admin, not the **Global** tab.

The following table describes the tab-level access privileges you can assign to the admin role profile at the **Device** level. It also provides cross-references to additional tables that detail granular privileges within a tab.

You can also configure an admin role profile to:

- [Define User Privacy Settings in the Admin Role Profile](#)
- [Restrict Admin Access to Commit Functions](#)
- [Restrict Admin Access to Validate Functions](#)
- [Provide Granular Access to Global Settings](#)

Access Level	Description	Enable	Read Only	Disable
Dashboard	Controls access to the <b>Dashboard</b> tab. If you disable this privilege, the administrator will not see the tab and will not have access to any of the Dashboard widgets.	Yes	No	Yes

Access Level	Description	Enable	Read Only	Disable
ACC	Controls access to the Application Command Center (ACC). If you disable this privilege, the <b>ACC</b> tab will not display in the web interface. Keep in mind that if you want to protect the privacy of your users while still providing access to the ACC, you can disable the <b>Privacy &gt; Show Full IP Addresses</b> option and/or the <b>Show User Names In Logs And Reports</b> option.	Yes	No	Yes
Monitor	Controls access to the <b>Monitor</b> tab. If you disable this privilege, the administrator will not see the <b>Monitor</b> tab and will not have access to any of the logs, packet captures, session information, reports or to App Scope. For more granular control over what monitoring information the admin can see, leave the Monitor option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Monitor Tab</a> .	Yes	No	Yes
Policies	Controls access to the <b>Policies</b> tab. If you disable this privilege, the administrator will not see the <b>Policies</b> tab and will not have access to any policy information. For more granular control over what policy information the admin can see, for example to enable access to a specific type of policy or to enable read-only access to policy information, leave the <b>Policies</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Policy Tab</a> .	Yes	No	Yes
Objects	Controls access to the <b>Objects</b> tab. If you disable this privilege, the administrator will not see the <b>Objects</b> tab and will not have access to any objects, security profiles, log forwarding profiles, decryption profiles, or schedules. For more granular control over what objects the admin can see, leave the <b>Objects</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Objects Tab</a> .	Yes	No	Yes
Network	Controls access to the <b>Network</b> tab. If you disable this privilege, the administrator will not see the <b>Network</b> tab and will not have access to any interface, zone, VLAN, virtual wire, virtual router, IPsec tunnel, DHCP, DNS Proxy, GlobalProtect, or QoS configuration information or to the network profiles. For more granular control over what objects the admin can see, leave the <b>Network</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Network Tab</a> .	Yes	No	Yes

Access Level	Description	Enable	Read Only	Disable
Device	<p>Controls access to the <b>Device</b> tab. If you disable this privilege, the administrator will not see the <b>Device</b> tab and will not have access to any device-wide configuration information, such as User-ID, High Availability, server profile or certificate configuration information. For more granular control over what objects the admin can see, leave the <b>Objects</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Device Tab</a>.</p>  You cannot enable access to the <b>Admin Roles</b> or <b>Administrators</b> nodes for a role-based administrator even if you enable full access to the <b>Device</b> tab.	Yes	No	Yes

## Provide Granular Access to the Monitor Tab

In some cases you might want to enable the administrator to view some but not all areas of the **Monitor** tab. For example, you might want to restrict operations administrators to the Config and System logs only, because they do not contain sensitive user data. Although this section of the admin role definition specifies what areas of the **Monitor** tab the administrator can see, you can also couple privileges in this section with privacy privileges, such as disabling the ability to see usernames in logs and reports. One thing to keep in mind, however, is that any system-generated reports will still show usernames and IP addresses even if you disable that functionality in the role. For this reason, if you do not want the administrator to see any of the private user information, disable access to the specific reports as detailed in the following table.

The following table lists the **Monitor** tab access levels and the administrator roles for which they are available.



Device Group and Template roles can see log data only for the device groups that are within the access domains assigned to those roles.

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Monitor	Enables or disables access to the <b>Monitor</b> tab. If disabled, the admin will not see this tab or any of the associated logs or reports.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Logs	Enables or disables access to all log files. You can also leave this privilege enabled and then disable specific logs that you do not want the admin to see. Keep in mind that if you want to protect the privacy of your users while still providing access to one or more of the logs, you can disable the <b>Privacy &gt; Show Full Ip Addresses</b> option and/or the <b>Show User Names In Logs And Reports</b> option.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Traffic	Specifies whether the admin can see the traffic logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Threat	Specifies whether the admin can see the threat logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
URL Filtering	Specifies whether the admin can see the URL filtering logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
WildFire Submissions	Specifies whether the admin can see the WildFire logs. These logs are only available if you have a WildFire subscription.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Data Filtering	Specifies whether the admin can see the data filtering logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
HIP Match	Specifies whether the admin can see the HIP Match logs. HIP Match logs are only available if you have a GlobalProtect portal license and gateway subscription.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Configuration	Specifies whether the admin can see the configuration logs.	Firewall: Yes Panorama: Yes Device Group/Template: No	Yes	No	Yes
System	Specifies whether the admin can see the system logs.	Firewall: Yes Panorama: Yes Device Group/Template: No	Yes	No	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Alarms	Specifies whether the admin can see system-generated alarms.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Automated Correlation Engine	Enables or disables access to the correlation objects and correlated event logs generated on the firewall.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Correlation Objects	Specifies whether the admin can view and enable/disable the correlation objects.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Correlated Events	Specifies whether the admin	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Packet Capture	Specifies whether the admin can see packet captures (pcaps) from the <b>Monitor</b> tab. Keep in mind that packet captures are raw flow data and as such may contain user IP addresses. Disabling the <b>Show Full IP Addresses</b> privileges will not obfuscate the IP address in the pcap and you should therefore disable the Packet Capture privilege if you are concerned about user privacy.	Firewall: Yes Panorama: No Device Group/Template: No	Yes	Yes	Yes
App Scope	Specifies whether the admin can see the App Scope visibility and analysis tools. Enabling App Scope enables access to all of the <b>App Scope</b> charts.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Session Browser	Specifies whether the admin can browse and filter current running sessions on the firewall. Keep in mind that the session browser shows raw flow data and as such may contain user IP addresses. Disabling the <b>Show Full IP Addresses</b> privileges will not obfuscate the IP address in the session browser and you should therefore disable the <b>Session Browser</b> privilege if you are concerned about user privacy.	Firewall: Yes Panorama: No Device Group/Template: No	Yes	No	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Botnet	Specifies whether the admin can generate and view botnet analysis reports or view botnet reports in read-only mode. Disabling the <b>Show Full IP Addresses</b> privileges will not obfuscate the IP address in scheduled botnet reports and you should therefore disable the <b>Botnet</b> privilege if you are concerned about user privacy.	Firewall: Yes Panorama: No Device Group/Template: No	Yes	Yes	Yes
PDF Reports	Enables or disables access to all PDF reports. You can also leave this privilege enabled and then disable specific PDF reports that you do not want the admin to see. Keep in mind that if you want to protect the privacy of your users while still providing access to one or more of the reports, you can disable the <b>Privacy &gt; Show Full IP Addresses</b> option and/or the <b>Show User Names In Logs And Reports</b> option.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Manage PDF Summary	Specifies whether the admin can view, add or delete PDF summary report definitions. With read-only access, the admin can see PDF summary report definitions, but not add or delete them. If you disable this option, the admin can neither view the report definitions nor add/delete them.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes
PDF Summary Reports	Specifies whether the admin can see the generated PDF Summary reports in <b>Monitor &gt; Reports</b> . If you disable this option, the <b>PDF Summary Reports</b> category will not display in the <b>Reports</b> node.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
User Activity Report	Specifies whether the admin can view, add or delete User Activity report definitions and download the reports. With read-only access, the admin can see User Activity report definitions, but not add, delete, or download them. If you disable this option, the admin cannot see this category of PDF report.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes
Report Groups	Specifies whether the admin can view, add or delete report group definitions. With read-only access, the admin can see report group definitions, but not add or delete them. If you disable this option, the admin cannot see this category of PDF report.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Email Scheduler	Specifies whether the admin can schedule report groups for email. Because the generated reports that get emailed may contain sensitive user data that is not removed by disabling the <b>Privacy &gt; Show Full IP Addresses</b> option and/or the <b>Show User Names In Logs And Reports</b> options and because they may also show log data to which the admin does not have access, you should disable the <b>Email Scheduler</b> option if you have user privacy requirements.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes
Manage Custom Reports	Enables or disables access to all custom report functionality. You can also leave this privilege enabled and then disable specific custom report categories that you do not want the admin to be able to access. Keep in mind that if you want to protect the privacy of your users while still providing access to one or more of the reports, you can disable the <b>Privacy &gt; Show Full IP Addresses</b> option and/or the <b>Show User Names In Logs And Reports</b> option.   Reports that are scheduled to run rather than run on demand will show IP address and user information. In this case, be sure to restrict access to the corresponding report areas. In addition, the custom report feature does not restrict the ability to generate reports that contain log data contained in logs that are excluded from the admin role.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Application Statistics	Specifies whether the admin can create a custom report that includes data from the application statistics database.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Data Filtering Log	Specifies whether the admin can create a custom report that includes data from the Data Filtering logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Threat Log	Specifies whether the admin can create a custom report that includes data from the Threat logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Threat Summary	Specifies whether the admin can create a custom report that includes data from the Threat Summary database.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Traffic Log	Specifies whether the admin can create a custom report that includes data from the Traffic logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Traffic Summary	Specifies whether the admin can create a custom report that includes data from the Traffic Summary database.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
URL Log	Specifies whether the admin can create a custom report that includes data from the URL Filtering logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Hipmatch	Specifies whether the admin can create a custom report that includes data from the HIP Match logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
WildFire Log	Specifies whether the admin can create a custom report that includes data from the WildFire logs.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
View Scheduled Custom Reports	Specifies whether the admin can view a custom report that has been scheduled to generate.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
View Predefined Application Reports	Specifies whether the admin can view Application Reports. Privacy privileges do not impact reports available on the <b>Monitor &gt; Reports</b> node and you should therefore disable access to the reports if you have user privacy requirements.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
View Predefined Threat Reports	Specifies whether the admin can view Threat Reports. Privacy privileges do not impact reports available on the <b>Monitor &gt; Reports</b> node and you should therefore disable access to the reports if you have user privacy requirements.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
View Predefined URL Filtering Reports	Specifies whether the admin can view URL Filtering Reports. Privacy privileges do not impact reports available on the <b>Monitor &gt; Reports</b> node and you should therefore disable access to the reports if you have user privacy requirements.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
View Predefined Traffic Reports	Specifies whether the admin can view Traffic Reports. Privacy privileges do not impact reports available on the <b>Monitor &gt; Reports</b> node and you should therefore disable access to the reports if you have user privacy requirements.	Firewall: Yes Panorama: Yes Device Group/Template: Yes	Yes	No	Yes

## Provide Granular Access to the Policy Tab

If you enable the Policy option in the admin role profile, you can then enable, disable, or provide read-only access to specific nodes within the tab as necessary for the admin role you are defining. By enabling access to a specific policy type, you enable the ability to view, add, or delete policy rules. By enabling read-only access to a specific policy, you enable the admin to view the corresponding policy rule base, but not add or delete rules. Disabling access to a specific type of policy prevents the admin from seeing the policy rule base.

Because policy that is based on specific users (by user name or IP address) must be explicitly defined, privacy settings that disable the ability to see full IP addresses or user names do not apply to the Policy tab. Therefore, you should only allow access to the Policy tab to administrators that are excluded from user privacy restrictions.

Access Level	Description	Enable	Read Only	Disable
Security	Enable this privilege to allow the admin to view, add, and/or delete security rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the security rulebase, disable this privilege.	Yes	Yes	Yes
NAT	Enable this privilege to allow the admin to view, add, and/or delete NAT rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the NAT rulebase, disable this privilege.	Yes	Yes	Yes
QoS	Enable this privilege to allow the admin to view, add, and/or delete QoS rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the QoS rulebase, disable this privilege.	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Policy Based Forwarding	Enable this privilege to allow the admin to view, add, and/or delete Policy-Based Forwarding (PBF) rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the PBF rulebase, disable this privilege.	Yes	Yes	Yes
Decryption	Enable this privilege to allow the admin to view, add, and/or delete decryption rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the decryption rulebase, disable this privilege.	Yes	Yes	Yes
Application Override	Enable this privilege to allow the admin to view, add, and/or delete application override policy rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the application override rulebase, disable this privilege.	Yes	Yes	Yes
Captive Portal	Enable this privilege to allow the admin to view, add, and/or delete Captive Portal rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the Captive Portal rulebase, disable this privilege.	Yes	Yes	Yes
DoS Protection	Enable this privilege to allow the admin to view, add, and/or delete DoS protection rules. Set the privilege to read-only if you want the admin to be able to see the rules, but not modify them. To prevent the admin from seeing the DoS protection rulebase, disable this privilege.	Yes	Yes	Yes

## Provide Granular Access to the Objects Tab

An *object* is a container that groups specific policy filter values—such as IP addresses, URLs, applications, or services—for simplified rule definition. For example, an address object might contain specific IP address definitions for the web and application servers in your DMZ zone.

When deciding whether to allow access to the objects tab as a whole, determine whether the admin will have policy definition responsibilities. If not, the admin probably does not need access to the tab. If, however, the admin will need to create policy, you can enable access to the tab and then provide granular access privileges at the node level.

By enabling access to a specific node, you give the admin the privilege to view, add, and delete the corresponding object type. Giving read-only access allows the admin to view the already defined objects, but not create or delete any. Disabling a node prevents the admin from seeing the node in the web interface.

Access Level	Description	Enable	Read Only	Disable
Addresses	Specifies whether the admin can view, add, or delete address objects for use in security policy.	Yes	Yes	Yes
Address Groups	Specifies whether the admin can view, add, or delete address group objects for use in security policy.	Yes	Yes	Yes
Regions	Specifies whether the admin can view, add, or delete regions objects for use in security, decryption, or DoS policy.	Yes	Yes	Yes
Applications	Specifies whether the admin can view, add, or delete application objects for use in policy.	Yes	Yes	Yes
Application Groups	Specifies whether the admin can view, add, or delete application group objects for use in policy.	Yes	Yes	Yes
Application Filters	Specifies whether the admin can view, add, or delete application filters for simplification of repeated searches.	Yes	Yes	Yes
Services	Specifies whether the admin can view, add, or delete service objects for use in creating policy rules that limit the port numbers an application can use.	Yes	Yes	Yes
Service Groups	Specifies whether the admin can view, add, or delete service group objects for use in security policy.	Yes	Yes	Yes
Tags	Specifies whether the admin can view, add, or delete tags that have been defined on the device.	Yes	Yes	Yes
GlobalProtect	Specifies whether the admin can view, add, or delete HIP objects and profiles. You can restrict access to both types of objects at the GlobalProtect level, or provide more granular control by enabling the GlobalProtect privilege and restricting HIP Object or HIP Profile access.	Yes	No	Yes
HIP Objects	Specifies whether the admin can view, add, or delete HIP objects, which are used to define HIP profiles. HIP Objects also generate HIP Match logs.	Yes	Yes	Yes
HIP Profiles	Specifies whether the admin can view, add, or delete HIP Profiles for use in security policy and/or for generating HIP Match logs.	Yes	Yes	Yes
Dynamic Block Lists	Specifies whether the admin can view, add, or delete dynamic block lists for use in security policy.	Yes	Yes	Yes
Custom Objects	Specifies whether the admin can see the custom spyware and vulnerability signatures. You can restrict access to either enable or disable access to all custom signatures at this level, or provide more granular control by enabling the Custom Objects privilege and then restricting access to each type of signature.	Yes	No	Yes

Access Level	Description	Enable	Read Only	Disable
Data Patterns	Specifies whether the admin can view, add, or delete custom data pattern signatures for use in creating custom Vulnerability Protection profiles.	Yes	Yes	Yes
Spyware	Specifies whether the admin can view, add, or delete custom spyware signatures for use in creating custom Vulnerability Protection profiles.	Yes	Yes	Yes
Vulnerability	Specifies whether the admin can view, add, or delete custom vulnerability signatures for use in creating custom Vulnerability Protection profiles.	Yes	Yes	Yes
URL Category	Specifies whether the admin can view, add, or delete custom URL categories for use in policy.	Yes	Yes	Yes
Security Profiles	Specifies whether the admin can see security profiles. You can restrict access to either enable or disable access to all security profiles at this level, or provide more granular control by enabling the Security Profiles privilege and then restricting access to each type of profile.	Yes	No	Yes
Antivirus	Specifies whether the admin can view, add, or delete antivirus profiles.	Yes	Yes	Yes
Anti-Spyware	Specifies whether the admin can view, add, or delete Anti-Spyware profiles.	Yes	Yes	Yes
Vulnerability Protection	Specifies whether the admin can view, add, or delete Vulnerability Protection profiles.	Yes	Yes	Yes
URL Filtering	Specifies whether the admin can view, add, or delete URL filtering profiles.	Yes	Yes	Yes
File Blocking	Specifies whether the admin can view, add, or delete file blocking profiles.	Yes	Yes	Yes
Data Filtering	Specifies whether the admin can view, add, or delete data filtering profiles.	Yes	Yes	Yes
DoS Protection	Specifies whether the admin can view, add, or delete DoS protection profiles.	Yes	Yes	Yes
Security Profile Groups	Specifies whether the admin can view, add, or delete security profile groups.	Yes	Yes	Yes
Log Forwarding	Specifies whether the admin can view, add, or delete log forwarding profiles.	Yes	Yes	Yes
Decryption Profile	Specifies whether the admin can view, add, or delete decryption profiles.	Yes	Yes	Yes
Schedules	Specifies whether the admin can view, add, or delete schedules for limiting a security policy to a specific date and/or time range.	Yes	Yes	Yes

## Provide Granular Access to the Network Tab

When deciding whether to allow access to the **Network** tab as a whole, determine whether the admin will have network administration responsibilities, including GlobalProtect administration. If not, the admin probably does not need access to the tab.

You can also define access to the **Network** tab at the node level. By enabling access to a specific node, you give the admin the privilege to view, add, and delete the corresponding network configurations. Giving read-only access allows the admin to view the already-defined configuration, but not create or delete any. Disabling a node prevents the admin from seeing the node in the web interface.

Access Level	Description	Enable	Read Only	Disable
Interfaces	Specifies whether the admin can view, add, or delete interface configurations.	Yes	Yes	Yes
Zones	Specifies whether the admin can view, add, or delete zones.	Yes	Yes	Yes
VLANs	Specifies whether the admin can view, add, or delete VLANs.	Yes	Yes	Yes
Virtual Wires	Specifies whether the admin can view, add, or delete virtual wires.	Yes	Yes	Yes
Virtual Routers	Specifies whether the admin can view, add, modify or delete virtual routers.	Yes	Yes	Yes
IPSec Tunnels	Specifies whether the admin can view, add, modify, or delete IPSec Tunnel configurations.	Yes	Yes	Yes
DHCP	Specifies whether the admin can view, add, modify, or delete DHCP server and DHCP relay configurations.	Yes	Yes	Yes
DNS Proxy	Specifies whether the admin can view, add, modify, or delete DNS proxy configurations.	Yes	Yes	Yes
GlobalProtect	Specifies whether the admin can view, add, modify GlobalProtect portal and gateway configurations. You can disable access to the GlobalProtect functions entirely, or you can enable the GlobalProtect privilege and then restrict the role to either the portal or gateway configuration areas.	Yes	No	Yes
Portals	Specifies whether the admin can view, add, modify, or delete GlobalProtect portal configurations.	Yes	Yes	Yes
Gateways	Specifies whether the admin can view, add, modify, or delete GlobalProtect gateway configurations.	Yes	Yes	Yes
MDM	Specifies whether the admin can view add, modify, or delete GlobalProtect MDM server configurations.	Yes	Yes	Yes
QoS	Specifies whether the admin can view add, modify, or delete QoS configurations.	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
LLDP	Specifies whether the admin can view add, modify, or delete LLDP configurations.	Yes	Yes	Yes
Network Profiles	Sets the default state to enable or disable for all of the Network settings described below.	Yes	No	Yes
IKE Gateways	<p>Controls access to the <b>Network Profiles &gt; IKE Gateways</b> node. If you disable this privilege, the administrator will not see the <b>IKE Gateways</b> node or define gateways that include the configuration information necessary to perform IKE protocol negotiation with peer gateway.</p> <p>If the privilege state is set to read-only, you can view the currently configured IKE Gateways but cannot add or edit gateways.</p>	Yes	Yes	Yes
GlobalProtect IPSec Crypto	<p>Controls access to the <b>Network Profiles &gt; GlobalProtect IPSec Crypto</b> node.</p> <p>If you disable this privilege, the administrator will not see that node, or configure algorithms for authentication and encryption in VPN tunnels between a GlobalProtect gateway and clients.</p> <p>If you set the privilege to read-only, the administrator can view existing GlobalProtect IPSec Crypto profiles but cannot add or edit them.</p>	Yes	Yes	Yes
IPSec Crypto	<p>Controls access to the <b>Network Profiles &gt; IPSec Crypto</b> node. If you disable this privilege, the administrator will not see the <b>Network Profiles &gt; IPSec Crypto</b> node or specify protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPSec SA negotiation.</p> <p>If the privilege state is set to read-only, you can view the currently configured IPSec Crypto configuration but cannot add or edit a configuration.</p>	Yes	Yes	Yes
IKE Crypto	Controls how devices exchange information to ensure secure communication. Specify the protocols and algorithms for identification, authentication, and encryption in VPN tunnels based on IPsec SA negotiation (IKEv1 Phase-1).	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Monitor	<p>Controls access to the <b>Network Profiles &gt; Monitor</b> node. If you disable this privilege, the administrator will not see the <b>Network Profiles &gt; Monitor</b> node or be able to create or edit a monitor profile that is used to monitor IPSec tunnels and monitor a next-hop device for policy-based forwarding (PBF) rules.</p> <p>If the privilege state is set to read-only, you can view the currently configured monitor profile configuration but cannot add or edit a configuration.</p>	Yes	Yes	Yes
Interface Mgmt	<p>Controls access to the <b>Network Profiles &gt; Interface Mgmt</b> node. If you disable this privilege, the administrator will not see the <b>Network Profiles &gt; Interface Mgmt</b> node or be able to specify the protocols that are used to manage the firewall.</p> <p>If the privilege state is set to read-only, you can view the currently configured Interface management profile configuration but cannot add or edit a configuration.</p>	Yes	Yes	Yes
Zone Protection	<p>Controls access to the <b>Network Profiles &gt; Zone Protection</b> node. If you disable this privilege, the administrator will not see the <b>Network Profiles &gt; Zone Protection</b> node or be able to configure a profile that determines how the firewall responds to attacks from specified security zones.</p> <p>If the privilege state is set to read-only, you can view the currently configured Zone Protection profile configuration but cannot add or edit a configuration.</p>	Yes	Yes	Yes
QoS Profile	<p>Controls access to the <b>Network Profiles &gt; QoS</b> node. If you disable this privilege, the administrator will not see the <b>Network Profiles &gt; QoS</b> node or be able to configure a QoS profile that determines how QoS traffic classes are treated.</p> <p>If the privilege state is set to read-only, you can view the currently configured QoS profile configuration but cannot add or edit a configuration.</p>	Yes	Yes	Yes
LLDP Profile	<p>Controls access to the <b>Network Profiles &gt; LLDP</b> node. If you disable this privilege, the administrator will not see the <b>Network Profiles &gt; LLDP</b> node or be able to configure an LLDP profile that controls whether the interfaces on the firewall can participate in the Link Layer Discovery Protocol.</p> <p>If the privilege state is set to read-only, you can view the currently configured LLDP profile configuration but cannot add or edit a configuration.</p>	Yes	Yes	Yes

## Provide Granular Access to the Device Tab

Access Level	Description	Enable	Read Only	Disable
Setup	<p>Controls access to the <b>Setup</b> node. If you disable this privilege, the administrator will not see the <b>Setup</b> node or have access to device-wide setup configuration information, such as Management, Operations, Services, Content-ID, WildFire, Session, or Hardware Security Module (HSM) setup information.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes
Management	<p>Controls access to the <b>Management</b> node. If you disable this privilege, the administrator will not be able to configure settings such as the hostname, domain, timezone, authentication, logging and reporting, Panorama, management interface, banner, message, and password complexity settings, and more.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes
Operations	<p>Controls access to the <b>Operations</b> node. If you disable this privilege, the administrator will not be able to manage configuration files, or reboot or shut down the firewall, among other things.</p>	Yes	Yes	Yes
Services	<p>Controls access to the <b>Services</b> node. If you disable this privilege, the administrator will not be able to configure services for DNS servers, an update server, proxy server, or NTP servers, or set up service routes.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes
Content-ID	<p>Controls access to the <b>Content-ID</b> node. If you disable this privilege, the administrator will not be able to configure URL filtering or Content-ID.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes
WildFire	<p>Controls access to the <b>WildFire</b> node. If you disable this privilege, the administrator will not be able to configure WildFire settings.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Session	<p>Controls access to the <b>Session</b> node. If you disable this privilege, the administrator will not be able to configure session settings or timeouts for TCP, UDP or ICMP, or configure decryption or VPN session settings.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes
HSM	<p>Controls access to the <b>HSM</b> node. If you disable this privilege, the administrator will not be able to configure a Hardware Security Module.</p> <p>If the privilege state is set to read-only, you can view the current configuration but cannot make any changes.</p>	Yes	Yes	Yes
Config Audit	<p>Controls access to the <b>Config Audit</b> node. If you disable this privilege, the administrator will not see the <b>Config Audit</b> node or have access to any device-wide configuration information.</p>	Yes	No	Yes
Admin Roles	<p>Controls access to the <b>Admin Roles</b> node. This function can only be allowed for read-only access.</p> <p>If you disable this privilege, the administrator will not see the <b>Admin Roles</b> node or have access to any device-wide information concerning admin roles configuration.</p> <p>If you set this privilege to read-only, you can view the configuration information for all admin roles configured on the device.</p>	No	Yes	Yes
Administrators	<p>Controls access to the <b>Administrators</b> node. This function can only be allowed for read-only access.</p> <p>If you disable this privilege, the administrator will not see the <b>Administrators</b> node or have access to information about their own admin account.</p> <p>If you set this privilege to read-only, the administrator can view the configuration information for their own admin account. They will not see any information about other admin accounts configured on the device.</p>	No	Yes	Yes
Virtual Systems	<p>Controls access to the <b>Virtual Systems</b> node. If you disable this privilege, the administrator will not see or be able to configure virtual systems.</p> <p>If the privilege state is set to read-only, you can view the currently configured virtual systems but cannot add or edit a configuration.</p>	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Shared Gateways	<p>Controls access to the <b>Shared Gateways</b> node. Shared gateways allow virtual systems to share a common interface for external communications.</p> <p>If you disable this privilege, the administrator will not see or be able to configure shared gateways.</p> <p>If the privilege state is set to read-only, you can view the currently configured shared gateways but cannot add or edit a configuration.</p>	Yes	Yes	Yes
User Identification	<p>Controls access to the <b>User Identification</b> node. If you disable this privilege, the administrator will not see the <b>User Identification</b> node or have access to device-wide User Identification configuration information, such as User Mapping, User-ID Agents, Service, Terminal Services Agents, Group Mappings Settings or Captive Portal Settings.</p> <p>If you set this privilege to read-only, the administrator can view configuration information for the device but is not allowed to perform any configuration procedures.</p>	Yes	Yes	Yes
VM Information Source	<p>Controls access to the <b>VM Information Source</b> node that allows you to configure the firewall/Windows User-ID agent to collect VM inventory automatically. If you disable this privilege, the administrator will not see the <b>VM Information Source</b> node.</p> <p>If you set this privilege to read-only, the administrator can view the VM information sources configured but cannot add, edit, or delete any sources.</p> <p> This privilege is not available to Device Group and Template administrators.</p>	Yes	Yes	Yes
High Availability	<p>Controls access to the <b>High Availability</b> node. If you disable this privilege, the administrator will not see the <b>High Availability</b> node or have access to device-wide high availability configuration information such as General setup information or Link and Path Monitoring.</p> <p>If you set this privilege to read-only, the administrator can view High Availability configuration information for the device but is not allowed to perform any configuration procedures.</p>	Yes	Yes	Yes
Certificate Management	Sets the default state to enable or disable for all of the Certificate settings described below.	Yes	No	Yes

Access Level	Description	Enable	Read Only	Disable
Certificates	<p>Controls access to the <b>Certificates</b> node. If you disable this privilege, the administrator will not see the <b>Certificates</b> node or be able to configure or access information regarding Device Certificates or Default Trusted Certificate Authorities.</p> <p>If you set this privilege to read-only, the administrator can view Certificate configuration information for the device but is not allowed to perform any configuration procedures.</p>	Yes	Yes	Yes
Certificate Profile	<p>Controls access to the <b>Certificate Profile</b> node. If you disable this privilege, the administrator will not see the <b>Certificate Profile</b> node or be able to create certificate profiles.</p> <p>If you set this privilege to read-only, the administrator can view Certificate Profiles that are currently configured for the device but is not allowed to create or edit a certificate profile.</p>	Yes	Yes	Yes
OCSP Responder	<p>Controls access to the <b>OCSP Responder</b> node. If you disable this privilege, the administrator will not see the <b>OCSP Responder</b> node or be able to define a server that will be used to verify the revocation status of certificates issued by the PAN-OS device.</p> <p>If you set this privilege to read-only, the administrator can view the <b>OCSP Responder</b> configuration for the device but is not allowed to create or edit an OCSP responder configuration.</p>	Yes	Yes	Yes
SSL/TLS Service Profile	<p>Controls access to the <b>SSL/TLS Service Profile</b> node. If you disable this privilege, the administrator will not see the node or configure a profile that specifies a certificate and a protocol version or range of versions for device services that use SSL/TLS.</p> <p>If you set this privilege to read-only, the administrator can view existing SSL/TLS Service profiles but cannot create or edit them.</p>	Yes	Yes	Yes
Response Pages	<p>Controls access to the <b>Response Pages</b> node. If you disable this privilege, the administrator will not see the <b>Response Page</b> node or be able to define a custom HTML message that is downloaded and displayed instead of a requested web page or file.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Response Page</b> configuration for the device but is not allowed to create or edit a response page configuration.</p>	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Log Settings	Sets the default state to enable or disable for all of the Log settings described below.	Yes	No	Yes
System	Controls access to the <b>Log Settings &gt; System</b> node. If you disable this privilege, the administrator will not see the <b>Log Settings &gt; System</b> node or be able to specify the severity levels of the system log entries that are logged remotely with Panorama and sent as SNMP traps, syslog messages, and/or email notifications.  If you set this privilege to read-only, the administrator can view the <b>Log Settings &gt; System</b> configuration for the device but is not allowed to create or edit a configuration.	Yes	Yes	Yes
Config	Controls access to the <b>Log Settings &gt; Config</b> node. If you disable this privilege, the administrator will not see the <b>Log Settings &gt; Config</b> node or be able to specify the configuration log entries that are logged remotely with Panorama, and sent as syslog messages and/or email notification.  If you set this privilege to read-only, the administrator can view the <b>Log Settings &gt; Config</b> configuration for the device but is not allowed to create or edit a configuration.	Yes	Yes	Yes
HIP Match	Controls access to the <b>Log Settings &gt; HIP Match</b> node. If you disable this privilege, the administrator will not see the <b>Log Settings &gt; HIP Match</b> node or be able to specify the Host Information Profile (HIP) match log settings that are used to provide information on security rules that apply to GlobalProtect clients.  If you set this privilege to read-only, the administrator can view the <b>Log Settings &gt; HIP</b> configuration for the device but is not allowed to create or edit a configuration.	Yes	Yes	Yes
Alarms	Controls access to the <b>Log Settings &gt; Alarms</b> node. If you disable this privilege, the administrator will not see the <b>Log Settings &gt; Alarms</b> node or be able to configure notifications that are generated when a security rule (or group of rules) has been hit repeatedly in a set period of time.  If you set this privilege to read-only, the administrator can view the <b>Log Settings &gt; Alarms</b> configuration for the device but is not allowed to create or edit a configuration.	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Manage Logs	<p>Controls access to the <b>Log Settings &gt; Manage Logs</b> node. If you disable this privilege, the administrator will not see the <b>Log Settings &gt; Manage Logs</b> node or be able to clear the indicated logs.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Log Settings &gt; Manage Logs</b> information but cannot clear any of the logs.</p>	Yes	Yes	Yes
Server Profiles	Sets the default state to enable or disable for all of the Server Profiles settings described below.	Yes	No	Yes
SNMP Trap	<p>Controls access to the <b>Server Profiles &gt; SNMP Trap</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; SNMP Trap</b> node or be able to specify one or more SNMP trap destinations to be used for system log entries.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; SNMP Trap Logs</b> information but cannot specify SNMP trap destinations.</p>	Yes	Yes	Yes
Syslog	<p>Controls access to the <b>Server Profiles &gt; Syslog</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; Syslog</b> node or be able to specify one or more syslog servers.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; Syslog</b> information but cannot specify syslog servers.</p>	Yes	Yes	Yes
Email	<p>Controls access to the <b>Server Profiles &gt; Email</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; Email</b> node or be able to configure an email profile that can be used to enable email notification for system and configuration log entries</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; Email</b> information but cannot configure an email profile.</p>	Yes	Yes	Yes
Netflow	<p>Controls access to the <b>Server Profiles &gt; Netflow</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; Netflow</b> node or be able to define a NetFlow server profile, which specifies the frequency of the export along with the NetFlow servers that will receive the exported data.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; Netflow</b> information but cannot define a Netflow profile.</p>	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
RADIUS	<p>Controls access to the <b>Server Profiles &gt; RADIUS</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; RADIUS</b> node or be able to configure settings for the RADIUS servers that are identified in authentication profiles.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; RADIUS</b> information but cannot configure settings for the RADIUS servers.</p>	Yes	Yes	Yes
TACACS+	<p>Controls access to the <b>Server Profiles &gt; TACACS+</b> node.</p> <p>If you disable this privilege, the administrator will not see the node or configure settings for the TACACS+ servers that authentication profiles reference.</p> <p>If you set this privilege to read-only, the administrator can view existing TACACS+ server profiles but cannot add or edit them.</p>	Yes	Yes	Yes
LDAP	<p>Controls access to the <b>Server Profiles &gt; LDAP</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; LDAP</b> node or be able to configure settings for the LDAP servers to use for authentication by way of authentication profiles.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; LDAP</b> information but cannot configure settings for the LDAP servers.</p>	Yes	Yes	Yes
Kerberos	<p>Controls access to the <b>Server Profiles &gt; Kerberos</b> node. If you disable this privilege, the administrator will not see the <b>Server Profiles &gt; Kerberos</b> node or configure a Kerberos server that allows users to authenticate natively to a domain controller.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Server Profiles &gt; Kerberos</b> information but cannot configure settings for Kerberos servers.</p>	Yes	Yes	Yes
Local User Database	Sets the default state to enable or disable for all of the Local User Database settings described below.	Yes	No	Yes
Users	<p>Controls access to the <b>Local User Database &gt; Users</b> node. If you disable this privilege, the administrator will not see the <b>Local User Database &gt; Users</b> node or set up a local database on the firewall to store authentication information for remote access users, device administrators, and captive portal users.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Local User Database &gt; Users</b> information but cannot set up a local database on the firewall to store authentication information.</p>	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
User Groups	<p>Controls access to the <b>Local User Database &gt; Users</b> node. If you disable this privilege, the administrator will not see the <b>Local User Database &gt; Users</b> node or be able to add user group information to the local database.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Local User Database &gt; Users</b> information but cannot add user group information to the local database.</p>	Yes	Yes	Yes
Authentication Profile	<p>Controls access to the <b>Authentication Profile</b> node. If you disable this privilege, the administrator will not see the <b>Authentication Profile</b> node or be able to create or edit authentication profiles that specify local database, RADIUS, TACACS+, LDAP, or Kerberos settings that can be assigned to administrator accounts.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Authentication Profile</b> information but cannot create or edit an authentication profile.</p>	Yes	Yes	Yes
Authentication Sequence	<p>Controls access to the <b>Authentication Sequence</b> node. If you disable this privilege, the administrator will not see the <b>Authentication Sequence</b> node or be able to create or edit an authentication sequence.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Authentication Profile</b> information but cannot create or edit an authentication sequence.</p>	Yes	Yes	Yes
Access Domain	<p>Controls access to the <b>Access Domain</b> node. If you disable this privilege, the administrator will not see the <b>Access Domain</b> node or be able to create or edit an access domain.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Access Domain</b> information but cannot create or edit an access domain.</p>	Yes	Yes	Yes
Scheduled Log Export	<p>Controls access to the <b>Scheduled Log Export</b> node. If you disable this privilege, the administrator will not see the <b>Scheduled Log Export</b> node or be able schedule exports of logs and save them to a File Transfer Protocol (FTP) server in CSV format or use Secure Copy (SCP) to securely transfer data between the device and a remote host.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Scheduled Log Export Profile</b> information but cannot schedule the export of logs.</p>	Yes	No	Yes

Access Level	Description	Enable	Read Only	Disable
Software	<p>Controls access to the <b>Software</b> node. If you disable this privilege, the administrator will not see the <b>Software</b> node or view the latest versions of the PAN-OS software available from Palo Alto Networks, read the release notes for each version, and select a release to download and install.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Software</b> information but cannot download or install software.</p>	Yes	Yes	Yes
GlobalProtect Client	<p>Controls access to the <b>GlobalProtect Client</b> node. If you disable this privilege, the administrator will not see the <b>GlobalProtect Client</b> node or view available GlobalProtect releases, download the code or activate the GlobalProtect agent.</p> <p>If you set this privilege to read-only, the administrator can view the available <b>GlobalProtect Client</b> releases but cannot download or install the agent software.</p>	Yes	Yes	Yes
Dynamic Updates	<p>Controls access to the <b>Dynamic Updates</b> node. If you disable this privilege, the administrator will not see the <b>Dynamic Updates</b> node or be able to view the latest updates, read the release notes for each update, or select an update to upload and install.</p> <p>If you set this privilege to read-only, the administrator can view the available <b>Dynamic Updates</b> releases, read the release notes but cannot upload or install the software.</p>	Yes	Yes	Yes
Licenses	<p>Controls access to the <b>Licenses</b> node. If you disable this privilege, the administrator will not see the <b>Licenses</b> node or be able to view the licenses installed or activate licenses.</p> <p>If you set this privilege to read-only, the administrator can view the installed <b>Licenses</b>, but cannot perform license management functions.</p>	Yes	Yes	Yes
Support	<p>Controls access to the <b>Support</b> node. If you disable this privilege, the administrator will not see the <b>Support</b> node or be able to access product and security alerts from Palo Alto Networks or generate tech support or stats dump files.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Support</b> node and access product and security alerts but cannot generate tech support or stats dump files.</p>	Yes	Yes	Yes

Access Level	Description	Enable	Read Only	Disable
Master Key and Diagnostics	<p>Controls access to the <b>Master Key and Diagnostics</b> node. If you disable this privilege, the administrator will not see the <b>Master Key and Diagnostics</b> node or be able to specify a master key to encrypt private keys on the firewall.</p> <p>If you set this privilege to read-only, the administrator can view the <b>Master Key and Diagnostics</b> node and view information about master keys that have been specified but cannot add or edit a new master key configuration.</p>	Yes	Yes	Yes

## Define User Privacy Settings in the Admin Role Profile

Access Level	Description	Enable	Read Only	Disable
Privacy	Sets the default state to enable or disable for all of the privacy settings described below.	Yes	N/A	Yes
Show Full IP addresses	<p>When set to disable, full IP addresses obtained by traffic running through the Palo Alto firewall are not shown in logs or reports. In place of the IP addresses that are normally displayed, the relevant subnet is displayed.</p>  Scheduled reports that are displayed in the interface through <b>Monitor &gt; Reports</b> and reports that are sent via scheduled emails will still display full IP addresses. Because of this exception, we recommend that the following settings within the <b>Monitor</b> tab be set to disable: Custom Reports, Application Reports, Threat Reports, URL Filtering Reports, Traffic Reports and Email Scheduler.	Yes	N/A	Yes
Show User Names in Logs and Reports	<p>When set to disable, user names obtained by traffic running through the Palo Alto Networks firewall are not shown in logs or reports. Columns where the user names would normally be displayed are empty.</p>  Scheduled reports that are displayed in the interface through <b>Monitor &gt; Reports</b> or reports that are sent via the email scheduler will still display user names. Because of this exception, we recommend that the following settings within the Monitor tab be set to disable: Custom Reports, Application Reports, Threat Reports, URL Filtering Reports, Traffic Reports and Email Scheduler.	Yes	N/A	Yes

Access Level	Description	Enable	Read Only	Disable
View Pcap Files	When set to disable, packet capture files that are normally available within the Traffic, Threat and Data Filtering logs are not displayed.	Yes	N/A	Yes

## Restrict Admin Access to Commit Functions

### Restrict User Access Using the Commit Setting

Access Level	Description	Enable	Read Only	Disable
Commit	When set to disable, an admin cannot commit any changes to a configuration.	Yes	N/A	Yes

## Restrict Admin Access to Validate Functions

### Restrict User Access Using the Validate Setting

Access Level	Description	Enable	Read Only	Disable
Validate	When set to disable, an admin cannot validate a configuration.	Yes	N/A	Yes

## Provide Granular Access to Global Settings

### Restrict User Access Using the Global Settings

Access Level	Description	Enable	Read Only	Disable
Global	Sets the default state to enable or disable for all of the global settings described below. In effect, this setting is only for System Alarms at this time.	Yes	N/A	Yes
System Alarms	When set to disable, an admin cannot view or acknowledge alarms that are generated.	Yes	N/A	Yes

## Provide Granular Access to the Panorama Tab

The following table lists the **Panorama** tab access levels and the custom Panorama administrator roles for which they are available. Firewall administrators cannot access any of these privileges.

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Setup	<p>Specifies whether the administrator can view or edit Panorama setup information, such as <b>Management</b>, <b>Operations</b>, <b>Services</b>, <b>WildFire</b>, or <b>HSM</b>.</p> <p>If you set the privilege to:</p> <ul style="list-style-type: none"> <li>• read-only, the administrator can see the information but cannot edit it.</li> <li>• disable this privilege, the administrator cannot see or edit the information.</li> </ul>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
High Availability	<p>Specifies whether the administrator can view and manage high availability (HA) settings for the Panorama management server.</p> <p>If you set this privilege to read-only, the administrator can view HA configuration information for the Panorama management server but can't manage the configuration.</p> <p>If you disable this privilege, the administrator can't see or manage HA configuration settings for the Panorama management server.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Config Audit	Specifies whether the administrator can run Panorama configuration audits. If you disable this privilege, the administrator can't run Panorama configuration audits.	Panorama: Yes Device Group/Template: No	Yes	No	Yes
Administrators	<p>Specifies whether the administrator can view Panorama administrator account details.</p> <p>You can't enable full access to this function: just read-only access. (Only Panorama administrators with a dynamic role can add, edit, or delete Panorama administrators.) With read-only access, the administrator can see information about his or her own account but no other Panorama administrator accounts.</p> <p>If you disable this privilege, the administrator can't see information about any Panorama administrator account, including his or her own.</p>	Panorama: Yes Device Group/Template: No	No	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Admin Roles	<p>Specifies whether the administrator can view Panorama administrator roles.</p> <p>You can't enable full access to this function: just read-only access. (Only Panorama administrators with a dynamic role can add, edit, or delete custom Panorama roles.)</p> <p>With read-only access, the administrator can see Panorama administrator role configurations but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage Panorama administrator roles.</p>	<p>Panorama: Yes Device Group/Template: No</p>	No	Yes	Yes
Access Domain	<p>Specifies whether the administrator can view, add, edit, delete, or clone access domain configurations for Panorama administrators. (This privilege controls access only to the configuration of access domains, not access to the device groups, templates, and firewall contexts that are assigned to access domains.)</p> <p>If you set this privilege to read-only, the administrator can view Panorama access domain configurations but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage Panorama access domain configurations.</p>	<p>Panorama: Yes Device Group/Template: No</p>  <p>You assign access domains to Device Group and Template administrators so they can access the configuration and monitoring data within the device groups, templates, and firewall contexts that are assigned to those access domains.</p>	Yes	Yes	Yes
Authentication Profile	<p>Specifies whether the administrator can view, add, edit, delete, or clone authentication profiles for Panorama administrators.</p> <p>If you set this privilege to read-only, the administrator can view Panorama authentication profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage Panorama authentication profiles.</p>	<p>Panorama: Yes Device Group/Template: No</p>	Yes	Yes	Yes



Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Device Groups	<p>Specifies whether the administrator can view, edit, add, or delete device groups.</p> <p>If you set this privilege to read-only, the administrator can see device group configurations but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage device group configurations.</p>	<p>Panorama: Yes Device Group/Template: Yes</p>  Device Group and Template administrators can access only the device groups that are within the access domains assigned to those administrators.	Yes	Yes	Yes
Managed Collectors	<p>Specifies whether the administrator can view, edit, add, or delete managed collectors.</p> <p>If you set this privilege to read-only, the administrator can see managed collector configurations but can't manage them.</p> <p>If you disable this privilege, the administrator can't view, edit, add, or delete managed collector configurations.</p> <p> This privilege applies only to the <b>Panorama &gt; Managed Collectors</b> page. An administrator with <b>Device Deployment</b> privileges can still use the <b>Panorama &gt; Device Deployment</b> pages to install updates on managed collectors.</p>	<p>Panorama: Yes Device Group/Template: No</p>	Yes	Yes	Yes
Collector Groups	<p>Specifies whether the administrator can view, edit, add, or delete Collector Groups.</p> <p>If you set this privilege to read-only, the administrator can see Collector Groups but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage Collector Groups.</p>	<p>Panorama: Yes Device Group/Template: No</p>	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
VMware Service Manager	<p>Specifies whether the administrator can view and edit VMware Service Manager settings.</p> <p>If you set this privilege to read-only, the administrator can see the settings but can't perform any related configuration or operational procedures.</p> <p>If you disable this privilege, the administrator can't see the settings or perform any related configuration or operational procedures.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Certificate Management	Sets the default state, enabled or disabled, for all of the Panorama certificate management privileges.	Panorama: Yes Device Group/Template: No	Yes	No	Yes
Certificates	<p>Specifies whether the administrator can view, edit, generate, delete, revoke, renew, or export certificates. This privilege also specifies whether the administrator can import or export HA keys.</p> <p>If you set this privilege to read-only, the administrator can see Panorama certificates but can't manage the certificates or HA keys.</p> <p>If you disable this privilege, the administrator can't see or manage Panorama certificates or HA keys.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Certificate Profile	<p>Specifies whether the administrator can view, add, edit, delete or clone Panorama certificate profiles.</p> <p>If you set this privilege to read-only, the administrator can see Panorama certificate profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage Panorama certificate profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
SSL/TLS Service Profile	<p>Specifies whether the administrator can view, add, edit, delete or clone SSL/TLS Service profiles.</p> <p>If you set this privilege to read-only, the administrator can see SSL/TLS Service profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage SSL/TLS Service profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Log Settings	Sets the default state, enabled or disabled, for all the log setting privileges.	Panorama: Yes Device Group/Template: No	Yes	No	Yes
System	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of System logs to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the System log forwarding settings but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p> <p> On a Panorama M-Series appliance, this privilege pertains only to System logs that Panorama generates. On a Panorama virtual appliance, this privilege applies to System logs that Panorama generates and to System logs that Panorama collects from firewalls. The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of System logs that an M-Series appliance collects from firewalls. The <b>Device &gt; Log Settings</b> page controls the forwarding of System logs directly from firewalls to external services (without aggregation on Panorama).</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Config	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of Config logs to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the Config log forwarding settings but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p>  <p>On a Panorama M-Series appliance, this privilege pertains only to Config logs that Panorama generates. On a Panorama virtual appliance, this privilege applies to Config logs that Panorama generates and to Config logs that Panorama collects from firewalls.</p> <p>The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of Config logs that an M-Series appliance collects from firewalls.</p> <p>The <b>Device &gt; Log Settings</b> page controls the forwarding of Config logs directly from firewalls to external services (without aggregation on Panorama).</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
HIP Match	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of HIP Match logs from a Panorama virtual appliance to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the forwarding settings of HIP Match logs but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p> <p> The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of HIP Match logs from a Panorama M-Series appliance. The <b>Device &gt; Log Settings</b> page controls the forwarding of HIP Match logs directly from firewalls to external services (without aggregation on Panorama).</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Correlation	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of Correlation logs to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the Correlation log forwarding settings but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p> <p> The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of Correlation logs from a Panorama M-Series appliance. The <b>Device &gt; Log Settings</b> page controls the forwarding of Correlation logs directly from firewalls to external services (without aggregation on Panorama).</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Traffic	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of Traffic logs from a Panorama virtual appliance to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the forwarding settings of Traffic logs but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p>  The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of Traffic logs from a Panorama M-Series appliance. The <b>Objects &gt; Log Forwarding</b> page controls the forwarding of Traffic logs directly from firewalls to external services (without aggregation on Panorama).	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Threat	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of Threat logs from a Panorama virtual appliance to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the forwarding settings of Threat logs but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p>  The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of Threat logs from a Panorama M-Series appliance. The <b>Objects &gt; Log Forwarding</b> page controls the forwarding of Threat logs directly from firewalls to external services (without aggregation on Panorama).	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Wildfire	<p>Specifies whether the administrator can see and configure the settings that control the forwarding of WildFire logs from a Panorama virtual appliance to external services (syslog, email, or SNMP trap servers).</p> <p>If you set this privilege to read-only, the administrator can see the forwarding settings of WildFire logs but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the settings.</p> <p> The <b>Panorama &gt; Collector Groups</b> page controls the forwarding of WildFire logs from a Panorama M-Series appliance. The <b>Objects &gt; Log Forwarding</b> page controls the forwarding of WildFire logs directly from firewalls to external services (without aggregation on Panorama).</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Server Profiles	<p>Sets the default state, enabled or disabled, for all the server profile privileges.</p> <p> These privileges pertain only to the server profiles that are used for forwarding logs that Panorama generates or collects from firewalls and the server profiles that are used for authenticating Panorama administrators. The <b>Device &gt; Server Profiles</b> pages control the server profiles that are used for forwarding logs directly from firewalls to external services (without aggregation on Panorama) and for authenticating firewall administrators.</p>	Panorama: Yes Device Group/Template: No	Yes	No	Yes
SNMP Trap	<p>Specifies whether the administrator can see and configure SNMP trap server profiles.</p> <p>If you set this privilege to read-only, the administrator can see SNMP trap server profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage SNMP trap server profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Syslog	<p>Specifies whether the administrator can see and configure Syslog server profiles.</p> <p>If you set this privilege to read-only, the administrator can see Syslog server profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage Syslog server profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Email	<p>Specifies whether the administrator can see and configure email server profiles.</p> <p>If you set this privilege to read-only, the administrator can see email server profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage email server profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
RADIUS	<p>Specifies whether the administrator can see and configure the RADIUS server profiles that are used to authenticate Panorama administrators.</p> <p>If you set this privilege to read-only, the administrator can see the RADIUS server profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the RADIUS server profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
TACACS+	<p>Specifies whether the administrator can see and configure the TACACS+ server profiles that are used to authenticate Panorama administrators.</p> <p>If you disable this privilege, the administrator can't see the node or configure settings for the TACACS+ servers that authentication profiles reference.</p> <p>If you set this privilege to read-only, the administrator can view existing TACACS+ server profiles but can't add or edit them.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
LDAP	<p>Specifies whether the administrator can see and configure the LDAP server profiles that are used to authenticate Panorama administrators.</p> <p>If you set this privilege to read-only, the administrator can see the LDAP server profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the LDAP server profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Kerberos	<p>Specifies whether the administrator can see and configure the Kerberos server profiles that are used to authenticate Panorama administrators.</p> <p>If you set this privilege to read-only, the administrator can see the Kerberos server profiles but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the Kerberos server profiles.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Scheduled Config Export	<p>Specifies whether the administrator can view, add, edit, delete, or clone scheduled Panorama configuration exports.</p> <p>If you set this privilege to read-only, the administrator can view the scheduled exports but can't manage them.</p> <p>If you disable this privilege, the administrator can't see or manage the scheduled exports.</p>	Panorama: Yes Device Group/Template: No	Yes	No	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Software	<p>Specifies whether the administrator can: view information about Panorama software updates; download, upload, or install the updates; and view the associated release notes.</p> <p>If you set this privilege to read-only, the administrator can view information about Panorama software updates and view the associated release notes but can't perform any related operations.</p> <p>If you disable this privilege, the administrator can't see Panorama software updates, see the associated release notes, or perform any related operations.</p> <p> This privilege pertains only to software installed on a Panorama management server. The <b>Panorama &gt; Device Deployment &gt; Software</b> page controls access to PAN-OS software deployed on firewalls and Panorama software deployed on Dedicated Log Collectors.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Dynamic Updates	<p>Specifies whether the administrator can: view information about Panorama content updates (for example, WildFire updates); download, upload, install, or revert the updates; and view the associated release notes.</p> <p>If you set this privilege to read-only, the administrator can view information about Panorama content updates and view the associated release notes but can't perform any related operations.</p> <p>If you disable this privilege, the administrator can't see Panorama content updates, see the associated release notes, or perform any related operations.</p> <p> This privilege pertains only to content updates installed on a Panorama management server. The <b>Panorama &gt; Device Deployment &gt; Dynamic Updates</b> page controls access to content updates deployed on firewalls and Dedicated Log Collectors.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Support	<p>Specifies whether the administrator can: view Panorama support license information, product alerts, and security alerts; activate a support license, generate Tech Support files, and manage cases</p> <p>If you set this privilege to read-only, the administrator can view Panorama support information, product alerts, and security alerts, but can't activate a support license, generate Tech Support files, or manage cases.</p> <p>If you disable this privilege, the administrator can't: see Panorama support information, product alerts, or security alerts; activate a support license, generate Tech Support files, or manage cases.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes
Device Deployment	<p>Sets the default state, enabled or disabled, for all the device deployment privileges.</p> <p> These privilege pertain only to software and content updates that Panorama administrators deploy on firewalls and Dedicated Log Collectors. The <b>Panorama &gt; Software and Panorama &gt; Dynamic Updates</b> pages control the software and content updates installed on a Panorama management server.</p>	Panorama: Yes Device Group/Template: Yes	Yes	No	Yes
Software	<p>Specifies whether the administrator can: view information about the software updates installed on firewalls and Log Collectors; download, upload, or install the updates; and view the associated release notes.</p> <p>If you set this privilege to read-only, the administrator can see information about the software updates and view the associated release notes but can't deploy the updates to firewalls or dedicated Log Collectors.</p> <p>If you disable this privilege, the administrator can't see information about the software updates, see the associated release notes, or deploy the updates to firewalls or Dedicated Log Collectors.</p>	Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
SSL VPN Client	<p>Specifies whether the administrator can: view information about SSL VPN client software updates on firewalls; download, upload, or activate the updates; and view the associated release notes.</p> <p>If you set this privilege to read-only, the administrator can see information about SSL VPN client software updates and view the associated release notes but can't activate the updates on firewalls.</p> <p>If you disable this privilege, the administrator can't see information about SSL VPN client software updates, see the associated release notes, or activate the updates on firewalls.</p>	Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes
GlobalProtect Client	<p>Specifies whether the administrator can: view information about GlobalProtect agent/app software updates on firewalls; download, upload, or activate the updates; and view the associated release notes.</p> <p>If you set this privilege to read-only, the administrator can see information about GlobalProtect agent/app software updates and view the associated release notes but can't activate the updates on firewalls.</p> <p>If you disable this privilege, the administrator can't see information about GlobalProtect agent/app software updates, see the associated release notes, or activate the updates on firewalls.</p>	Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes

Access Level	Description	Admin Role Availability	Enable	Read Only	Disable
Dynamic Updates	<p>Specifies whether the administrator can: view information about the content updates (for example, Applications updates) installed on firewalls and Dedicated Log Collectors; download, upload, or install the updates; and view the associated release notes.</p> <p>If you set this privilege to read-only, the administrator can see information about the content updates and view the associated release notes but can't deploy the updates to firewalls or Dedicated Log Collectors.</p> <p>If you disable this privilege, the administrator can't see information about the content updates, see the associated release notes, or deploy the updates to firewalls or Dedicated Log Collectors.</p>	Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes
Licenses	<p>Specifies whether the administrator can view, refresh, and activate firewall licenses.</p> <p>If you set this privilege to read-only, the administrator can view firewall licenses but can't refresh or activate those licenses.</p> <p>If you disable this privilege, the administrator can't view, refresh, or activate firewall licenses.</p>	Panorama: Yes Device Group/Template: Yes	Yes	Yes	Yes
Master Key and Diagnostics	<p>Specifies whether the administrator can view and configure a master key by which to encrypt private keys on Panorama.</p> <p>If you set this privilege to read-only, the administrator can view the Panorama master key configuration but can't change it.</p> <p>If you disable this privilege, the administrator can't see or edit the Panorama master key configuration.</p>	Panorama: Yes Device Group/Template: No	Yes	Yes	Yes

## Panorama Web Interface Access

The custom Panorama administrator roles allow you to define access to the options on Panorama and the ability to only allow access to Device Groups and Templates (**Policies**, **Objects**, **Network**, **Device** tabs).

The admin roles you can create are **Panorama** and **Device Group and Template**. You can't assign CLI access privileges to a **Device Group and Template** admin role. If you assign superuser privileges for the CLI to a **Panorama** admin role, administrators with that role can access all features regardless of the web interface privileges you assign.

Access Level	Description	Enable	Read Only	Disable
Dashboard	Controls access to the <b>Dashboard</b> tab. If you disable this privilege, the administrator will not see the tab and will not have access to any of the Dashboard widgets.	Yes	No	Yes
ACC	Controls access to the Application Command Center (ACC). If you disable this privilege, the <b>ACC</b> tab will not display in the web interface. Keep in mind that if you want to protect the privacy of your users while still providing access to the ACC, you can disable the <b>Privacy &gt; Show Full IP Addresses</b> option and/or the <b>Show User Names In Logs And Reports</b> option.	Yes	No	Yes
Monitor	Controls access to the <b>Monitor</b> tab. If you disable this privilege, the administrator will not see the <b>Monitor</b> tab and will not have access to any of the logs, packet captures, session information, reports or to App Scope. For more granular control over what monitoring information the admin can see, leave the Monitor option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Monitor Tab</a> .	Yes	No	Yes
Policies	Controls access to the <b>Policies</b> tab. If you disable this privilege, the administrator will not see the <b>Policies</b> tab and will not have access to any policy information. For more granular control over what policy information the admin can see, for example to enable access to a specific type of policy or to enable read-only access to policy information, leave the <b>Policies</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Policy Tab</a> .	Yes	No	Yes
Objects	Controls access to the <b>Objects</b> tab. If you disable this privilege, the administrator will not see the <b>Objects</b> tab and will not have access to any objects, security profiles, log forwarding profiles, decryption profiles, or schedules. For more granular control over what objects the admin can see, leave the <b>Objects</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Objects Tab</a> .	Yes	No	Yes

Access Level	Description	Enable	Read Only	Disable
Network	Controls access to the <b>Network</b> tab. If you disable this privilege, the administrator will not see the <b>Network</b> tab and will not have access to any interface, zone, VLAN, virtual wire, virtual router, IPsec tunnel, DHCP, DNS Proxy, GlobalProtect, or QoS configuration information or to the network profiles. For more granular control over what objects the admin can see, leave the <b>Network</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Network Tab</a> .	Yes	No	Yes
Device	Controls access to the <b>Device</b> tab. If you disable this privilege, the administrator will not see the <b>Device</b> tab and will not have access to any device-wide configuration information, such as User-ID, High Availability, server profile or certificate configuration information. For more granular control over what objects the admin can see, leave the <b>Device</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Device Tab</a> .   You can't enable access to the <b>Admin Roles</b> or <b>Administrators</b> nodes for a role-based administrator even if you enable full access to the <b>Device</b> tab.	Yes	No	Yes
Panorama	Controls access to the <b>Panorama</b> tab. If you disable this privilege, the administrator will not see the <b>Panorama</b> tab and will not have access to any Panorama-wide configuration information, such as Managed Devices, Managed Collectors, or Collector Groups.  For more granular control over what objects the admin can see, leave the <b>Panorama</b> option enabled and then enable or disable specific nodes on the tab as described in <a href="#">Provide Granular Access to the Panorama Tab</a> .	Yes	No	Yes
Validate	When set to disable, an admin cannot validate a configuration.	Yes	N/A	Yes

# Reference: Port Numbers Used by Palo Alto Networks Devices

The following tables list the ports that Palo Alto Networks devices use to communicate with each other, or with other services on the network.

- ▲ Ports Used for Management Functions
- ▲ Ports Used for HA
- ▲ Ports Used for Panorama
- ▲ Ports Used for GlobalProtect
- ▲ Ports Used for User-ID

## Ports Used for Management Functions

Destination Port	Protocol	Description
22	TCP	Used for communication from a client system to the firewall CLI interface.
80	TCP	The port the firewall listens on for <a href="#">Online Certificate Status Protocol (OCSP)</a> updates when acting as an OCSP responder.
123	UDP	Port the firewall uses for NTP updates.
443	TCP	Used for communication from a client system to the firewall web interface. This is also the port the firewall and User-ID agent listens on for <a href="#">VM Information source</a> updates. For monitoring an AWS environment, this is the only port that is used. For monitoring a VMware vCenter/ESXi environment, the listening port defaults to 443, but it is configurable.
162	UDP	Port the firewall, Panorama, or a Log Collector uses to <a href="#">Forward Traps to an SNMP Manager</a> .   This port doesn't need to be open on the Palo Alto Networks device. You must configure the Simple Network Management Protocol (SNMP) manager to listen on this port. For details, refer to the documentation of your SNMP management software.
161	UDP	Port the firewall listens on for polling requests (GET messages) from the SNMP manager.
514	TCP	Port that the firewall, Panorama, or a Log Collector uses to send logs to a syslog server if you <a href="#">Configure Syslog Monitoring</a> , and the ports that the PAN-OS integrated User-ID agent or Windows-based User-ID agent listens on for authentication syslog messages if you <a href="#">Configure User-ID to Receive User Mappings from a Syslog Sender</a> .
514	UDP	
6514	SSL	

Destination Port	Protocol	Description
2055	UDP	Default port the firewall uses to send NetFlow records to a NetFlow collector if you <a href="#">Configure NetFlow Exports</a> , but this is configurable.
5008	TCP	Port the GlobalProtect Mobile Security Manager listens on for HIP requests from the <a href="#">GlobalProtect gateways</a> . If you are using a third-party MDM system, you can configure the gateway to use a different port as required by the MDM vendor.
6080	TCP	Ports used for <a href="#">Captive Portal</a> : 6080 for NT LAN Manager (NTLM) authentication,
6081	TCP	6081 for Captive Portal in transparent mode, and 6082 for Captive Portal in redirect mode.
6082	TCP	

## Ports Used for HA

Firewalls configured as [High Availability](#) (HA) peers must be able to communicate with each other to maintain state information (HA1 control link) and synchronize data (HA2 data link). In Active/Active HA deployments the peer firewalls must also forward packets to the HA peer that owns the session. The HA3 link is a Layer 2 (MAC-in-MAC) link and it does not support Layer 3 addressing or encryption.

Destination Port	Protocol	Description
28769	TCP	Used for the HA1 control link for clear text communication between the HA peer firewalls. The HA1 link is a Layer 3 link and requires an IP address.
28260	TCP	
28	TCP	Used for the HA1 control link for encrypted communication (SSH over TCP) between the HA peer firewalls.
28770	TCP	Listening port for HA1 backup links.
28771	TCP	Used for heartbeat backups. Palo Alto Networks recommends enabling heartbeat backup on the MGT interface if you use an in-band port for the HA1 or the HA1 backup links.
99	IP	Used for the HA2 link to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between firewalls in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active device (Active/Passive) or active-primary (Active/Active) to the passive device (Active/Passive) or active-secondary (Active/Active). The HA2 link is a Layer 2 link, and it uses ether type 0x7261 by default.
29281	UDP	The HA data link can also be configured to use either IP (protocol number 99) or UDP (port 29281) as the transport, and thereby allow the HA data link to span subnets.

## Ports Used for Panorama

Destination Port	Protocol	Description
22	TCP	Used for communication from a client system to the <a href="#">Panorama</a> CLI interface.
443	TCP	Used for communication from a client system to the Panorama web interface.
3978	TCP	Used for communication between Panorama and managed devices (firewalls and Log Collectors) as well as for communication among Log Collectors in a Collector Group: <ul style="list-style-type: none"> <li>For communication between Panorama and firewalls, this is a bi-directional connection on which the firewalls forward logs to Panorama and Panorama pushes configuration changes to the firewalls. Context switching commands are sent over the same connection.</li> <li>Log Collectors use this destination port to forward logs to Panorama.</li> <li>For communication with the default Log Collector on an M-Series appliance in Panorama mode and with Dedicated Log Collectors (M-Series appliances in Log Collector mode).</li> </ul>
28769 (5.1 and later)	TCP	Used for the HA connectivity and synchronization between Panorama HA peers using clear text communication. Communication can be initiated by either peer.
28260 (5.0 and later)	TCP	
49160 (5.0 and earlier)	TCP	
28	TCP	Used for the HA connectivity and synchronization between Panorama HA peers using encrypted communication (SSH over TCP). Communication can be initiated by either peer.
28270 (6.0 and later)	TCP	Used for communication among Log Collectors in a Collector Group for log distribution.
49190 (5.1 and earlier)		
2049	TCP	Used by the Panorama virtual appliance to write logs to the NFS datastore.

## Ports Used for GlobalProtect

Destination Port	Protocol	Description
443	TCP	Used for communication between GlobalProtect agents and portals, or GlobalProtect agents and gateways and for SSL tunnel connections. GlobalProtect gateways also use this port to collect host information from GlobalProtect agents and perform host information profile (HIP) checks.
4501	UDP	Used for IPSec tunnel connections between GlobalProtect agents and gateways.

For tips on how to use a loopback interface to provide access to GlobalProtect on different ports and addresses, refer to [Can GlobalProtect Portal Page be Configured to be Accessed on any Port?](#).

## Ports Used for User-ID

**User-ID** is a feature that enables mapping of user IP addresses to usernames and group memberships, enabling user- or group-based policy and visibility into user activity on your network (for example, to be able to quickly track down a user who may be the victim of a threat). To perform this mapping, the firewall, the User-ID agent (either installed on a Windows-based system or the PAN-OS integrated agent running on the firewall), and/or the Terminal Services agent must be able to connect to directory services on your network to perform [Group Mapping](#) and [User Mapping](#). Additionally, if the agents are running on systems external to the firewall, they must be able to connect to the firewall to communicate the IP address to username mappings to the firewall. The following table lists the communication requirements for User-ID along with the port numbers required to establish connections.

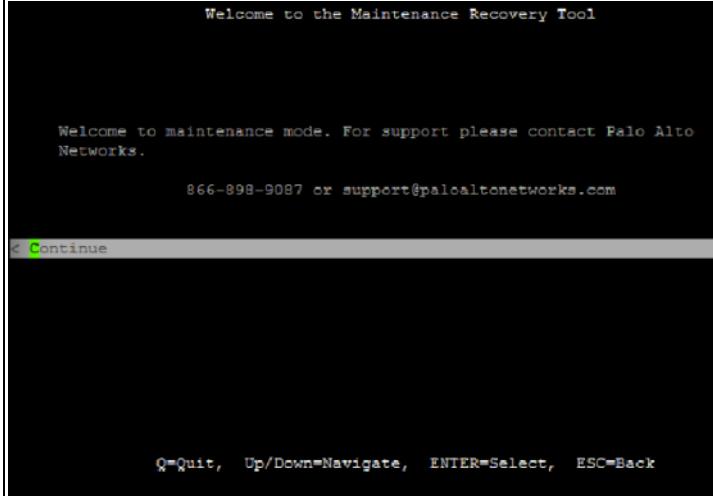
Destination Port	Protocol	Description
389	TCP	Port the firewall uses to connect to an LDAP server (plaintext or Start Transport Layer Security ( <a href="#">Start TLS</a> ) to <a href="#">Map Users to Groups</a> .
3268	TCP	Port the firewall uses to connect to an Active Directory global catalog server (plaintext or <a href="#">Start TLS</a> ) to <a href="#">Map Users to Groups</a> .
636	TCP	Port the firewall uses for LDAP over SSL connections with an LDAP server to <a href="#">Map Users to Groups</a> .
3269	TCP	Port the firewall uses for LDAP over SSL connections with an Active Directory global catalog server to <a href="#">Map Users to Groups</a> .
514	TCP	Port the PAN-OS integrated User-ID agent or Windows-based User-ID agent
514	UDP	listens on for authentication syslog messages if you <a href="#">Configure User-ID to Receive User Mappings from a Syslog Sender</a> .
6514	SSL	
5007	TCP	Port the firewall listens on for user mapping information from the <a href="#">User-ID</a> or <a href="#">Terminal Services</a> agent. The agent sends the IP address and username mapping along with a timestamp whenever it learns of a new or updated mapping. In addition, it connects to the firewall at regular intervals to refresh known mappings.
5006	TCP	Port the User-ID agent listens on for <a href="#">User-ID XML API</a> requests. The source for this communication is typically the system running a script that invokes the API.
88	UDP/TCP	Port the User-ID agent uses to authenticate to a Kerberos server. The device tries UDP first and falls back to TCP.
1812	UDP	Port the User-ID agent uses to authenticate to a RADIUS server.
49	TCP	Port the User-ID agent uses to authenticate to a TACACS+ server.

<b>Destination Port</b>	<b>Protocol</b>	<b>Description</b>
135	TCP	Port the User-ID agent uses to establish TCP-based WMI connections with the Microsoft Remote Procedure Call (RPC) Endpoint Mapper. The Endpoint Mapper then assigns the agent a randomly assigned port in the 49152-65535 port range. The agent uses this connection to make RPC queries for Exchange Server or AD server security logs, session tables. This is also the port used to access Terminal Services. The User-ID agent also uses this port to connect to client systems to perform <a href="#">Windows Management Instrumentation (WMI) probing</a> .
139	TCP	Port the User-ID agent uses to establish TCP-based NetBIOS connections to the AD server so that it can send RPC queries for security logs and session information. The User-ID agent also uses this port to connect to client systems for <a href="#">NetBIOS probing</a> (supported on the Windows-based User-ID agent only).
445	TCP	Port the User-ID agent uses to connect to the Active Directory (AD) using TCP-based SMB connections to the AD server for access to user logon information (print spooler and Net Logon).

# Reset the Firewall to Factory Default Settings

Resetting the firewall to factory defaults will result in the loss of all configuration settings and logs.

## Reset the Firewall to Factory Default Settings

<p><b>Step 1</b> Set up a console connection to the firewall.</p>	<ol style="list-style-type: none"><li>1. Connect a serial cable from your computer to the Console port and connect to the firewall using terminal emulation software (9600-8-N-1).  If your computer does not have a 9-pin serial port, use a USB-to-serial port connector.</li><li>2. Enter your login credentials.</li><li>3. Enter the following CLI command: <code>debug system maintenance-mode</code> The firewall will reboot in the maintenance mode.</li></ol>
<p><b>Step 2</b> Reset the system to factory default settings.</p>	<ol style="list-style-type: none"><li>1. When the device reboots, press <code>Enter</code> to continue to the maintenance mode menu. <p>Welcome to the Maintenance Recovery Tool</p><p>Welcome to maintenance mode. For support please contact Palo Alto Networks.</p><p>866-898-9087 or support@paloaltonetworks.com</p><p>&lt; Continue</p><p>Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back</p></li><li>2. Select <code>Factory Reset</code> and press <code>Enter</code>.</li><li>3. Select <code>Factory Reset</code> and press <code>Enter</code> again. The firewall will reboot without any configuration settings. The default username and password to log in to the firewall is <code>admin/admin</code>. To perform initial configuration on the firewall and to set up network connectivity, see <a href="#">Integrate the Firewall into Your Management Network</a>.</li></ol>





# Authentication

---

Many of the services that Palo Alto Networks devices provide require authentication, including administrator access to the web interface and end user access to Captive Portal, GlobalProtect portals, and GlobalProtect gateways. The authentication methods that you can configure vary by service, and can include Kerberos single sign-on (SSO), external authentication services, certificates and certificate profiles, local database accounts, RADIUS Vendor-Specific Attributes (VSAs), and NT LAN Manager (NTLM).

The following topics describe authentication methods that are common to most device services, procedures to configure them, how to test authentication profiles, and how to troubleshoot authentication issues:

- ▲ [Configure Kerberos Single Sign-On](#)
- ▲ [Configure External Authentication](#)
- ▲ [Test Authentication Server Connectivity](#)
- ▲ [Troubleshoot Authentication Issues](#)

# Configure Kerberos Single Sign-On

Palo Alto Networks devices support Kerberos V5 single sign-on (SSO) to authenticate administrators to the web interface and end users to Captive Portal. A network that supports Kerberos SSO prompts a user to log in only for initial access to the network (for example, logging in to Microsoft Windows). After this initial login, the user can access any browser-based service in the network (for example, the firewall web interface) without having to log in again until the SSO session expires. (Your Kerberos administrator sets the duration of SSO sessions.) If you enable both Kerberos SSO and [external authentication services](#) (for example, a RADIUS server), the device first tries SSO and, only if that fails, falls back to the external service for authentication.

To support Kerberos SSO, your network requires:

- A Kerberos infrastructure, including a key distribution center (KDC) with an authentication server (AS) and ticket-granting service (TGS).
- A Kerberos account for each Palo Alto Networks device that will authenticate users. An account is required to create a Kerberos keytab, which is a file that contains the principal name and hashed password of the device. The SSO process requires the keytab.

## Configure Kerberos Single Sign-On

Step 1 Create a Kerberos keytab.	<ol style="list-style-type: none"> <li>1. Log in to the KDC and open a command prompt.</li> <li>2. Enter the following command, where &lt;principal_name&gt;, &lt;password&gt;, and &lt;algorithm&gt; are variables. The Kerberos principal name and password are of the device, not the user.  <pre>ktpass /princ &lt;principal_name&gt; /pass &lt;password&gt; /crypto &lt;algorithm&gt; /ptype KRB5_NT_PRINCIPAL /out &lt;file_name&gt;.keytab</pre> </li> </ol> <p> If the device is in FIPS or CC mode, the algorithm must be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96. Otherwise, you can also use des3-cbc-sha1 or arcfour-hmac. To use an Advanced Encryption Standard (AES) algorithm, the functional level of the KDC must be Windows Server 2008 or later and you must enable AES encryption for the device account.</p> <p>The algorithm in the keytab must match the algorithm in the service ticket that the TGS issues to clients. Your Kerberos administrator determines which algorithms the service tickets use.</p>
Step 2 Import the keytab into an authentication profile.	<p><a href="#">Configure an authentication profile.</a></p> <ol style="list-style-type: none"> <li>1. Enter the <b>Kerberos Realm</b> (usually the DNS domain of the users, except that the realm is uppercase).</li> <li>2. <b>Import</b> the <b>Kerberos Keytab</b> that you created for the device.</li> </ol>
Step 3 Assign the authentication profile to the user account or device service.	<ul style="list-style-type: none"> <li>• <a href="#">Configure an administrator account</a>.</li> <li>• <a href="#">Configure Captive Portal</a>.</li> </ul>

## Configure External Authentication

Palo Alto Networks devices can use external servers for many services that require authentication, including administrator access to the web interface and end user access to Captive Portal, GlobalProtect portals and GlobalProtect gateways. The server protocols that Palo Alto Networks devices support include Lightweight Directory Access Protocol (LDAP), Kerberos, Terminal Access Controller Access-Control System Plus (TACACS+), and Remote Authentication Dial-In User Service (RADIUS). If you enable both external authentication and [Kerberos single sign-on \(SSO\)](#), the device first tries SSO and, only if that fails, falls back to the external server for authentication. To configure external authentication, you create an authentication server profile, assign it to an authentication profile, and then enable authentication for an administrator account or device service by assigning the authentication profile to it.

- ▲ [Configure Authentication Server Profiles](#)
- ▲ [Configure an Authentication Profile and Sequence](#)
- ▲ [Enable External Authentication for Users and Services](#)

## Configure Authentication Server Profiles

- ▲ Configure a RADIUS Server Profile
- ▲ RADIUS Vendor-Specific Attributes for Palo Alto Networks Devices
- ▲ Configure a TACACS+ Server Profile
- ▲ Configure an LDAP Server Profile
- ▲ Configure a Kerberos Server Profile
- ▲ Set CHAP and PAP Authentication for RADIUS and TACACS+ Servers

## Configure a RADIUS Server Profile

You can configure Palo Alto Networks devices to use a RADIUS server for authenticating users, managing administrator accounts (if they are not local), and collecting RADIUS Vendor-Specific Attributes (VSAs) from GlobalProtect clients. To use a RADIUS server for managing administrator accounts or collecting GlobalProtect clients VSAs, you must define VSAs on the RADIUS server. For details, see the list of supported [RADIUS Vendor-Specific Attributes for Palo Alto Networks Devices](#).



By default, when authenticating to the RADIUS server, the firewall or Panorama first tries Challenge-Handshake Authentication Protocol (CHAP) and falls back to Password Authentication Protocol (PAP) under certain conditions. Optionally, you can override this automatic protocol selection and configure the firewall or Panorama to always use a specific protocol. For details, see [Set CHAP and PAP Authentication for RADIUS and TACACS+ Servers](#).

When sending authentication requests to a RADIUS server, the firewall and Panorama use the authentication profile name as the network access server (NAS) identifier, even if the profile is assigned to an authentication sequence for the service that initiates the authentication process.

### Configure a RADIUS Server Profile

**Step 1** Select **Device > Server Profiles > RADIUS** and click **Add**.

**Step 2** Enter a **Profile Name** to identify the server profile.

**Step 3** For a firewall with more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where the profile is available.

**Step 4** For the **Timeout**, enter an interval in seconds after which an authentication request times out (range is 1-30, default is 3).

**Step 5** Enter the number of automatic **Retries** following a **Timeout** before the request fails (range is 1-5, default is 3).

**Step 6** For each RADIUS server, click **Add** and enter a **Name** (to identify the server), server IP address or FQDN (**RADIUS Server** field), **Secret/Confirm Secret** (a key to encrypt passwords), and server **Port** for authentication requests (default is 1812).

**Step 7** Click **OK** and **Commit**.

## RADIUS Vendor-Specific Attributes for Palo Alto Networks Devices

Palo Alto Networks devices support the following RADIUS Vendor-Specific Attributes (VSAs). To define VSAs on a RADIUS server, you must specify the vendor code (25461 for Palo Alto Networks devices) and the VSA name and number. Some VSAs also require a value.

Name	Number	Value
<b>VSAs for administrator account management and authentication</b>		
PaloAlto-Admin-Role	1	A default (dynamic) administrative role name or a custom administrative role name on the firewall.
PaloAlto-Admin-Access-Domain	2	The name of an access domain for firewall administrators (configured in the <b>Device &gt; Access Domains</b> page). Define this VSA if the firewall has multiple virtual systems.
PaloAlto-Panorama-Admin-Role	3	A default (dynamic) administrative role name or a custom administrative role name on Panorama.
PaloAlto-Panorama-Admin-Access-Domain	4	The name of an access domain for Device Group and Template administrators (configured in the <b>Panorama &gt; Access Domains</b> page).
PaloAlto-User-Group	5	The name of a user group that an authentication profile references.
<b>VSAs forwarded from GlobalProtect clients to the RADIUS server</b>		
PaloAlto-User-Domain	6	Don't specify a value when you define these VSAs.
PaloAlto-Client-Source-IP	7	
PaloAlto-Client-OS	8	
PaloAlto-Client-Hostname	9	
PaloAlto-GlobalProtect-Client-Version	10	

## Configure a TACACS+ Server Profile

Terminal Access Controller Access-Control System Plus (TACACS+) protocol provides better [Authentication](#) security than RADIUS because it encrypts usernames and passwords (instead of just passwords), and is also more reliable (it uses TCP instead of UDP).



By default, when authenticating to the TACACS+ server, the firewall or Panorama first tries Challenge-Handshake Authentication Protocol (CHAP) and falls back to Password Authentication Protocol (PAP) under certain conditions. Optionally, you can override this automatic protocol selection and configure the firewall or Panorama to always use a specific protocol. For details, see [Set CHAP and PAP Authentication for RADIUS and TACACS+ Servers](#).

### Configure a TACACS+ Server Profile

**Step 1** Select **Device > Server Profiles > TACACS+** and click **Add**.

**Step 2** Enter a **Profile Name** to identify the server profile.

**Step 3** For a firewall with more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where the profile is available.

**Step 4** For the **Timeout**, enter an interval in seconds after which an authentication request times out (range is 1-20, default is 3).

**Step 5** Select the **Use single connection for all authentication** check box to use the same TCP session for all authentications that use this profile. This option improves performance by avoiding the need to start and end a separate TCP session for each authentication. The check box is cleared by default.

**Step 6** For each TACACS+ server, click **Add** and enter a **Name** (to identify the server), server IP address or FQDN (**TACACS+ Server** field), **Secret/Confirm Secret** (a key to encrypt usernames and passwords), and server **Port** for authentication requests (default is 49).

**Step 7** Click **OK** and **Commit**.

## Configure an LDAP Server Profile

An LDAP server profile enables you to:

- Authenticate administrators and end users of Palo Alto Networks devices.
- Define security rules based on user or group. The LDAP server profile instructs the firewall how to connect and authenticate to the server and how to search the directory for user and group information. You must also configure User-ID to [Map Users to Groups](#). Then you can select users or groups when defining policy rules.

### Configure an LDAP Server Profile

**Step 1** Select **Device > Server Profiles > LDAP** and click **Add**.

**Step 2** Enter a **Profile Name** to identify the server profile.

**Step 3** For a firewall with more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where the profile is available.

**Step 4** For each LDAP server (up to four), click **Add** and enter a **Name** (to identify the server), server IP address (**LDAP Server** field), and server **Port** (default 389).

**Step 5** Select the server **Type** from the drop-down: **active-directory**, **e-directory**, **sun**, or **other**.

**Step 6** If you want the device to use SSL or TLS for a more secure connection with the directory server, select the **Require SSL/TLS secured connection** check box (it is selected by default). The protocol that the device uses depends on the server **Port**:

- 389 (default)—TLS (Specifically, the device uses the [Start TLS operation](#), which upgrades the initial plaintext connection to TLS.)
- 636—SSL
- Any other port—The device first tries to use TLS. If the directory server doesn't support TLS, the device falls back to SSL.

**Step 7** To improve security, you can select the **Verify Server Certificate for SSL sessions** check box (it is cleared by default) so that the device verifies the certificate that the directory server presents for SSL/TLS connections. If the verification fails, the connection fails. To enable verification, you must also select the **Require SSL/TLS secured connection** check box. The device verifies the certificate in two respects:

- The certificate is trusted and valid. For the device to trust the certificate, its root certificate authority (CA) and any intermediate certificates must be in the certificate store under **Device > Certificate Management > Certificates > Device Certificates**. Import the certificate if necessary: see [Import a Certificate and Private Key](#).
- The certificate name must match the host **Name** of the LDAP server. The device first checks the certificate attribute Subject AltName for matching, then tries the attribute Subject DN. If the certificate uses the FQDN of the directory server, you must enter that FQDN in the **LDAP Server** field for the name matching to succeed.

**Step 8** Click **OK** and **Commit**.

## Configure a Kerberos Server Profile

A Kerberos server profile enables users to natively authenticate to an Active Directory domain controller or a Kerberos V5-compliant [authentication server](#). This authentication method is interactive, requiring users to enter usernames and passwords, in contrast with [Kerberos single sign-on \(SSO\)](#), which involves transparent authentication.



To use a Kerberos server for authentication, the server must be accessible over an IPv4 address. IPv6 addresses are not supported.

### Configure a Kerberos Server Profile

**Step 1** Select **Device > Server Profiles > Kerberos** and click **Add**.

**Step 2** Enter a **Profile Name** to identify the server profile.

**Step 3** For a firewall with more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where the profile is available.

**Step 4** For each Kerberos server, click **Add** and enter a **Name** (to identify the server), server IPv4 address or FQDN (**Kerberos Server** field), and an optional **Port** number for communication with the server (default 88).

**Step 5** Click **OK** and **Commit**.

## Set CHAP and PAP Authentication for RADIUS and TACACS+ Servers

When you configure a Palo Alto Networks device to use [RADIUS](#) or [TACACS+](#) server authentication for a particular service (for example, Captive Portal), the device first tries to authenticate to the server using Challenge-Handshake Authentication Protocol (CHAP). The device falls back to Password Authentication Protocol (PAP) if the server rejects the CHAP request. This will happen if, for example, the server doesn't support CHAP or isn't configured for CHAP. CHAP is the preferred protocol because it is more secure than PAP. After the device falls back to PAP for a particular RADIUS or TACACS+ server, the device uses only PAP in subsequent attempts to authenticate to that server. PAN-OS records a fall back to PAP as a medium severity event in the System logs. If you modify any fields in the RADIUS or TACACS+ server profile and then commit the changes, the device reverts to first trying CHAP for that server.

In Release 7.0.6 and later releases, you can force the firewall or Panorama to always use a specific protocol for authenticating to the RADIUS or TACACS+ server by entering the following operational CLI command (the `auto` option reverts to the default automatic selection):

```
set authentication radius-auth-type [ auto | chap | pap ]
```

 When configuring a RADIUS or TACACS+ server for CHAP, you must define user accounts with [reversibly encrypted passwords](#). Otherwise, CHAP authentication will fail.

## Configure an Authentication Profile and Sequence

An authentication profile defines the authentication service that validates the login credentials of firewall or Panorama administrators and Captive Portal or GlobalProtect end users. The authentication service can be a local database (firewalls only), an external service (RADIUS, TACACS+, LDAP, or Kerberos server), or [Kerberos single sign-on \(SSO\)](#).

Some networks have multiple databases for different users and user groups (for example, TACACS+ and LDAP). To authenticate users in such cases, configure an authentication sequence, which is a ranked order of authentication profiles that the firewall or Panorama matches a user against during login. The firewall or Panorama checks against each profile in sequence until one successfully authenticates the user (the firewall always checks the local database first if the sequence includes one). A user is denied access only if authentication fails for all the profiles in the authentication sequence.

Configure an Authentication Profile and Sequence	
<b>Step 1</b> Create a Kerberos keytab.  Required if the device will use Kerberos SSO authentication.	<a href="#">Create a Kerberos keytab</a> . A keytab is a file that contains Kerberos account information (principal name and hashed password) for the device.
<b>Step 2</b> Configure an external server profile.  Required if the device will use an external service for authentication.	<ul style="list-style-type: none"><li>• <a href="#">Configure a RADIUS Server Profile</a>.</li><li>• <a href="#">Configure a TACACS+ Server Profile</a>.</li><li>• <a href="#">Configure an LDAP Server Profile</a>.</li><li>• <a href="#">Configure a Kerberos Server Profile</a>.</li></ul>

**Configure an Authentication Profile and Sequence (Continued)**

<p><b>Step 3</b> Configure an authentication profile.</p> <p>Define one or both of the following authentication phases:</p> <ul style="list-style-type: none"><li>• Kerberos SSO—The firewall or Panorama first tries SSO authentication. If that fails, it falls back to the specified authentication <b>Type</b>.</li><li>• Local database or external authentication—The firewall or Panorama prompts the user to enter login credentials, and uses its local database (firewalls only) or an external service to authenticate the user.</li></ul>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Authentication Profile</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> to identify the authentication profile.</li><li>3. If the firewall has more than one virtual system (vsys), select a <b>Location</b> (a vsys or <b>Shared</b>) where the profile is available.</li><li>4. In the <b>Authentication</b> tab, select the authentication <b>Type</b>. If you select <b>RADIUS</b>, <b>TACACS+</b>, <b>LDAP</b>, or <b>Kerberos</b>, select the authentication <b>Server Profile</b> from the drop-down.  If the <b>Type</b> is <b>LDAP</b>, define the <b>Login Attribute</b>. For Active Directory, enter <b>sAMAccountName</b> as the value.</li><li>5. (Optional) Specify <b>User Domain</b> and <b>Username Modifier</b> options as follows to modify the domain/username string that the user will enter during login. This is useful when the authentication service requires the string in a particular format and you don't want to rely on users to correctly enter the domain.<ul style="list-style-type: none"><li>• To send only the unmodified user input, leave the <b>User Domain</b> blank (the default) and set the <b>Username Modifier</b> to the variable <b>%USERINPUT%</b> (the default).</li><li>• To prepend a domain to the user input, enter a <b>User Domain</b> and set the <b>Username Modifier</b> to <b>%USERDOMAIN%\%USERINPUT%</b>.</li><li>• To append a domain to the user input, enter a <b>User Domain</b> and set the <b>Username Modifier</b> to <b>%USERINPUT%@%USERDOMAIN%</b>.</li></ul></li><li>6. If you want to enable Kerberos SSO, enter the <b>Kerberos Realm</b> (usually the DNS domain of the users, except that the realm is uppercase) and <b>Import</b> the <b>Kerberos Keytab</b> that you created for the device.</li><li>7. Select the <b>Advanced</b> tab and, in the Allow List, click <b>Add</b> to select the users and groups that can authenticate with this profile. You can select users/groups from the local database or, if you configured an LDAP server profile, from an LDAP-based directory service such as Active Directory. Selecting <b>all</b> allows every user to authenticate. By default, the list is empty, meaning no users can authenticate.  You can also create and allow custom groups based on LDAP filters: see <a href="#">Map Users to Groups</a>.</li><li>8. Enter the number of <b>Failed Attempts</b> (0-10) to log in that the device allows before locking out the user. The default value 0 means there is no limit.</li><li>9. Enter the <b>Lockout Time</b> (0-60), which is the number of minutes for which the device locks out the user after reaching the <b>Failed Attempts</b> limit. The default value 0 means the lockout applies until an administrator unlocks the user account.</li><li>10. Click <b>OK</b> to save the authentication profile.</li></ol>
---	--

**Configure an Authentication Profile and Sequence (Continued)**

<b>Step 4</b> Configure an authentication sequence.  Required if you want the firewall or Panorama to try multiple authentication profiles to authenticate users. The firewall or Panorama evaluates the profiles in top-to-bottom order until one profile successfully authenticates the user.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Authentication Sequence</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> to identify the authentication sequence.</li><li>3. If the firewall has more than one virtual system (vsys), select a <b>Location</b> (a vsys or <b>Shared</b>) where the sequence is available.  To expedite the authentication process, the best practice is to select the <b>Use domain to determine authentication profile</b> check box: the device will match the domain name that a user enters during login with the <b>User Domain</b> or <b>Kerberos Realm</b> of an authentication profile in the sequence, and then use that profile to authenticate the user. If the device doesn't find a match, or if you clear the check box, the device tries the profiles in the top-to-bottom sequence.</li><li>4. For each authentication profile to include, click <b>Add</b> and select from the drop-down. To change the evaluation order of the profiles, select a profile and click <b>Move Up</b> or <b>Move Down</b>.</li><li>5. Click <b>OK</b> to save the authentication sequence.</li></ol>
<b>Step 5</b> Assign the authentication profile or sequence.	Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.

## Enable External Authentication for Users and Services

Palo Alto Networks devices can use [external services](#) to authenticate administrators and end users.

<b>Enable External Authentication</b>	
<b>Step 1</b> Configure an external server profile.	<ul style="list-style-type: none"><li>• <a href="#">Configure a RADIUS Server Profile</a>.</li><li>• <a href="#">Configure a TACACS+ Server Profile</a>.</li><li>• <a href="#">Configure an LDAP Server Profile</a>.</li><li>• <a href="#">Configure a Kerberos Server Profile</a>.</li></ul>
<b>Step 2</b> Assign the server profile to an authentication profile.  Optionally, you can assign multiple authentication profiles to an authentication sequence.	<ol style="list-style-type: none"><li>1. <a href="#">Configure an Authentication Profile and Sequence</a>.</li><li>2. <a href="#">Test Authentication Server Connectivity</a>.</li></ol>
<b>Step 3</b> Assign the authentication profile or sequence to an administrator account or to a firewall service for end users.	<ul style="list-style-type: none"><li>• Administrators: <a href="#">Configure an Administrative Account</a>.</li><li>• End user services:<ul style="list-style-type: none"><li>• <a href="#">Configure Captive Portal</a>.</li><li>• <a href="#">Configure the GlobalProtect portal</a>.</li><li>• <a href="#">Configure the GlobalProtect gateway</a>.</li></ul></li></ul>

## Test Authentication Server Connectivity

After you configure an authentication profile on a Palo Alto Networks firewall or Panorama manager, you can use the test authentication feature to determine if the device can communicate with the back-end authentication server and if the authentication request was successful. You can additionally test authentication profiles used for GlobalProtect and Captive Portal authentication. You can perform authentication tests on the candidate configuration, so that you know the configuration is correct before committing.

Authentication server connectivity testing is supported for local database, RADIUS, TACACS+, LDAP, and Kerberos authentication.

The following topics describe how to use the test authentication command and provides use case examples:

- ▲ [Run the Test Authentication Command](#)
- ▲ [Local Database Authentication Profile Use Case](#)
- ▲ [RADIUS Authentication Profile Use Case](#)
- ▲ [TACACS+ Authentication Profile Use Case](#)
- ▲ [LDAP Authentication Profile Use Case](#)
- ▲ [Kerberos Authentication Profile Use Case](#)

## Run the Test Authentication Command

### Run the Test Authentication Command

**Step 1** On the PAN-OS firewall or Panorama server, [Configure an authentication profile](#). You do not need to commit the authentication or server profile configuration prior to testing.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access.

This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Test an authentication profile by entering the following command:

```
admin@PA-3060> test authentication authentication-profile <authentication-profile-name> username <username> password
```

For example, to test an authentication profile named my-profile for a user named bsimpson, run the following command:

```
admin@PA-3060> test authentication authentication-profile my-profile username bsimpson password
```



When entering authentication profile names and server profile names in the test command, the names are case sensitive. Also, if the authentication profile has a username modifier defined, you must enter the modifier with the username. For example, if you add the username modifier %USERINPUT%@%USERDOMAIN% for a user named bsimpson and the domain name is mydomain.com, enter bsimpson@mydomain.com as the username. This will ensure that the correct credentials are sent to the authentication server. In this example, mydomain.com is the domain that you define in the User Domain field in the Authentication profile.

**Step 5** View the output of the test results.

If the authentication profile is configured correctly, the output displays **Authentication succeeded**. If there is a configuration issue, the output displays information to help you troubleshoot the configuration.

For example use cases on the supported authentication profile types, see [Local Database Authentication Profile Use Case](#).



The output results vary based on several factors related to the authentication type that you are testing as well as the type of issue. For example, RADIUS and TACACS+ use different underlying libraries, so the same issue that exists for both of these types will produce different errors. Also, if there is a network problem, such as using an incorrect port or IP address in the authentication server profile, the output error is not specific. This is because the test command cannot perform the initial handshake between the firewall and the authentication server to determine details about the issue.

## Local Database Authentication Profile Use Case

The following example shows how to test a Local Database authentication profile named LocalDB for a user named User1-LocalDB and how to troubleshoot error conditions that arise. For details on using the test authentication command, see [Run the Test Authentication Command](#).

### Local Database Authentication Profile Test Example

**Step 1** On the PAN-OS firewall, ensure that you have an administrator configured with the type Local Database. For information on administrator accounts, refer to [Manage Firewall Administrators](#).

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access.

This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile LocalDB-Profile username User1-LocalDB password
```

**Step 5** When prompted, enter the password for the User1-LocalDB account. The following output shows that the test failed:

Allow list check error:

```
Do allow list check before sending out authentication request...
```

```
User User1-LocalDB is not allowed with authentication profile LocalDB-Profile
```

In this case, the last line of the output shows that the user is not allowed, which indicates a configuration problem in the authentication profile.

**Step 6** To resolve this issue, modify the authentication profile and add the user to the Allow List.

1. On the firewall, select **Device > Authentication Profile** and modify the profile named LocalDB-Profile.
2. Click the **Advanced** tab and add User1-LocalDB to the Allow List.
3. Click **OK** to save the change.

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
```

```
name "User1-LocalDB" has an exact match in allow list
```

```
Authentication by Local User Database for user "User1-LocalDB"
```

```
Authentication succeeded for Local User Database user "User1-LocalDB"
```

## RADIUS Authentication Profile Use Case

The following example shows how to test a RADIUS profile named RADIUS-Profile for a user named User2-RADIUS and how to troubleshoot error conditions that arise. For details on using the test authentication command, see [Run the Test Authentication Command](#).

### RADIUS Authentication Profile Test Example

**Step 1** On the PAN-OS firewall, [Configure a RADIUS Server Profile](#) and [Configure an authentication profile](#). In the authentication profile, you select the new RADIUS server profile in the **Server Profile** drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access.

This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile RADIUS-Profile username  
User2-RADIUS password
```

**Step 5** When prompted, enter the password for the User2-RADIUS account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...  
name "User2-RADIUS" is in group "all"  
Authentication to RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"  
Egress: 10.5.104.98  
Authentication type: CHAP  
Now send request to remote server ...  
RADIUS error: Invalid RADIUS response received - Bad MD5  
Authentication failed against RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"
```

In this case, the output shows **Bad MD5**, which indicates that there may be an issue with the secret defined in the RADIUS server profile.

---

**RADIUS Authentication Profile Test Example**

---

**Step 6** To resolve this issue, modify the RADIUS server profile and ensure that the secret defined on the RADIUS server matches the secret in the server profile.

1. On the firewall, select **Device > Server Profiles > RADIUS** and modify the profile named RADIUS-Profile.
  2. In the Servers section, locate the RADIUS server and modify the **Secret** field.
  3. Type in the correct secret and then retype to confirm.
  4. Click **OK** to save the change.
- 

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...

name "User2-RADIUS" is in group "all"

Authentication to RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"

Egress: 10.5.104.98

Authentication type: CHAP

Now send request to remote server ...

RADIUS CHAP auth request is NOT accepted, try PAP next

Authentication type: PAP

Now send request to remote server ...

Authentication succeeded against RADIUS server at 10.5.104.99:1812 for user "User2-RADIUS"

Authentication succeeded for user "User2-RADIUS"
```

---

## TACACS+ Authentication Profile Use Case

The following example shows how to test a TACACS+ profile named TACACS-Profile for a user named User3-TACACS and how to troubleshoot error conditions that arise. For details on using the test authentication command, see [Run the Test Authentication Command](#).

### TACACS+ Authentication Profile Test Example

**Step 1** On the PAN-OS firewall, [Configure a TACACS+ Server Profile](#) and [Configure an authentication profile](#). In the authentication profile, you select the new TACACS+ server profile in the **Server Profile** drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access.

This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile TACACS-Profile username  
User3-TACACS password
```

---

**TACACS+ Authentication Profile Test Example**

---

- Step 5** When prompted, enter the password for the User3-TACASC account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User2-TACACS" is in group "all"
Authentication to TACACS+ server at '10.5.196.62' for user 'User2-TACACS'
Server port: 49, timeout: 30, flag: 0
Egress: 10.5.104.98
Attempting CHAP authentication ...
CHAP authentication request is created
Sending credential: xxxxxxx
Failed to send CHAP authentication request: Network read timed out
Attempting PAP authentication ...
PAP authentication request is created
Failed to send PAP authentication request: Network read timed out
Returned status: -1
Authentication failed against TACACS+ server at 10.5.196.62:49 for user User2-TACACS
Authentication failed for user "User2-TACACS"
```

The output shows error `Network read timed out`, which indicates that the TACACS+ server could not decrypt the authentication request. In this case, there may be an issue with the secret defined in the TACACS+ server profile.

- 
- Step 6** To resolve this issue, modify the TACACS+ server profile and ensure that the secret defined on the TACACS+ server matches the secret in the server profile.
1. On the firewall, select **Device > Server Profiles > TACACS+** and modify the profile named TACACS-Profile.
  2. In the Servers section, locate the TACACS+ server and modify the **Secret** field.
  3. Type in the correct secret and then retype to confirm.
  4. Click **OK** to save the change.
-

**TACACS+ Authentication Profile Test Example**

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...
name "User2-TACACS" is in group "all"
Authentication to TACACS+ server at '10.5.196.62' for user 'User2-TACACS'
Server port: 49, timeout: 30, flag: 0
Egress: 10.5.104.98
Attempting CHAP authentication ...
CHAP authentication request is created
Sending credential: xxxxxxx
CHAP authentication request is sent
Authentication succeeded!
Authentication succeeded for user "User2-TACACS"
```

## LDAP Authentication Profile Use Case

The following example shows how to test a LDAP authentication profile named LDAP-Profile for a user named User4-LDAP and how to troubleshoot error conditions that arise. For details on using the test authentication command, see [Run the Test Authentication Command](#).

### LDAP Authentication Profile Test Example

**Step 1** On the PAN-OS firewall, [Configure an LDAP Server Profile](#) and [Configure an authentication profile](#). In the authentication profile, you select the new LDAP server profile in the **Server Profile** drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access.

This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile LDAP-Profile username User4-LDAP password
```

**Step 5** When prompted, enter the password for the User4-LDAP account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User4-LDAP" is in group "all"
Authentication to LDAP server at 10.5.104.99 for user "User4-LDAP"
Egress: 10.5.104.98
Type of authentication: plaintext
Starting LDAP connection...
Succeeded to create a session with LDAP server
parse error of dn and attributes for user "User4-LDAP"
Authentication failed against LDAP server at 10.5.104.99:389 for user "User4-LDAP"
Authentication failed for user "User4-LDAP"
```

The output shows **parse error of dn and attributes for user User4-LDAP**, which indicates a BIND DN value issues in the LDAP server profile. In this case, a Domain Component (DC) value is incorrect.

### LDAP Authentication Profile Test Example

- Step 6** To resolve this issue, modify the LDAP server profile and ensure that the Bind DN DC value is correct by comparing the DC value with the DC value of the LDAP server.
1. On the firewall, select **Device > Server Profiles > LDAP** and modify the profile named LDAP-Profile.
  2. In the Server settings section, enter the correct value for the DC in the **Bind DN** field. In this case, the correct value for the DC is MGMT-GROUP
  3. Click **OK** to save the change.

- Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...

name "User4-LDAP" is in group "all"

Authentication to LDAP server at 10.5.104.99 for user "User4-LDAP"

Egress: 10.5.104.98

Type of authentication: plaintext

Starting LDAP connection...

Succeeded to create a session with LDAP server

DN sent to LDAP server: CN=User4-LDAP,CN=Users,DC=MGMT-GROUP,DC=local

User expires in days: never

Authentication succeeded for user "User4-LDAP"
```

## Kerberos Authentication Profile Use Case

The following example shows how to test a Kerberos profile named Kerberos-Profile for a user named User5-Kerberos and how to troubleshoot error conditions that arise. For details on using the test authentication command, see [Run the Test Authentication Command](#).

### Kerberos Authentication Profile Test Example

**Step 1** On the PAN-OS firewall, [Configure a Kerberos Server Profile](#) and [Configure an authentication profile](#). In the authentication profile, you select the new Kerberos server profile in the **Server Profile** drop-down.

**Step 2** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 3** (Firewalls with virtual systems configured) Define the target virtual system that the test command will access.

This is required on firewalls with multiple virtual systems (vsys) configured, so the test authentication command can locate the user (Global Protect or Captive Portal, for example) in the correct vsys.

To define the target vsys:

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, if the user is defined in vsys2, run the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



The **target-vsys** command is per-login session, so the system clears the option when you log off.

**Step 4** Run the following CLI command:

```
admin@PA-3060> test authentication authentication-profile Kerberos-Profile username User5-Kerberos password
```

**Step 5** When prompted, enter the password for the User5-Kerberos account. The following output shows that the test failed:

```
Do allow list check before sending out authentication request...
name "User5-Kerberos" is in group "all"
Authentication to KERBEROS server at '10.5.104.99' for user 'User5-Kerberos'
Realm: 'Bad-MGMT-GROUP.LOCAL'
Egress: 10.5.104.98
KERBEROS configuration file is created
KERBEROS authcontext is created. Now authenticating ...
Kerberos principal is created
Sending authentication request to KDC...
Authentication failure: Wrong realm: 'Bad-MGMT-GROUP.LOCAL' (code: -1765328316)
Authentication failed against KERBEROS server at 10.5.104.99:88 for user "User5-Kerberos"
Authentication failed for user "User5-Kerberos"
```

In this case, the output shows **wrong realm**, which indicates that the Kerberos realm has an incorrect value.

### Kerberos Authentication Profile Test Example

**Step 6** To resolve this issue, modify the Kerberos server profile and ensure that the Realm value is correct by comparing the realm name on the Kerberos server.

1. On the firewall, select **Device > Authentication Profiles** and modify the profile named Kerberos-Profile.
2. In the Kerberos Realm field, enter the correct value. In this case, the correct realm is mgmt-group.local.
3. Click **OK** to save the change.

**Step 7** Run the test command again. The following output shows that the test is successful:

```
Do allow list check before sending out authentication request...

name "User5-Kerberos" is in group "all"

Authentication to KERBEROS server at '10.5.104.99' for user 'User5-Kerberos'

Realm: 'MGMT-GROUP.LOCAL'

Egress: 10.5.104.98

KERBEROS configuration file is created

KERBEROS authcontext is created. Now authenticating ...

Kerberos principal is created

Sending authentication request to KDC...

Authentication succeeded!

Authentication succeeded for user "User5-Kerberos"
```

## Troubleshoot Authentication Issues

When users fail to authenticate to a Palo Alto Networks device, or the [Authentication](#) process takes longer than expected, analyzing authentication-related information can help you determine whether the failure or delay resulted from:

- User behavior—for example, users are locked out after entering the wrong credentials or a high volume of users are simultaneously attempting access.
- System or network issues—for example, an authentication server is inaccessible.
- Configuration issues—for example, the Allow List of an authentication profile doesn't have all the users it should have.

The following CLI commands display information that can help you troubleshoot these issues:

Task	Command
<p>Use the <code>show authentication locked-users</code> command to display the number of locked user accounts associated with the authentication profile (<code>auth-profile</code> option), authentication sequence (<code>is-seq</code> option), or virtual system (<code>vsys</code> option).</p> <p> To unlock users, use the following operational command:</p> <pre>request authentication [unlock-admin   unlock-user]</pre>	<pre>show authentication locked-users {     vsys &lt;value&gt;       auth-profile &lt;value&gt;       is-seq         {yes   no}         {auth-profile   vsys} &lt;value&gt; }</pre>

Task	Command
<p>Use the <code>debug authentication</code> command to troubleshoot authentication events.</p> <p>Use the <code>show</code> options to display authentication request statistics and the current debugging level:</p> <ul style="list-style-type: none"> <li>• <code>show</code> displays the current debugging level for the authentication service (<code>authd</code>).</li> <li>• <code>show-active-requests</code> displays the number of active checks for authentication requests, allow lists, and locked user accounts.</li> <li>• <code>show-pending-requests</code> displays the number of pending checks for authentication requests, allow lists, and locked user accounts.</li> <li>• <code>connection-show</code> displays authentication request and response statistics for all authentication servers or for a specific protocol type.</li> </ul> <p>Use the <code>connection-debug</code> options to enable or disable authentication debugging:</p> <ul style="list-style-type: none"> <li>• Use the <code>on</code> option to enable or the <code>off</code> option to disable debugging for <code>authd</code>.</li> <li>• Use the <code>connection-debug-on</code> option to enable or the <code>connection-debug-off</code> option to disable debugging for all authentication servers or for a specific protocol type.</li> </ul>	<pre>debug authentication {   on {debug   dump   error   info   warn}     show     show-active-requests     show-pending-requests     connection-show     {     connection-id       protocol-type     {       Kerberos connection-id &lt;value&gt;         LDAP connection-id &lt;value&gt;         RADIUS connection-id &lt;value&gt;         TACACS+ connection-id &lt;value&gt;       }   }   connection-debug-on     {     connection-id       debug-prefix       protocol-type     {       Kerberos connection-id &lt;value&gt;         LDAP connection-id &lt;value&gt;         RADIUS connection-id &lt;value&gt;         TACACS+ connection-id &lt;value&gt;       }   }   connection-debug-off     {     connection-id       protocol-type     {       Kerberos connection-id &lt;value&gt;         LDAP connection-id &lt;value&gt;         RADIUS connection-id &lt;value&gt;         TACACS+ connection-id &lt;value&gt;       }   }   connection-debug-on }</pre>



# Certificate Management

---

---

The following topics describe the different keys and certificates that Palo Alto Networks® devices use, and how to obtain and manage them:

- ▲ [Keys and Certificates](#)
- ▲ [Certificate Revocation](#)
- ▲ [Certificate Deployment](#)
- ▲ [Set Up Verification for Certificate Revocation Status](#)
- ▲ [Configure the Master Key](#)
- ▲ [Obtain Certificates](#)
- ▲ [Export a Certificate and Private Key](#)
- ▲ [Configure a Certificate Profile](#)
- ▲ [Configure an SSL/TLS Service Profile](#)
- ▲ [Configure the Key Size for SSL Forward Proxy Server Certificates](#)
- ▲ [Revoke and Renew Certificates](#)
- ▲ [Secure Keys with a Hardware Security Module](#)

## Keys and Certificates

To ensure trust between parties in a secure communication session, Palo Alto Networks devices use digital certificates. Each certificate contains a cryptographic key to encrypt plaintext or decrypt ciphertext. Each certificate also includes a digital signature to authenticate the identity of the issuer. The issuer must be in the list of trusted certificate authorities (CAs) of the authenticating party. Optionally, the authenticating party verifies the issuer did not revoke the certificate (see [Certificate Revocation](#)).

Palo Alto Networks devices use certificates in the following applications:

- User authentication for Captive Portal, GlobalProtect™, Mobile Security Manager, and web interface access to a Palo Alto Networks device.
- Device authentication for GlobalProtect VPN (remote user-to-site or large scale).
- Device authentication for IPSec site-to-site VPN with Internet Key Exchange (IKE).
- Decrypting inbound and outbound SSL traffic.

A firewall decrypts the traffic to apply policy rules, then re-encrypts it before forwarding the traffic to the final destination. For outbound traffic, the firewall acts as a forward proxy server, establishing an SSL/TLS connection to the destination server. To secure a connection between itself and the client, the firewall uses a *signing certificate* to automatically generate a copy of the destination server certificate.

The following table describes the keys and certificates that Palo Alto Networks devices use. As a best practice, use different keys and certificates for each usage.

**Table: Palo Alto Networks Device Keys/Certificates**

Key/Certificate Usage	Description
Administrative Access	Secure access to device administration interfaces (HTTPS access to the web interface) requires a server certificate for the MGT interface (or a designated interface on the dataplane if the device does not use MGT) and, optionally, a certificate to authenticate the administrator.
Captive Portal	In deployments where Captive Portal identifies users who access HTTPS resources, designate a server certificate for the Captive Portal interface. If you configure Captive Portal to use certificates (instead of, or in addition to, username/password credentials) for user identification, designate a user certificate also. For more information on Captive Portal, see <a href="#">Map IP Addresses to Usernames Using Captive Portal</a> .
Forward Trust	For outbound SSL/TLS traffic, if a firewall acting as a forward proxy trusts the CA that signed the certificate of the destination server, the firewall uses the forward trust CA certificate to generate a copy of the destination server certificate to present to the client. To set the key size, see <a href="#">Configure the Key Size for SSL Forward Proxy Server Certificates</a> . For added security, store the key on a hardware security module (for details, see <a href="#">Secure Keys with a Hardware Security Module</a> ).
Forward Untrust	For outbound SSL/TLS traffic, if a firewall acting as a forward proxy does not trust the CA that signed the certificate of the destination server, the firewall uses the forward untrust CA certificate to generate a copy of the destination server certificate to present to the client.

Key/Certificate Usage	Description
SSL Inbound Inspection	The keys that decrypt inbound SSL/TLS traffic for inspection and policy enforcement. For this application, import onto the firewall a private key for each server that is subject to SSL/TLS inbound inspection. See <a href="#">Configure SSL Inbound Inspection</a> .
SSL Exclude Certificate	Certificates for servers to exclude from SSL/TLS decryption. For example, if you enable SSL decryption but your network includes servers for which the firewall should not decrypt traffic (for example, web services for your HR systems), import the corresponding certificates onto the firewall and configure them as SSL Exclude Certificates. See <a href="#">Configure Decryption Exceptions</a> .
GlobalProtect	All interaction among <a href="#">GlobalProtect</a> components occurs over SSL/TLS connections. Therefore, as part of the GlobalProtect deployment, deploy server certificates for all GlobalProtect portals, gateways, and Mobile Security Managers. Optionally, deploy certificates for authenticating users also.  Note that the GlobalProtect <a href="#">Large Scale VPN (LSVPN)</a> feature requires a CA signing certificate.
Site-to-Site VPNs (IKE)	In a site-to-site IPSec VPN deployment, peer devices use Internet Key Exchange (IKE) gateways to establish a secure channel. IKE gateways use certificates or preshared keys to authenticate the peers to each other. You configure and assign the certificates or keys when defining an IKE gateway on a firewall. See <a href="#">Site-to-Site VPN Overview</a> .
Master Key	The firewall uses a master key to encrypt all private keys and passwords. If your network requires a secure location for storing private keys, you can use an encryption (wrapping) key stored on a hardware security module (HSM) to encrypt the master key. For details, see <a href="#">Encrypt a Master Key Using an HSM</a> .
Secure Syslog	The certificate to enable secure connections between the firewall and a syslog server. See <a href="#">Syslog Field Descriptions</a> .
Trusted Root CA	The designation for a root certificate issued by a CA that the firewall trusts. The firewall can use a self-signed root CA certificate to automatically issue certificates for other applications (for example, <a href="#">SSL Forward Proxy</a> ).  Also, if a firewall must establish secure connections with other firewalls, the root CA that issues their certificates must be in the list of trusted root CAs on the firewall.

# Certificate Revocation

Palo Alto Networks devices use digital certificates to ensure trust between parties in a secure communication session. Configuring a device to check the revocation status of certificates provides additional security. A party that presents a revoked certificate is not trustworthy. When a certificate is part of a chain, the device checks the status of every certificate in the chain except the root CA certificate, for which the device cannot verify revocation status.

Various circumstances can invalidate a certificate before the expiration date. Some examples are a change of name, change of association between subject and certificate authority (for example, an employee terminates employment), and compromise (known or suspected) of the private key. Under such circumstances, the certificate authority that issued the certificate must revoke it.

Palo Alto Networks devices support the following methods for verifying certificate revocation status. If you configure both, the devices first try the OCSP method; if the OCSP server is unavailable, the devices use the CRL method.

- ▲ [Certificate Revocation List \(CRL\)](#)
- ▲ [Online Certificate Status Protocol \(OCSP\)](#)



In PAN-OS, certificate revocation status verification is an optional feature. It is a best practice to enable it for certificate profiles, which define user and device authentication for Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access to Palo Alto Network devices.

## Certificate Revocation List (CRL)

Each certificate authority (CA) periodically issues a certificate revocation list (CRL) to a public repository. The CRL identifies revoked certificates by serial number. After the CA revokes a certificate, the next CRL update will include the serial number of that certificate.

The Palo Alto Networks firewall downloads and caches the last-issued CRL for every CA listed in the trusted CA list of the firewall. Caching only applies to validated certificates; if a firewall never validated a certificate, the firewall cache does not store the CRL for the issuing CA. Also, the cache only stores a CRL until it expires.

The firewall supports CRLs only in Distinguished Encoding Rules (DER) format. If the firewall downloads a CRL in any other format—for example, Privacy Enhanced Mail (PEM) format—any revocation verification process that uses that CRL will fail when a user performs an activity that triggers the process (for example, sending outbound SSL data). The firewall will generate a system log for the verification failure. If the verification was for an SSL certificate, the firewall will also display the SSL Certificate Errors Notify response page to the user.

To use CRLs for verifying the revocation status of certificates used for the decryption of inbound and outbound SSL/TLS traffic, see [Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption](#).

To use CRLs for verifying the revocation status of certificates that authenticate users and devices, configure a certificate profile and assign it to the interfaces that are specific to the application: Captive Portal, GlobalProtect (remote user-to-site or large scale), site-to-site IPSec VPN, or web interface access to Palo Alto Networks devices. For details, see [Configure Revocation Status Verification of Certificates Used for User/Device Authentication](#).

## Online Certificate Status Protocol (OCSP)

When establishing an SSL/TLS session, clients can use Online Certificate Status Protocol (OCSP) to check the revocation status of the authentication certificate. The authenticating client sends a request containing the serial number of the certificate to the OCSP responder (server). The responder searches the database of the certificate authority (CA) that issued the certificate and returns a response containing the status (*good*, *revoked* or *unknown*) to the client. The advantage of the OCSP method is that it can verify status in real-time, instead of depending on the issue frequency (hourly, daily, or weekly) of CRLs.

The Palo Alto Networks firewall downloads and caches OCSP status information for every CA listed in the trusted CA list of the firewall. Caching only applies to validated certificates; if a firewall never validated a certificate, the firewall cache does not store the OCSP information for the issuing CA. If your enterprise has its own public key infrastructure (PKI), you can configure the firewall as an OCSP responder (see [Configure an OCSP Responder](#)).

To use OCSP for verifying the revocation status of certificates when the firewall functions as an SSL forward proxy, perform the steps under [Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption](#).

The following applications use certificates to authenticate users and/or devices: Captive Portal, GlobalProtect (remote user-to-site or large scale), site-to-site IPSec VPN, and web interface access to Palo Alto Networks devices. To use OCSP for verifying the revocation status of the certificates:

- Configure an OCSP responder.
- Enable the HTTP OCSP service on the firewall.
- Create or obtain a certificate for each application.
- Configure a certificate profile for each application.
- Assign the certificate profile to the relevant application.

To cover situations where the OCSP responder is unavailable, configure CRL as a fall-back method. For details, see [Configure Revocation Status Verification of Certificates Used for User/Device Authentication](#).

# Certificate Deployment

The basic approaches to deploy certificates for Palo Alto Networks devices are:

- **Obtain certificates from a trusted third-party CA**—The benefit of obtaining a certificate from a trusted third-party certificate authority (CA) such as VeriSign or GoDaddy is that end clients will already trust the certificate because common browsers include root CA certificates from well-known CAs in their trusted root certificate stores. Therefore, for applications that require end clients to establish secure connections with a Palo Alto Network device, purchase a certificate from a CA that the end clients trust to avoid having to pre-deploy root CA certificates to the end clients. (Some such applications are a GlobalProtect portal or GlobalProtect Mobile Security Manager.) However, note that most third-party CAs cannot issue signing certificates. Therefore, this type of certificate is not appropriate for applications (for example, SSL/TLS decryption and large-scale VPN) that require the firewall to issue certificates. See [Obtain a Certificate from an External CA](#).
- **Obtain certificates from an enterprise CA**—Enterprises that have their own internal CA can use it to issue certificates for firewall applications and import them onto the firewall. The benefit is that end clients probably already trust the enterprise CA. You can either generate the needed certificates and import them onto the firewall, or generate a certificate signing request (CSR) on the firewall and send it to the enterprise CA for signing. The benefit of this method is that the private key does not leave the firewall. An enterprise CA can also issue a signing certificate, which the firewall uses to automatically generate certificates (for example, for GlobalProtect large-scale VPN or sites requiring SSL/TLS decryption). See [Import a Certificate and Private Key](#).
- **Generate self-signed certificates**—You can [Create a Self-Signed Root CA Certificate](#) on the firewall and use it to automatically issue certificates for other firewall applications. Note that if you use this method to generate certificates for an application that requires an end client to trust the certificate, end users will see a certificate error because the root CA certificate is not in their trusted root certificate store. To prevent this, deploy the self-signed root CA certificate to all end user systems. You can deploy the certificates manually or use a centralized deployment method such as an Active Directory Group Policy Object (GPO).

# Set Up Verification for Certificate Revocation Status

To verify the revocation status of certificates, the firewall uses Online Certificate Status Protocol (OCSP) and/or certificate revocation lists (CRLs). For details on these methods, see [Certificate Revocation](#). If you configure both methods, the firewall first tries OCSP and only falls back to the CRL method if the OCSP responder is unavailable. If your enterprise has its own public key infrastructure (PKI), you can configure the firewall to function as the OCSP responder.

The following topics describe how to configure the firewall to verify certificate revocation status:

- ▲ [Configure an OCSP Responder](#)
- ▲ [Configure Revocation Status Verification of Certificates Used for User/Device Authentication](#)
- ▲ [Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption](#)

## Configure an OCSP Responder

To use Online Certificate Status Protocol (OCSP) for verifying the revocation status of certificates, you must configure the firewall to access an OCSP responder (server). The entity that manages the OCSP responder can be a third-party certificate authority (CA) or, if your enterprise has its own public key infrastructure (PKI), the firewall itself. For details on OCSP, see [Certificate Revocation](#).

Configure an OCSP Responder	
Step 1 Define an OCSP responder.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Certificate Management &gt; OCSP Responder</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> to identify the responder (up to 31 characters). The name is case-sensitive. It must be unique and use only letters, numbers, spaces, hyphens, and underscores.</li><li>3. If the device has more than one virtual system (vsys), select a <b>Location</b> (vsys or <b>Shared</b>) for the certificate.</li><li>4. In the <b>Host Name</b> field, enter the host name (recommended) or IP address of the OCSP responder. From this value, PAN-OS automatically derives a URL and adds it to the certificate being verified. If you configure the firewall itself as an OCSP responder, the host name must resolve to an IP address in the interface that the firewall uses for OCSP services (specified in <a href="#">Step 3</a>).</li><li>5. Click <b>OK</b>.</li></ol>
Step 2 Enable OCSP communication on the firewall.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Management</b>.</li><li>2. In the Management Interface Settings section, edit to select the <b>HTTP OCSP</b> check box, then click <b>OK</b>.</li></ol>

### Configure an OCSP Responder

<p><b>Step 3</b> Optionally, to configure the firewall itself as an OCSP responder, add an Interface Management Profile to the interface used for OCSP services.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b>.</li> <li>2. Click <b>Add</b> to create a new profile or click the name of an existing profile.</li> <li>3. Select the <b>HTTP OCSP</b> check box and click <b>OK</b>.</li> <li>4. Select <b>Network &gt; Interfaces</b> and click the name of the interface that the firewall will use for OCSP services. The OCSP <b>Host Name</b> specified in <a href="#">Step 1</a> must resolve to an IP address in this interface.</li> <li>5. Select <b>Advanced &gt; Other info</b> and select the Interface Management Profile you configured.</li> <li>6. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
--	--

## Configure Revocation Status Verification of Certificates Used for User/Device Authentication

The firewall uses certificates to authenticate users and devices for such applications as Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access to Palo Alto Networks devices. To improve security, it is a best practice to configure the firewall to verify the revocation status of certificates that it uses for device/user authentication.

### Configure Revocation Status Verification of Certificates Used for User/Device Authentication

<p><b>Step 1</b> Configure a <a href="#">Certificate Profile</a> for each application.</p>	<p>Assign one or more root CA certificates to the profile and select how the firewall verifies certificate revocation status. The common name (FQDN or IP address) of a certificate must match an interface to which you apply the profile in <a href="#">Step 2</a>. For details on the certificates that various applications use, see <a href="#">Keys and Certificates</a></p>
<p><b>Step 2</b> Assign the certificate profiles to the relevant applications.</p>	<p>The steps to assign a certificate profile depend on the application that requires it.</p>

## Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption

The firewall decrypts inbound and outbound SSL/TLS traffic to apply security rules and rules, then re-encrypts the traffic before forwarding it. (For details, see [SSL Inbound Inspection](#) and [SSL Forward Proxy](#).) You can configure the firewall to verify the revocation status of certificates used for decryption as follows.



Enabling revocation status verification for SSL/TLS decryption certificates will add time to the process of establishing the session. The first attempt to access a site might fail if the verification does not finish before the session times out. For these reasons, verification is disabled by default.

<b>Configure Revocation Status Verification of Certificates Used for SSL/TLS Decryption</b>	
<b>Step 1</b> Define the service-specific timeout intervals for revocation status requests.	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Session</b> and, in the Session Features section, select <b>Decryption Certificate Revocation Settings</b>.</li> <li>2. Perform one or both of the following steps, depending on whether the firewall will use <b>Online Certificate Status Protocol (OCSP)</b> or the <b>Certificate Revocation List (CRL)</b> method to verify the revocation status of certificates. If the firewall will use both, it first tries OCSP; if the OCSP responder is unavailable, the firewall then tries the CRL method. <ul style="list-style-type: none"> <li>• In the CRL section, select the <b>Enable</b> check box and enter the <b>Receive Timeout</b>. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from the CRL service.</li> <li>• In the OCSP section, select the <b>Enable</b> check box and enter the <b>Receive Timeout</b>. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from the OCSP responder.</li> </ul> <p>Depending on the <b>Certificate Status Timeout</b> value you specify in <b>Step 2</b>, the firewall might register a timeout before either or both of the <b>Receive Timeout</b> intervals pass.</p> </li> </ol>
<b>Step 2</b> Define the total timeout interval for revocation status requests.	Enter the <b>Certificate Status Timeout</b> . This is the interval (1-60 seconds) after which the firewall stops waiting for a response from any certificate status service and applies the session-blocking logic you optionally define in <b>Step 3</b> . The <b>Certificate Status Timeout</b> relates to the OCSP/CRL <b>Receive Timeout</b> as follows: <ul style="list-style-type: none"> <li>• If you enable both OCSP and CRL—The firewall registers a request timeout after the lesser of two intervals passes: the <b>Certificate Status Timeout</b> value or the aggregate of the two <b>Receive Timeout</b> values.</li> <li>• If you enable only OCSP—The firewall registers a request timeout after the lesser of two intervals passes: the <b>Certificate Status Timeout</b> value or the OCSP <b>Receive Timeout</b> value.</li> <li>• If you enable only CRL—The firewall registers a request timeout after the lesser of two intervals passes: the <b>Certificate Status Timeout</b> value or the CRL <b>Receive Timeout</b> value.</li> </ul>
<b>Step 3</b> Define the blocking behavior for <i>unknown</i> certificate status or a revocation status request timeout.	If you want the firewall to block SSL/TLS sessions when the OCSP or CRL service returns a certificate revocation status of <i>unknown</i> , select the <b>Block Session With Unknown Certificate Status</b> check box. Otherwise, the firewall proceeds with the session.  If you want the firewall to block SSL/TLS sessions after it registers a request timeout, select the <b>Block Session On Certificate Status Check Timeout</b> check box. Otherwise, the firewall proceeds with the session.
<b>Step 4</b> Save and apply your entries.	Click <b>OK</b> and <b>Commit</b> .

# Configure the Master Key

Every firewall and Panorama management server has a default master key that encrypts all the private keys and passwords in the configuration to secure them (such as the private key used for SSL Forward Proxy Decryption).

If you deploy firewalls or Panorama in a high availability (HA) configuration, use the same master key on both HA peers. Otherwise, HA synchronization will not work properly.

If you use Panorama, use the same master key on Panorama and all managed firewalls. Otherwise, Panorama cannot push configurations to the firewalls.



As a best practice, configure a new master key instead of using the default, periodically change the key, and store the key in a safe location. For extra security you can also [Encrypt a Master Key Using an HSM](#).

## Configure a Master Key

**Step 1** Select **Device > Master Key and Diagnostics** and, in the Master Key section, click the Edit icon.

**Step 2** Enter the **Current Master Key** if one exists.

**Step 3** Define a new **New Master Key** and then **Confirm New Master Key**. The key must contain exactly 16 characters.

**Step 4** (Optional) To specify the master key **Life Time**, enter the number of **Days** and/or **Hours** after which the key will expire. If you set a life time, create a new master key before the old key expires.

**Step 5** (Optional) If you set a key life time, enter a **Time for Reminder** that specifies the number of **Days** and **Hours** preceding master key expiration when the firewall emails you a reminder.

**Step 6** (Optional) Select whether to use an **HSM** to encrypt the master key. For details, see [Encrypt a Master Key Using an HSM](#).

**Step 7** Click **OK** and **Commit**.

## Obtain Certificates

- ▲ Create a Self-Signed Root CA Certificate
- ▲ Generate a Certificate on the Device
- ▲ Import a Certificate and Private Key
- ▲ Obtain a Certificate from an External CA

## Create a Self-Signed Root CA Certificate

A self-signed root certificate authority (CA) certificate is the top-most certificate in a certificate chain. A firewall can use this certificate to automatically issue certificates for other uses. For example, the firewall issues certificates for SSL/TLS decryption and for satellite devices in a GlobalProtect large-scale VPN.

When establishing a secure connection with the firewall, the remote client must trust the root CA that issued the certificate. Otherwise, the client browser will display a warning that the certificate is invalid and might (depending on security settings) block the connection. To prevent this, after generating the self-signed root CA certificate, import it into the client systems.



On a Palo Alto Networks device, you can generate self-signed certificates only if they are CA certificates.

### Generate a Self-signed Root CA Certificate

- Step 1 Select **Device > Certificate Management > Certificates > Device Certificates**.
- Step 2 If the device has more than one virtual system (vsys), select a **Location** (vsys or **Shared**) for the certificate.
- Step 3 Click **Generate**.
- Step 4 Enter a **Certificate Name**, such as *GlobalProtect\_CA*. The name is case-sensitive and can have up to 31 characters. It must be unique and use only letters, numbers, hyphens, and underscores.
- Step 5 In the **Common Name** field, enter the FQDN (recommended) or IP address of the interface where you will configure the service that will use this certificate.
- Step 6 If the device has more than one vsys and you want the certificate to be available to every vsys, select the **Shared** check box.
- Step 7 Leave the **Signed By** field blank to designate the certificate as self-signed.
- Step 8 (Required) Select the **Certificate Authority** check box.
- Step 9 Leave the **OCSP Responder** field blank; revocation status verification doesn't apply to root CA certificates.
- Step 10 Click **Generate** and **Commit**.

## Generate a Certificate on the Device

Palo Alto Networks devices use certificates to authenticate clients, servers, users, and devices in several applications, including SSL/TLS decryption, Captive Portal, GlobalProtect, site-to-site IPSec VPN, and device web interface access. Generate certificates for each usage: for details, see [Keys and Certificates](#).

To generate a certificate, you must first [Create a Self-Signed Root CA Certificate](#) or import one ([Import a Certificate and Private Key](#)) to sign it. To use Online Certificate Status Protocol (OCSP) for verifying certificate revocation status, [Configure an OCSP Responder](#) before generating the certificate.

### Generate a Certificate on the Device

**Step 1** Select **Device > Certificate Management > Certificates > Device Certificates**.

**Step 2** If the device has more than one virtual system (vsys), select a **Location** (vsys or **Shared**) for the certificate.

**Step 3** Click **Generate**.

**Step 4** Enter a **Certificate Name**. The name is case-sensitive and can have up to 31 characters. It must be unique and use only letters, numbers, hyphens, and underscores.

**Step 5** In the **Common Name** field, enter the FQDN (recommended) or IP address of the interface where you will configure the service that will use this certificate.

**Step 6** If the device has more than one vsys and you want the certificate to be available to every vsys, select the **Shared** check box.

**Step 7** In the **Signed By** field, select the root CA certificate that will issue the certificate.

**Step 8** (Optional) Select an **OCSP Responder**.

**Step 9** For the key generation **Algorithm**, select **RSA** (default) or **Elliptical Curve DSA** (ECDSA). ECDSA is recommended for client browsers and operating systems that support it.



Firewalls that run PAN-OS 6.1 and earlier releases will delete any ECDSA certificates that you push from Panorama™, and any RSA certificates signed by an ECDSA certificate authority (CA) will be invalid on those firewalls.

**Step 10** Select the **Number of Bits** to define the certificate key length. Higher numbers are more secure but require more processing time.

**Step 11** Select the **Digest** algorithm. From most to least secure, the options are: **sha512**, **sha384**, **sha256** (default), **sha1**, and **md5**.

**Step 12** For the **Expiration**, enter the number of days (default is 365) for which the certificate is valid.

**Step 13** (Optional) **Add the Certificate Attributes** to uniquely identify the firewall and the service that will use the certificate.



If you add a **Host Name** (DNS name) attribute, it is a best practice for it to match the **Common Name**. The host name populates the Subject Alternative Name field of the certificate.

**Step 14** Click **Generate** and, in the Device Certificates page, click the certificate Name.



Regardless of the time zone on the firewall, it always displays the corresponding Greenwich Mean Time (GMT) for certificate validity and expiration dates/times.

**Generate a Certificate on the Device (Continued)**

**Step 15** Select the check boxes that correspond to the intended use of the certificate on the firewall.

For example, if the firewall will use this certificate to secure forwarding of syslogs to an external syslog server, select the **Certificate for Secure Syslog** check box.

**Step 16** Click **OK** and **Commit**.

## Import a Certificate and Private Key

If your enterprise has its own public key infrastructure (PKI), you can import a certificate and private key into the firewall from your enterprise certificate authority (CA). Enterprise CA certificates (unlike most certificates purchased from a trusted, third-party CA) can automatically issue CA certificates for applications such as SSL/TLS decryption or large-scale VPN.



On a Palo Alto Networks device, you can import self-signed certificates only if they are CA certificates.

Instead of importing a self-signed root CA certificate into all the client systems, it is a best practice to import a certificate from the enterprise CA because the clients will already have a trust relationship with the enterprise CA, which simplifies the deployment.

If the certificate you will import is part of a certificate chain, it is a best practice to import the entire chain.

### Import a Certificate and Private Key

**Step 1** From the enterprise CA, export the certificate and private key that the firewall will use for authentication.

When exporting a private key, you must enter a passphrase to encrypt the key for transport. Ensure the management system can access the certificate and key files. When importing the key onto the firewall, you must enter the same passphrase to decrypt it.

**Step 2** Select **Device > Certificate Management > Certificates > Device Certificates**.

**Step 3** If the device has more than one virtual system (vsys), select a **Location** (vsys or **Shared**) for the certificate.

**Step 4** Click **Import** and enter a **Certificate Name**. The name is case-sensitive and can have up to 31 characters. It must be unique and use only letters, numbers, hyphens, and underscores.

**Step 5** To make the certificate available to all virtual systems, select the **Shared** check box. This check box appears only if the device supports multiple virtual systems.

**Step 6** Enter the path and name of the **Certificate File** received from the CA, or **Browse** to find the file.

**Step 7** Select a **File Format**:

- **Encrypted Private Key and Certificate (PKCS12)**—This is the default and most common format, in which the key and certificate are in a single container (**Certificate File**). If a hardware security module (HSM) will store the private key for this certificate, select the **Private key resides on Hardware Security Module** check box.
- **Base64 Encoded Certificate (PEM)**—You must import the key separately from the certificate. If a hardware security module (HSM) stores the private key for this certificate, select the **Private key resides on Hardware Security Module** check box and skip Step 8. Otherwise, select the **Import Private Key** check box, enter the **Key File** or **Browse** to it, then perform Step 8.

**Step 8** Enter and re-enter (confirm) the **Passphrase** used to encrypt the private key.

**Step 9** Click **OK**. The Device Certificates page displays the imported certificate.

## Obtain a Certificate from an External CA

The advantage of obtaining a certificate from an external certificate authority (CA) is that the private key does not leave the firewall. To obtain a certificate from an external CA, generate a certificate signing request (CSR) and submit it to the CA. After the CA issues a certificate with the specified attributes, import it onto the firewall. The CA can be a well-known, public CA or an enterprise CA.

To use Online Certificate Status Protocol (OCSP) for verifying the revocation status of the certificate, [Configure an OCSP Responder](#) before generating the CSR.

Obtain a Certificate from an External CA	
<b>Step 1</b> Request the certificate from an external CA.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b>.</li> <li>If the device has more than one virtual system (vsys), select a <b>Location</b> (vsys or <b>Shared</b>) for the certificate.</li> <li>Click <b>Generate</b>.</li> <li>Enter a <b>Certificate Name</b>. The name is case-sensitive and can have up to 31 characters. It must be unique and use only letters, numbers, hyphens, and underscores.</li> <li>In the <b>Common Name</b> field, enter the FQDN (recommended) or IP address of the interface where you will configure the service that will use this certificate.</li> <li>If the device has more than one vsys and you want the certificate to be available to every vsys, select the <b>Shared</b> check box.</li> <li>In the <b>Signed By</b> field, select <b>External Authority (CSR)</b>.</li> <li>If applicable, select an <b>OCSP Responder</b>.</li> <li>(Optional) <b>Add</b> the <b>Certificate Attributes</b> to uniquely identify the firewall and the service that will use the certificate.</li> </ol> <p> If you add a <b>Host Name</b> attribute, it is a best practice for it to match the <b>Common Name</b> (this is mandatory for GlobalProtect). The host name populates the Subject Alternative Name field of the certificate.</p> <ol style="list-style-type: none"> <li>Click <b>Generate</b>. The Device Certificates tab displays the CSR with a Status of <i>pending</i>.</li> </ol>
<b>Step 2</b> Submit the CSR to the CA.	<ol style="list-style-type: none"> <li>Select the CSR and click <b>Export</b> to save the .csr file to a local computer.</li> <li>Upload the .csr file to the CA.</li> </ol>

**Obtain a Certificate from an External CA**

Step 3 Import the certificate.	<ol style="list-style-type: none"><li>1. After the CA sends a signed certificate in response to the CSR, return to the <b>Device Certificates</b> tab and click <b>Import</b>.</li><li>2. Enter the <b>Certificate Name</b> used to generate the CSR in <a href="#">Step 1-4</a>.</li><li>3. Enter the path and name of the PEM <b>Certificate File</b> that the CA sent, or <b>Browse</b> to it.</li><li>4. Click <b>OK</b>. The <b>Device Certificates</b> tab displays the certificate with a Status of <i>valid</i>.</li></ol>
Step 4 Configure the certificate.	<ol style="list-style-type: none"><li>1. Click the certificate <b>Name</b>.</li><li>2. Select the check boxes that correspond to the intended use of the certificate on the firewall. For example, if the firewall will use this certificate to secure forwarding of syslogs to an external syslog server, select the <b>Certificate for Secure Syslog</b> check box.</li><li>3. Click <b>OK</b> and <b>Commit</b>.</li></ol>

# Export a Certificate and Private Key

Palo Alto Networks recommends that you use your enterprise public key infrastructure (PKI) to distribute a certificate and private key in your organization. However, if necessary, you can also export a certificate and private key from the firewall or Panorama. You can use an exported certificate and private key in the following cases:

- [Administrator authentication to the device web interface](#)
- [GlobalProtect agent/app authentication to portals and gateways](#)
- [SSL Forward Proxy decryption](#)
- [Certificate signing requests \(CSRs\)](#)

## Export a Certificate and Private Key

**Step 1** Select **Device > Certificate Management > Certificates > Device Certificates**.

**Step 2** If the device has more than one virtual system (vsys), select a **Location** (a specific vsys or **Shared**) for the certificate.

**Step 3** Select the certificate, click **Export**, and select a **File Format**:

- **Base64 Encoded Certificate (PEM)**—This is the default format. It is the most common and has the broadest support on the Internet. If you want the exported file to include the private key, select the **Export Private Key** check box.
- **Encrypted Private Key and Certificate (PKCS12)**—This format is more secure than PEM but is not as common or as broadly supported. The exported file will automatically include the private key.
- **Binary Encoded Certificate (DER)**—More operating system types support this format than the others. You can export only the certificate, not the key: ignore the **Export Private Key** check box and passphrase fields.

**Step 4** Enter a **Passphrase** and **Confirm Passphrase** to encrypt the private key if the **File Format** is PKCS12 or if it is PEM and you selected the **Export Private Key** check box. You will use this passphrase when importing the certificate and key into client systems.

**Step 5** Click **OK** and save the certificate/key file to your computer.

# Configure a Certificate Profile

Certificate profiles define user and device authentication for Captive Portal, GlobalProtect, site-to-site IPSec VPN, Mobile Security Manager, and web interface access to Palo Alto Networks devices. The profiles specify which certificates to use, how to verify certificate revocation status, and how that status constrains access. Configure a certificate profile for each application.



It is a best practice to enable Online Certificate Status Protocol (OCSP) and/or Certificate Revocation List (CRL) status verification for certificate profiles. For details on these methods, see [Certificate Revocation](#).

## Configure a Certificate Profile

<b>Step 1</b> Obtain the certificate authority (CA) certificates you will assign.	<p>Perform one of the following steps to obtain the CA certificates you will assign to the profile. You must assign at least one.</p> <ul style="list-style-type: none"><li>• <a href="#">Generate a Certificate on the Device</a>.</li><li>• Export a certificate from your enterprise CA and then import it onto the firewall (see <a href="#">Step 3</a>).</li></ul>
<b>Step 2</b> Identify the certificate profile.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Certificate Management &gt; Certificates Profile</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> to identify the profile. The name is case-sensitive, must be unique and can use up to 31 characters that include only letters, numbers, spaces, hyphens, and underscores.</li><li>3. If the device has more than one virtual system (vsys), select a <b>Location</b> (vsys or Shared) for the certificate.</li></ol>
<b>Step 3</b> Assign one or more certificates.	<p>Perform the following steps for each CA certificate:</p> <ol style="list-style-type: none"><li>1. In the CA Certificates table, click <b>Add</b>.</li><li>2. Select a <b>CA Certificate</b>. Alternatively, to import a certificate, click <b>Import</b>, enter a <b>Certificate Name</b>, <b>Browse</b> to the <b>Certificate File</b> you exported from your enterprise CA, and click <b>OK</b>.</li><li>3. Optionally, if the firewall uses OCSP to verify certificate revocation status, configure the following fields to override the default behavior. For most deployments, these fields do not apply.<ul style="list-style-type: none"><li>• By default, the firewall uses the OCSP responder URL that you set in the procedure <a href="#">Configure an OCSP Responder</a>. To override that setting, enter a <b>Default OCSP URL</b> (starting with <code>http://</code> or <code>https://</code>).</li><li>• By default, the firewall uses the certificate selected in the <b>CA Certificate</b> field to validate OCSP responses. To use a different certificate for validation, select it in the <b>OCSP Verify CA Certificate</b> field.</li></ul></li><li>4. Click <b>OK</b>. The CA Certificates table displays the assigned certificate.</li></ol>

Configure a Certificate Profile	
<b>Step 4</b> Define the methods for verifying certificate revocation status and the associated blocking behavior.	<ol style="list-style-type: none"><li>1. Select <b>Use CRL</b> and/or <b>Use OCSP</b>. If you select both, the firewall first tries OCSP and falls back to the CRL method only if the OCSP responder is unavailable.</li><li>2. Depending on the verification method, enter the <b>CRL Receive Timeout</b> and/or <b>OCSP Receive Timeout</b>. These are the intervals (1-60 seconds) after which the firewall stops waiting for a response from the CRL/OCSP service.</li><li>3. Enter the <b>Certificate Status Timeout</b>. This is the interval (1-60 seconds) after which the firewall stops waiting for a response from any certificate status service and applies any session-blocking logic you define. The <b>Certificate Status Timeout</b> relates to the OCSP/CRL <b>Receive Timeout</b> as follows:<ul style="list-style-type: none"><li>• If you enable both OCSP and CRL—The firewall registers a request timeout after the lesser of two intervals passes: the <b>Certificate Status Timeout</b> value or the aggregate of the two <b>Receive Timeout</b> values.</li><li>• If you enable only OCSP—The firewall registers a request timeout after the lesser of two intervals passes: the <b>Certificate Status Timeout</b> value or the OCSP <b>Receive Timeout</b> value.</li><li>• If you enable only CRL—The firewall registers a request timeout after the lesser of two intervals passes: the <b>Certificate Status Timeout</b> value or the CRL <b>Receive Timeout</b> value.</li></ul></li><li>4. If you want the firewall to block sessions when the OCSP or CRL service returns a certificate revocation status of <i>unknown</i>, select the <b>Block session if certificate status is unknown</b> check box. Otherwise, the firewall proceeds with the session.</li><li>5. If you want the firewall to block sessions after it registers an OCSP or CRL request timeout, select the <b>Block session if certificate status cannot be retrieved within timeout</b> check box. Otherwise, the firewall proceeds with the session.</li></ol>
<b>Step 5</b> Save and apply your entries.	Click <b>OK</b> and <b>Commit</b> .

# Configure an SSL/TLS Service Profile

SSL/TLS service profiles specify a certificate and the allowed protocol versions for the SSL/TLS services of Palo Alto Networks devices. The devices use SSL/TLS for Captive Portal, GlobalProtect portals and gateways, inbound traffic on the management (MGT) interface, the URL Admin Override feature, and the User-ID™ syslog listening service. By defining the protocol versions, you can use a profile to restrict the cipher suites that are available for securing communication with the clients requesting the services. This improves network security by enabling devices to avoid SSL/TLS versions that have known weaknesses: if a service request involves a protocol version that is outside the specified range, the device downgrades or upgrades the connection to a supported version.



In the client systems that request firewall services, the certificate trust list (CTL) must include the certificate authority (CA) certificate that issued the certificate specified in the SSL/TLS service profile. Otherwise, users will see a certificate error when requesting firewall services. Most third-party CA certificates are present by default in client browsers. If an enterprise or firewall-generated CA certificate is the issuer, you must deploy that CA certificate to the CTL in client browsers.

## Configure an SSL/TLS Service Profile

**Step 1** For each desired service, generate or import a certificate on the firewall (see [Obtain Certificates](#)).



Use only signed certificates, not certificate authority (CA) certificates, in SSL/TLS services profile.

**Step 2** Select **Device > Certificate Management > SSL/TLS Service Profile**.

**Step 3** If the device has more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where the profile is available.

**Step 4** Click **Add** and enter a **Name** to identify the profile.

**Step 5** Select the **Certificate** you just obtained.

**Step 6** Define the range of protocols that the service can use:

- For the **Min Version**, select the earliest allowed TLS version: **TLSv1.0** (default), **TLSv1.1**, or **TLSv1.2**.
- For the **Max Version**, select the latest allowed TLS version: **TLSv1.0**, **TLSv1.1**, **TLSv1.2**, or **Max** (latest available version). The default is **Max**.

**Step 7** Click **OK** and **Commit**.

# Configure the Key Size for SSL Forward Proxy Server Certificates

When responding to a client in an [SSL Forward Proxy](#) session, the firewall creates a copy of the certificate that the destination server presents and uses the copy to establish a connection with the client. By default, the firewall generates certificates with the same key size as the certificate that the destination server presented. However, you can change the key size for the firewall-generated certificate as follows:

## Configure the Key Size for SSL Forward Proxy Server Certificates

**Step 1** Select **Device > Setup > Session** and, in the Decryption Settings section, click **SSL Forward Proxy Settings**.

**Step 2** Select a **Key Size**:

- **Defined by destination host**—The firewall determines the key size for the certificates it generates to establish SSL proxy sessions with clients based on the key size of the destination server certificate. If the destination server uses a 1,024-bit RSA key, the firewall generates a certificate with that key size and an SHA-1 hashing algorithm. If the destination server uses a key size larger than 1,024 bits (for example, 2,048 bits or 4,096 bits), the firewall generates a certificate that uses a 2,048-bit RSA key and SHA-256 algorithm. This is the default setting.
- **1024-bit RSA**—The firewall generates certificates that use a 1,024-bit RSA key and SHA-1 hashing algorithm regardless of the key size of the destination server certificates. As of December 31, 2013, public certificate authorities (CAs) and popular browsers have limited support for X.509 certificates that use keys of fewer than 2,048 bits. In the future, depending on security settings, when presented with such keys the browser might warn the user or block the SSL/TLS session entirely.
- **2048-bit RSA**—The firewall generates certificates that use a 2,048-bit RSA key and SHA-256 hashing algorithm regardless of the key size of the destination server certificates. Public CAs and popular browsers support 2,048-bit keys, which provide better security than the 1,024-bit keys.



Changing the key size setting clears the current certificate cache.

**Step 3** Click **OK** and **Commit**.

# Revoke and Renew Certificates

- ▲ [Revoke a Certificate](#)
- ▲ [Renew a Certificate](#)

## Revoke a Certificate

Various circumstances can invalidate a certificate before the expiration date. Some examples are a change of name, change of association between subject and certificate authority (for example, an employee terminates employment), and compromise (known or suspected) of the private key. Under such circumstances, the certificate authority (CA) that issued the certificate must revoke it. The following task describes how to revoke a certificate for which the firewall is the CA.

### Revoke a Certificate

- 
- Step 1 Select **Device > Certificate Management > Certificates > Device Certificates**.
- 
- Step 2 If the device supports multiple virtual systems, the tab displays a **Location** drop-down. Select the virtual system to which the certificate belongs.
- 
- Step 3 Select the certificate to revoke.
- 
- Step 4 Click **Revoke**. PAN-OS immediately sets the status of the certificate to revoked and adds the serial number to the Online Certificate Status Protocol (OCSP) responder cache or certificate revocation list (CRL). You need not perform a commit.
- 

## Renew a Certificate

If a certificate expires, or soon will, you can reset the validity period. If an external certificate authority (CA) signed the certificate and the firewall uses the Online Certificate Status Protocol (OCSP) to verify certificate revocation status, the firewall uses the OCSP responder information to update the certificate status (see [Configure an OCSP Responder](#)). If the firewall is the CA that issued the certificate, the firewall replaces it with a new certificate that has a different serial number but the same attributes as the old certificate.

### Renew a Certificate

- 
- Step 1 Select **Device > Certificate Management > Certificates > Device Certificates**.
- 
- Step 2 If the device has more than one virtual system (vsys), select a **Location** (vsys or **Shared**) for the certificate.
- 
- Step 3 Select a certificate to renew and click **Renew**.
- 
- Step 4 Enter a **New Expiration Interval** (in days).
- 
- Step 5 Click **OK** and **Commit**.
-

## Secure Keys with a Hardware Security Module

A hardware security module (HSM) is a physical device that manages digital keys. An HSM provides secure storage and generation of digital keys. It provides both logical and physical protection of these materials from non-authorized use and potential adversaries.

HSM clients integrated with Palo Alto Networks devices enable enhanced security for the private keys used in SSL/TLS decryption (both SSL forward proxy and SSL inbound inspection). In addition, you can use the HSM to encrypt device master keys.

The following topics describe how to integrate an HSM with your Palo Alto Networks devices:

- ▲ [Set up Connectivity with an HSM](#)
- ▲ [Encrypt a Master Key Using an HSM](#)
- ▲ [Store Private Keys on an HSM](#)
- ▲ [Manage the HSM Deployment](#)

## Set up Connectivity with an HSM

HSM clients are integrated with PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, and VM-Series firewalls and on Panorama (virtual appliance and M-Series appliance) for use with the following HSMs:

- SafeNet Network 5.2.1 or later
- Thales nShield Connect 11.62 or later



The HSM server version must be compatible with these client versions. Refer to the HSM vendor documentation for the client-server version compatibility matrix.

The following topics describe how to set up connectivity between the Palo Alto Networks device and one of the supported HSMs:

- ▲ [Set Up Connectivity with a SafeNet Network HSM](#)
- ▲ [Set Up Connectivity with a Thales nShield Connect HSM](#)

### Set Up Connectivity with a SafeNet Network HSM

To set up connectivity between the Palo Alto Networks device and a SafeNet Network HSM, you must specify the address of the HSM server and the password for connecting to it in the firewall configuration. In addition, you must register the firewall with the HSM server. Prior to beginning the configuration, make sure you have created a partition for the Palo Alto Networks devices on the HSM server.



HSM configuration is not synced between high availability firewall peers. Consequently, you must configure the HSM module separately on each of the peers.

In Active-Passive HA deployments, you must manually perform one failover to configure and authenticate each HA peer individually to the HSM. After this manual failover has been performed, user interaction is not required for the failover function.

#### Set up a Connectivity with a SafeNet Network HSM

<p><b>Step 1</b> Configure the firewall to communicate with the SafeNet Network HSM.</p>	<ol style="list-style-type: none"><li>1. Log in to the firewall web interface and select <b>Device &gt; Setup &gt; HSM</b>.</li><li>2. Edit the Hardware Security Module Provider section and select <b>Safenet Luna SA</b> (SafeNet Network) as the <b>Provider Configured</b>.</li><li>3. Click <b>Add</b> and enter a <b>Module Name</b>. This can be any ASCII string up to 31 characters in length.</li><li>4. Enter the IPv4 address of the HSM module as the <b>Server Address</b>. If you are configuring a high availability HSM configuration, enter module names and IP addresses for the additional HSM devices.</li><li>5. (Optional) If configuring a high availability HSM configuration, select the <b>High Availability</b> check box and add the following: a value for <b>Auto Recovery Retry</b> and a <b>High Availability Group Name</b>. If two HSM servers are configured, you should configure high availability. Otherwise the second HSM server is not used.</li><li>6. Click <b>OK</b> and <b>Commit</b>.</li></ol>
--	---

### Set up a Connectivity with a SafeNet Network HSM (Continued)

<p><b>Step 2</b> (Optional) Configure a service route to enable the firewall to connect to the HSM.</p> <p>By default, the firewall uses the Management Interface to communicate with the HSM. To use a different interface, you must configure a service route.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Services</b>.</li> <li>2. Select <b>Service Route Configuration</b> from the Services Features area.</li> <li>3. Select <b>Customize</b> from the Service Route Configuration area.</li> <li>4. Select the <b>IPv4</b> tab.</li> <li>5. Select <b>HSM</b> from the <b>Service</b> column.</li> <li>6. Select an interface to use for HSM from the <b>Source Interface</b> drop-down.</li> </ol> <p> If you select a dataplane connected port for HSM, issuing the <code>clear session all</code> CLI command will clear all existing HSM sessions, causing all HSM states to be brought down and then up. During the several seconds required for HSM to recover, all SSL/TLS operations will fail.</p> <ol style="list-style-type: none"> <li>7. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
<p><b>Step 3</b> Configure the firewall to authenticate to the HSM.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; HSM</b>.</li> <li>2. Select <b>Setup Hardware Security Module</b> in the Hardware Security Operations area.</li> <li>3. Select the HSM <b>Server Name</b> from the drop-down.</li> <li>4. Enter the <b>Administrator Password</b> to authenticate the firewall to the HSM.</li> <li>5. Click <b>OK</b>.</li> </ol> <p>The firewall attempts to perform an authentication with the HSM and displays a status message.</p> <ol style="list-style-type: none"> <li>6. Click <b>OK</b>.</li> </ol>
<p><b>Step 4</b> Register the firewall (the HSM client) with the HSM and assign it to a partition on the HSM.</p> <p> If the HSM already has a firewall with the same <code>&lt;cl-name&gt;</code> registered, you must remove the duplicate registration using the following command before registration will succeed:</p> <pre>client delete -client &lt;cl-name&gt;</pre> <p>where <code>&lt;cl-name&gt;</code> is the name of the client (firewall) registration you want to delete.</p>	<ol style="list-style-type: none"> <li>1. Log in to the HSM from a remote system.</li> <li>2. Register the firewall using the following command:  <code>client register -c &lt;cl-name&gt; -ip &lt;fw-ip-addr&gt;</code>          where <code>&lt;cl-name&gt;</code> is a name that you assign to the firewall for use on the HSM and <code>&lt;fw-ip-addr&gt;</code> is the IP address of the firewall that is being configured as an HSM client.</li> <li>3. Assign a partition to the firewall using the following command:  <code>client assignpartition -c &lt;cl-name&gt; -p &lt;partition-name&gt;</code>          where <code>&lt;cl-name&gt;</code> is the name assigned to the firewall in the <code>client register</code> command and <code>&lt;partition-name&gt;</code> is the name of a previously configured partition that you want to assign to the firewall.</li> </ol>

### Set up a Connectivity with a SafeNet Network HSM (Continued)

<p><b>Step 5</b> Configure the firewall to connect to the HSM partition.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; HSM</b>.</li> <li>2. Click the <b>Refresh</b> icon.</li> <li>3. Select the <b>Setup HSM Partition</b> in the Hardware Security Operations area.</li> <li>4. Enter the <b>Partition Password</b> to authenticate the firewall to the partition on the HSM.</li> <li>5. Click <b>OK</b>.</li> </ol>
<p><b>Step 6</b> (Optional) Configure an additional HSM for high availability (HA).</p>	<ol style="list-style-type: none"> <li>1. Follow <a href="#">Step 1</a> through <a href="#">Step 5</a> to add an additional HSM for high availability (HA). This process adds a new HSM to the existing HA group.</li> <li>2. If you remove an HSM from your configuration, repeat <a href="#">Step 5</a>. This will remove the deleted HSM from the HA group.</li> </ol>
<p><b>Step 7</b> Verify connectivity with the HSM.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; HSM</b>.</li> <li>2. Check the <b>Status</b> of the HSM connection: Green—HSM is authenticated and connected. Red—HSM was not authenticated or network connectivity to the HSM is down.</li> <li>3. View the following columns in Hardware Security Module Status area to determine authentication status: <b>Serial Number</b>—The serial number of the HSM partition if the HSM was successfully authenticated. <b>Partition</b>—The partition name on the HSM that was assigned on the firewall. <b>Module State</b>—The current operating state of the HSM. It always has the value Authenticated if the HSM is displayed in this table.</li> </ol>

## Set Up Connectivity with a Thales nShield Connect HSM

The following workflow describes how to configure the firewall to communicate with a Thales nShield Connect HSM. This configuration requires that you set up a remote filesystem (RFS) to use as a *hub* to sync key data for all firewalls in your organization that are using the HSM.



HSM configuration is not synced between high availability firewall peers. Consequently, you must configure the HSM module separately on each of the peers.

If the high availability firewall configuration is in Active-Passive mode, you must manually perform one failover to configure and authenticate each HA peer individually to the HSM. After this manual failover has been performed, user interaction is not required for the failover function.

## Set up Connectivity with a Thales nShield Connect HSM

<p><b>Step 1</b> Configure the Thales nShield Connect server as the firewall's HSM provider.</p>	<ol style="list-style-type: none"> <li>1. From the firewall web interface, select <b>Device &gt; Setup &gt; HSM</b> and edit the Hardware Security Module Provider section.</li> <li>2. Select <b>Thales Nshield Connect</b> as the <b>Provider Configured</b>.</li> <li>3. Click <b>Add</b> and enter a <b>Module Name</b>. This can be any ASCII string up to 31 characters in length.</li> <li>4. Enter the IPv4 address as the <b>Server Address</b> of the HSM module. If you are configuring a high availability HSM configuration, enter module names and IP addresses for the additional HSM devices.</li> <li>5. Enter the IPv4 address of the <b>Remote Filesystem Address</b>.</li> <li>6. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
<p><b>Step 2</b> (Optional) Configure a service route to enable the firewall to connect to the HSM.</p> <p>By default, the firewall uses the Management Interface to communicate with the HSM. To use a different interface, you must configure a service route.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Services</b>.</li> <li>2. Select <b>Service Route Configuration</b> from the Services Features area.</li> <li>3. Select <b>Customize</b> from the Service Route Configuration area.</li> <li>4. Select the <b>IPv4</b> tab.</li> <li>5. Select <b>HSM</b> from the <b>Service</b> column.</li> <li>6. Select an interface to use for HSM from the <b>Source Interface</b> drop-down.</li> </ol> <p> If you select a dataplane connected port for HSM, issuing the <code>clear session all</code> CLI command will clear all existing HSM sessions, causing all HSM states to be brought down and then up. During the several seconds required for HSM to recover, all SSL/TLS operations will fail.</p> <ol style="list-style-type: none"> <li>7. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
<p><b>Step 3</b> Register the firewall (the HSM client) with the HSM server.</p> <p>This step briefly describes the procedure for using the front panel interface of the Thales nShield Connect HSM. For more details, consult the Thales documentation.</p>	<ol style="list-style-type: none"> <li>1. Log in to the front panel display of the Thales nShield Connect HSM unit.</li> <li>2. On the unit front panel, use the right-hand navigation button to select <b>System &gt; System configuration &gt; Client config &gt; New client</b>.</li> <li>3. Enter the IP address of the firewall.</li> <li>4. Select <b>System &gt; System configuration &gt; Client config &gt; Remote file system</b> and enter the IP address of the client computer where you set up the remote file system.</li> </ol>

### Set up Connectivity with a Thales nShield Connect HSM (Continued)

<p><b>Step 4</b> Set up the remote filesystem to accept connections from the firewall.</p>	<ol style="list-style-type: none"> <li>1. Log in to the remote filesystem (RFS) from a Linux client.</li> <li>2. Obtain the electronic serial number (ESN) and the hash of the K<sub>NETI</sub> key. The K<sub>NETI</sub> key authenticates the module to clients:  <code>anonkneti &lt;ip-address&gt;</code>          where &lt;ip-address&gt; is the IP address of the HSM.          The following is an example:  <code>anonkneti 192.0.2.1 B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c</code>          In this example, <b>B1E2-2D4C-E6A2</b> is the ESM and 5a2e5107e70d525615a903f6391ad72b1c03352c is the hash of the K<sub>NETI</sub> key.</li> <li>3. Use the following command from a superuser account to perform the remote filesystem setup:  <code>rfs-setup --force &lt;ip-address&gt; &lt;ESN&gt; &lt;hash-Kneti-key&gt;</code>          where &lt;ip-address&gt; is the IP address of the HSM,  &lt;ESN&gt; is the electronic serial number (ESN) and  &lt;hash-Kneti-key&gt; is the hash of the KNETI key.          The following example uses the values obtained in this procedure:  <code>rfs-setup --force &lt;192.0.2.1&gt; &lt;B1E2-2D4C-E6A2&gt; &lt;5a2e5107e70d525615a903f6391ad72b1c03352c&gt;</code></li> <li>4. Use the following command to permit client submit on the Remote Filesystem:  <code>rfs-setup --gang-client --write-noauth &lt;FW-IPaddress&gt;</code>          where &lt;FW-IPaddress&gt; is the IP address of the firewall.</li> </ol>
<p><b>Step 5</b> Configure the firewall to authenticate to the HSM.</p>	<ol style="list-style-type: none"> <li>1. From the firewall web interface, select <b>Device &gt; Setup &gt; HSM</b>.</li> <li>2. Select <b>Setup Hardware Security Module</b> in the Hardware Security Operations area.</li> <li>3. Click <b>OK</b>.          The firewall attempts to perform an authentication with the HSM and displays a status message.</li> <li>4. Click <b>OK</b>.</li> </ol>
<p><b>Step 6</b> Synchronize the firewall with the remote filesystem.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Device &gt; Setup &gt; HSM</b>.</li> <li>2. Select <b>Synchronize with Remote Filesystem</b> in the Hardware Security Operations section.</li> </ol>

**Set up Connectivity with a Thales nShield Connect HSM (Continued)**

<b>Step 7</b> Verify that the firewall can connect to the HSM.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; HSM</b>.</li><li>2. Check the Status indicator to verify that the firewall is connected to the HSM: Green—HSM is authenticated and connected. Red—HSM was not authenticated or network connectivity to the HSM is down.</li><li>3. View the following columns in Hardware Security Module Status section to determine authentication status. <b>Name:</b> The name of the HSM attempting to be authenticated. <b>IP address:</b> The IP address of the HSM that was assigned on the firewall. <b>Module State:</b> The current operating state of the HSM: <b>Authenticated</b> or <b>Not Authenticated</b>.</li></ol>
--	--

## Encrypt a Master Key Using an HSM

A master key is configured on a Palo Alto Networks firewall to encrypt all private keys and passwords. If you have security requirements to store your private keys in a secure location, you can encrypt the master key using an encryption key that is stored on an HSM. The firewall then requests the HSM to decrypt the master key whenever it is required to decrypt a password or private key on the firewall. Typically, the HSM is located in a highly secure location that is separate from the firewall for greater security.

The HSM encrypts the master key using a wrapping key. To maintain security, this encryption key must occasionally be changed. For this reason, a command is provided on the firewall to rotate the wrapping key which changes the master key encryption. The frequency of this wrapping key rotation depends on your application.



Master key encryption using an HSM is not supported on firewalls configured in FIPS or CC mode.

The following topics describe how to encrypt the master key initially and how to refresh the master key encryption:

- ▲ [Encrypt the Master Key](#)
- ▲ [Refresh the Master Key Encryption](#)

### Encrypt the Master Key

If you have not previously encrypted the master key on a device, use the following procedure to encrypt it. Use this procedure for first time encryption of a key, or if you define a new master key and you want to encrypt it. If you want to refresh the encryption on a previously encrypted key, see [Refresh the Master Key Encryption](#).

#### Encrypt a Master Key Using an HSM

- 
- Step 1 Select **Device > Master Key and Diagnostics**.
- 
- Step 2 Specify the key that is currently used to encrypt all of the private keys and passwords on the firewall in the **Master Key** field.
- 
- Step 3 If changing the master key, enter the new master key and confirm.
- 
- Step 4 Select the **HSM** check box.
- Life Time:** The number of days and hours after which the master key expires (range 1-730 days).
- Time for Reminder:** The number of days and hours before expiration when the user is notified of the impending expiration (range 1-365 days).
- 
- Step 5 Click **OK**.
- 

### Refresh the Master Key Encryption

As a best practice, refresh the master key encryption on a regular basis by rotating the master key wrapping key on the HSM. This command is the same for both the SafeNet Network and Thales nShield Connect HSMs.

---

**Refresh the Master Key Encryption**

**Step 1** Use the following CLI command to rotate the wrapping key for the master key on an HSM:

```
> request hsm mkey-wrapping-key-rotation
```

If the master key is encrypted on the HSM, the CLI command will generate a new wrapping key on the HSM and encrypt the master key with the new wrapping key.

If the master key is not encrypted on the HSM, the CLI command will generate new wrapping key on the HSM for future use.

The old wrapping key is not deleted by this command.

---

## Store Private Keys on an HSM

For added security, you can use an HSM to secure the private keys used in SSL/TLS decryption for:

- **SSL Forward Proxy**—The HSM can store the private key of the Forward Trust certificate that signs certificates in SSL/TLS forward proxy operations. The firewall will then send the certificates that it generates during such operations to the HSM for signing before forwarding the certificates to the client.
- **SSL Inbound Inspection**—The HSM can store the private keys for the internal servers for which you are performing SSL/TLS inbound inspection.

<b>Store Private Keys on an HSM</b>	
<b>Step 1</b>	On the HSM, import or generate the certificate and private key used in your decryption deployment.
<b>Step 2</b>	(Thales nShield Connect only) Synchronize the key data from the Thales nShield remote filesystem to the firewall.   Synchronization with the SafeNet Network HSM is automatic.
<b>Step 3</b>	Import the certificate that corresponds to the HSM-stored key onto the firewall.
<b>Step 4</b>	(Forward Trust certificates only) Enable the certificate for use in SSL/TLS Forward Proxy.
<b>Step 5</b>	Verify that you successfully imported the certificate onto the firewall.
	For instructions on importing or generating a certificate and private key on the HSM, refer to your HSM documentation.
	<ol style="list-style-type: none"> <li>1. Access the firewall web interface and select <b>Device &gt; Setup &gt; HSM</b>.</li> <li>2. Select <b>Synchronize with Remote Filesystem</b> in the Hardware Security Operations section.</li> </ol>
	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Import</b>.</li> <li>2. Enter the <b>Certificate Name</b>.</li> <li>3. <b>Browse</b> to the <b>Certificate File</b> on the HSM.</li> <li>4. Select a <b>File Format</b>.</li> <li>5. Select <b>Private Key resides on Hardware Security Module</b>.</li> <li>6. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
	<ol style="list-style-type: none"> <li>1. Open the certificate you imported in <b>Step 3</b> for editing.</li> <li>2. Select <b>Forward Trust Certificate</b>.</li> <li>3. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
	Locate the certificate you imported in <b>Step 3</b> and check the icon in the Key column: <ul style="list-style-type: none"> <li>• Lock icon—The private key for the certificate is on the HSM.</li> <li>• Error icon—The private key is not on the HSM or the HSM is not properly authenticated or connected.</li> </ul>

## Manage the HSM Deployment

<b>Manage HSM</b>	
• View the HSM configuration settings.	Select <b>Device &gt; Setup &gt; HSM</b> .
• Display detailed HSM information.	Select <b>Show Detailed Information</b> from the Hardware Security Operations section. Information regarding the HSM servers, HSM HA status, and HSM hardware is displayed.
• Export Support file.	Select <b>Export Support File</b> from the Hardware Security Operations section. A test file is created to help customer support when addressing a problem with an HSM configuration on the firewall.
• Reset HSM configuration.	Select <b>Reset HSM Configuration</b> from the Hardware Security Operations section. Selecting this option removes all HSM connections. All authentication procedures must be repeated after using this option.



# High Availability

---

High availability (HA) is a configuration in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up two firewalls in an HA pair provides redundancy and allows you to ensure business continuity.

The Palo Alto Networks firewalls support stateful active/passive or active/active high availability with session and configuration synchronization. Some models of the Palo Alto Networks firewall, such as the PA-200 only support [HA lite](#) without session synchronization capability, and the [VM-Series firewall in AWS](#) only supports active/passive HA. The following topics provide more information about high availability and how to configure it in your environment.

- ▲ [HA Overview](#)
- ▲ [HA Concepts](#)
- ▲ [Set Up Active/Passive HA](#)
- ▲ [Reference: HA Synchronization](#)
- ▲ [HA Resources](#)

## HA Overview

On Palo Alto Networks firewalls, you can set up two firewalls as an HA pair. HA allows you to minimize downtime by making sure that an alternate firewall is available in the event that the peer firewall fails. The firewalls in an HA pair use dedicated or in-band HA ports on the firewall to synchronize data—network, object, and policy configurations—and to maintain state information. Firewall-specific configuration such as management interface IP address or administrator profiles, HA specific configuration, log data, and the Application Command Center (ACC) information is not shared between peers. For a consolidated application and log view across the HA pair, you must use Panorama, the Palo Alto Networks centralized management system.

When a failure occurs on a firewall in an HA pair and the peer firewall takes over the task of securing traffic, the event is called a *failover*. The conditions that trigger a failover are:

- One or more of the monitored interfaces fail. ([Link Monitoring](#))
- One or more of the destinations specified on the firewall cannot be reached. ([Path Monitoring](#))
- The firewall does not respond to heartbeat polls. ([Heartbeat Polling and Hello messages](#))

After you understand the [HA Concepts](#), continue to [Set Up Active/Passive HA](#).

## HA Concepts

The following topics provide conceptual information about how HA works on a Palo Alto Networks firewall:

- ▲ [HA Modes](#)
- ▲ [HA Links and Backup Links](#)
- ▲ [Device Priority and Preemption](#)
- ▲ [Failover Triggers](#)
- ▲ [HA Timers](#)

### HA Modes

You can set up the firewalls for HA in two modes:

- **Active/Passive**— One firewall actively manages traffic while the other is synchronized and ready to transition to the active state, should a failure occur. In this configuration, both firewalls share the same configuration settings, and one actively manages traffic until a path, link, system, or network failure occurs. When the active firewall fails, the passive firewall transitions to the active state and takes over seamlessly and enforces the same policies to maintain network security. Active/passive HA is supported in the virtual wire, Layer 2 and Layer 3 deployments. For information on setting up your firewalls in an active/passive configuration, see [Configure Active/Passive HA](#).



The PA-200 appliance only supports a lite version of active/passive HA. HA lite provides configuration synchronization and some runtime data synchronization such as IPSec security associations. It does not support any session synchronization, and therefore, HA Lite does not offer stateful failover.

- **Active/Active**— Both the firewalls in the pair are active and processing traffic, and work synchronously to handle session setup and session ownership. The active/active deployment is supported in virtual wire and Layer 3 deployments, and is only recommended for networks with asymmetric routing. For information on setting up the firewalls in an active/active configuration, refer to the [Active/Active High Availability Tech Note](#).

### HA Links and Backup Links

The firewalls in an HA pair use HA links to synchronize data and maintain state information. Some models of the firewall have dedicated HA ports—Control link (HA1) and Data link (HA2), while others require you to use the in-band ports as HA links.

On firewalls with dedicated HA ports such as the PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7000 Series firewalls (see [HA Ports on the PA-7000 Series Firewall](#)), use the dedicated HA ports to manage communication and synchronization between the firewalls. For firewalls without dedicated HA ports such as the PA-200, PA-500, and PA-2000 Series firewalls, as a best practice use the management port for the HA1 link to allow for a direct connection between the management planes on the firewalls, and an in-band port for the HA2 link.



The HA1 and HA2 links provide synchronization for functions that reside on the management plane. Using the dedicated HA interfaces on the management plane is more efficient than using the in-band ports as this eliminates the need to pass the synchronization packets over the dataplane.

- **Control Link:** The HA1 link is used to exchange hellos, heartbeats, and HA state information, and management plane sync for routing, and User-ID information. The firewalls also use this link to synchronize configuration changes with its peer. The HA1 link is a Layer 3 link and requires an IP address.

**Ports used for HA1:** TCP port 28769 and 28260 for clear text communication; port 28 for encrypted communication (SSH over TCP).

- **Data Link:** The HA2 link is used to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between firewalls in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active or active-primary firewall to the passive or active-secondary firewall. The HA2 link is a Layer 2 link, and it uses ether type 0x7261 by default.

**Ports used for HA2:** The HA data link can be configured to use either IP (protocol number 99) or UDP (port 29281) as the transport, and thereby allow the HA data link to span subnets.

Additionally, an HA3 link is used in Active/Active HA deployments. When there is an asymmetric route, the HA3 link is used for forwarding packets to the HA peer that owns the session. The HA3 link is a Layer 2 link and it does not support Layer 3 addressing or encryption.

- **Backup Links:** Provide redundancy for the HA1 and the HA2 links. In-band ports are used as backup links for both HA1 and HA2. Consider the following guidelines when configuring backup HA links:

- The IP addresses of the primary and backup HA links must not overlap each other.
- HA backup links must be on a different subnet from the primary HA links.
- HA1-backup and HA2-backup ports must be configured on separate physical ports. The HA1-backup link uses port 28770 and 28260.



Palo Alto Networks recommends enabling heartbeat backup (uses port 28771 on the MGT interface) if you use an in-band port for the HA1 or the HA1 backup links.

- **Packet-Forwarding Link:** In addition to the HA1 and HA2 links, an active/active deployment also requires a dedicated HA3 link. The firewalls use this link for forwarding packets to the peer during session setup and asymmetric traffic flow. The HA3 link is a Layer 2 link that uses MAC-in-MAC encapsulation; it does not support Layer 3 addressing or encryption. You can configure aggregate interfaces on the PA-3000 Series, PA-4000 Series, PA-5000 Series and PA-7000 Series firewalls as an HA3 link. The aggregate interfaces can also provide redundancy for the HA3 link; you cannot configure backup links for the HA3 link.

## HA Ports on the PA-7000 Series Firewall

HA connectivity on the PA-7000 Series mandates the use of specific ports on the Switch Management Card (SMC) for certain functions; for other functions, you can use the ports on the Network Processing Card (NPC). The PA-7000 Series firewalls synchronize sessions across the NPCs one-for-one.

Use the following table for information on the SMC ports that are designed for HA connectivity:

HA Links and Backup Links	Ports on the SMC	Description
<b>Control Link</b>	HA1-A Speed: Ethernet 10/100/1000	Used for HA control and synchronization in both <a href="#">HA Modes</a> . Connect this port directly from the HA1-A port on the first firewall to the HA1-A on the second firewall in the pair, or connect them together through a switch or router.  HA1 cannot be configured on NPC data ports or the MGT port.
<b>Control Link Backup</b>	HA1-B Speed: Ethernet 10/100/1000 port	Used for HA control and synchronization as a backup for HA1-A in both <a href="#">HA Modes</a> . Connect this port directly from the HA1-B port on the first firewall to the HA1-B on the second firewall in the pair, or connect them together through a switch or router.  HA1 Backup cannot be configured on NPC data ports or the MGT port.
<b>Data Link</b>  <b>Data Link Backup</b>	HSCI-A	The High Speed Chassis Interconnect (HSCI) ports are Quad Port SFP (QSFP) interfaces which are used to connect two PA-7000 Series firewalls in an HA configuration. Each port is comprised of four 10 gigabit links internally for a combined speed of 40 gigabits.
	HSCI-B	<p>The HSCI ports are not routable and must be connected directly to each other. The HSCI-A on the first chassis connects directly to HSCI-A on the second chassis and HSCI-B on the first chassis connects to HSCI-B on the second chassis. This will provide full 80 gigabit transfer rates. In software, both ports (HSCI-A and HSCI-B) are treated as one HA interface.</p> <p>Palo Alto Networks recommends using the dedicated HSCI ports for the HA2 link; the HA3 link must use the HSCI port. If the firewalls are deployed in:</p> <ul style="list-style-type: none"> <li>• an active/active configuration, the HA3 link must use the HSCI port. The HA2 link and HA2 backup links can use the HSCI port or data ports on the NPC.</li> <li>• an active/passive configuration, you can configure a data port on the NPC for the HA2 link or the HA2 backup link, if needed.</li> </ul>

For an overview of the Modules and Interface cards on the PA-7000 Series firewall, refer to the [PA-7000 Series Hardware Reference Guide](#).

## Device Priority and Preemption

The firewalls in an HA pair can be assigned a *device priority* value to indicate a preference for which firewall should assume the active or active-primary role. If you need to use a specific firewall in the HA pair for actively securing traffic, you must enable the preemptive behavior on both the firewalls and assign a device priority value for each firewall. The firewall with the lower numerical value, and therefore *higher priority*, is designated as active or active-primary. The other firewall is the active-secondary or passive firewall.

By default, preemption is disabled on the firewalls and must be enabled on both firewalls. When enabled, the preemptive behavior allows the firewall with the *higher priority* (lower numerical value) to resume as active or active-primary after it recovers from a failure. When preemption occurs, the event is logged in the system logs.

## Failover Triggers

When a failure occurs on one firewall and the peer takes over the task of securing traffic, the event is called a *failover*. A failover is triggered when a monitored metric on a firewall in the HA pair fails. The metrics that are monitored for detecting a firewall failure are:

- **Heartbeat Polling and Hello messages**

The firewalls use hello message and heartbeats to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other at the configured *Hello Interval* to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer over the control link, and the peer responds to the ping to establish that the firewalls are connected and responsive. By default, the interval for the heartbeat is 1000 milliseconds. For details on the HA timers that trigger a failover, see [HA Timers](#).

- **Link Monitoring**

The physical interfaces to be monitored are grouped into a link group and their state (link up or link down) is monitored. A link group can contain one or more physical interfaces. A firewall failure is triggered when any or all of the interfaces in the group fail. The default behavior is failure of any one link in the link group will cause the firewall to change the HA state to non-functional to indicate a failure of a monitored object.

- **Path Monitoring**

Monitors the full path through the network to mission-critical IP addresses. ICMP pings are used to verify reachability of the IP address. The default interval for pings is 200ms. An IP address is considered unreachable when 10 consecutive pings (the default value) fail, and a firewall failure is triggered when any or all of the IP addresses monitored become unreachable. The default behavior is any one of the IP addresses becoming unreachable will cause the firewall to change the HA state to non-functional to indicate a failure of a monitored object.

In addition to the failover triggers listed above, a failover also occurs when the administrator places the firewall in a suspended state or if preemption occurs.

On the PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls, a failover can occur when an internal health check fails. This health check is not configurable and is enabled to verify the operational status for all the components within the firewall.

## HA Timers

High availability (HA) timers are used to detect a firewall failure and trigger a failover. To reduce the complexity in configuring HA timers, you can select from three profiles: **Recommended**, **Aggressive** and **Advanced**. These profiles auto-populate the optimum HA timer values for the specific firewall platform to enable a speedier HA deployment.

Use the **Recommended** profile for typical failover timer settings and the **Aggressive** profile for faster failover timer settings. The **Advanced** profile allows you to customize the timer values to suit your network requirements.

The following table describes each timer included in the profiles and the current preset values across the different hardware models; these values are for current reference only and can change in a subsequent release.

**Recommended/Aggressive HA Timer Values by Platform**

Timers	Description	PA-7000 Series PA-5000 Series PA-4000 Series PA-3000 Series VM-Series	PA-2000 Series PA-500 Series PA-200 Series	Panorama Virtual Appliance Panorama M-Series
Monitor fail hold up time	Interval during which the firewall will remain active following a path monitor or link monitor failure. This setting is recommended to avoid an HA failover due to the occasional flapping of neighboring devices.	0/0	0/0	0/0
Preemption hold time	Time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall.	1/1	1/1	1/1
Heartbeat interval	Frequency at which the HA peers exchange heartbeat messages in the form of an ICMP (ping).	1000/1000 2000/1000 (only for VM-Series in AWS)	2000/1000	2000/1000

<b>Timers</b>	<b>Description</b>	<b>PA-7000 Series</b> <b>PA-5000 Series</b> <b>PA-4000 Series</b> <b>PA-3000 Series</b> <b>VM-Series</b>	<b>PA-2000 Series</b> <b>PA-500 Series</b> <b>PA-200 Series</b>	<b>Panorama Virtual Appliance</b> <b>Panorama M-Series</b>
Promotion hold time	Time that the passive firewall (in active/passive mode) or the active-secondary firewall (in active/active mode) will wait before taking over as the active or active-primary firewall after communications with the HA peer have been lost. This hold time will begin only after the peer failure declaration has been made.	2000/500	2000/500	2000/500
Additional master hold up time	Time interval that is applied to the same event as Monitor Fail Hold Up Time (range 0-60000 ms, default 500 ms). The additional time interval is applied only to the active firewall in active/passive mode and to the active-primary firewall in active/active mode. This timer is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously.	500/500	500/500	7000/5000
Hello interval	Interval in milliseconds between hello packets that are sent to verify that the HA functionality on the other firewall is operational. The range is 8000-60000 ms with a default of 8000 ms for all platforms.	8000/8000	8000/8000	8000/8000

Timers	Description	PA-7000 Series PA-5000 Series PA-4000 Series PA-3000 Series VM-Series	PA-2000 Series PA-500 Series PA-200 Series	Panorama Virtual Appliance Panorama M-Series
Maximum no. of flaps	A flap is counted when the firewall leaves the active state within 15 minutes after it last left the active state. This value indicates the maximum number of flaps that are permitted before the firewall is determined to be suspended and the passive firewall takes over (range 0-16; default 3).	3/3	3/3	Not Applicable

## Set Up Active/Passive HA

- ▲ Prerequisites for Active/Passive HA
- ▲ Configuration Guidelines for Active/Passive HA
- ▲ Configure Active/Passive HA
- ▲ Define HA Failover Conditions
- ▲ Verify Failover

## Prerequisites for Active/Passive HA

To set up high availability on your Palo Alto Networks firewalls, you need a pair of firewalls that meet the following requirements:

- The same model**—Both the firewalls in the pair must be of the same hardware model or virtual machine model.
- The same PAN-OS version**—Both the firewalls should be running the same PAN-OS version and must each be up-to-date on the application, URL, and threat databases. They must also both have the same multiple virtual systems capability (single or multi vsys).
- The same type of interfaces**—Dedicated HA links, or a combination of the management port and in-band ports that are set to *interface type* HA.
  - Determine the IP address for the HA1 (control) connection between the HA peers. The HA1 IP address for both peers must be on the same subnet if they are directly connected or are connected to the same switch.  
For firewalls without dedicated HA ports, you can use the management port for the control connection. Using the management port provides a direct communication link between the management planes on both firewalls. However, because the management ports will not be directly cabled between the peers, make sure that you have a route that connects these two interfaces across your network.
  - If you use Layer 3 as the transport method for the HA2 (data) connection, determine the IP address for the HA2 link. Use Layer 3 *only* if the HA2 connection must communicate over a routed network. The IP subnet for the HA2 links must not overlap with that of the HA1 links or with any other subnet assigned to the data ports on the firewall.
- The same set of licenses**—Licenses are unique to each firewall and cannot be shared between the firewalls. Therefore, you must license both firewalls identically. If both firewalls do not have an identical set of licenses, they cannot synchronize configuration information and maintain parity for a seamless failover.



If you have an existing firewall and you want to add a new firewall for HA purposes and the new firewall has an existing configuration, it is recommended that you [Reset the Firewall to Factory Default Settings](#) on the new firewall. This will ensure that the new firewall has a clean configuration. After HA is configured, you will then sync the configuration on the primary firewall to the newly introduced firewall with the clean config.

## Configuration Guidelines for Active/Passive HA

To set up an active (PeerA) passive (PeerB) pair in HA, you must configure some options identically on both firewalls and some independently (non-matching) on each firewall. These HA settings are not synchronized between the firewalls. For details on what is/is not synchronized, refer to [HA Synchronization](#).

To proceed with the instructions on configuring the firewalls in HA, see [Configure Active/Passive HA](#).

The following table lists the settings that you must configure identically on both firewalls:

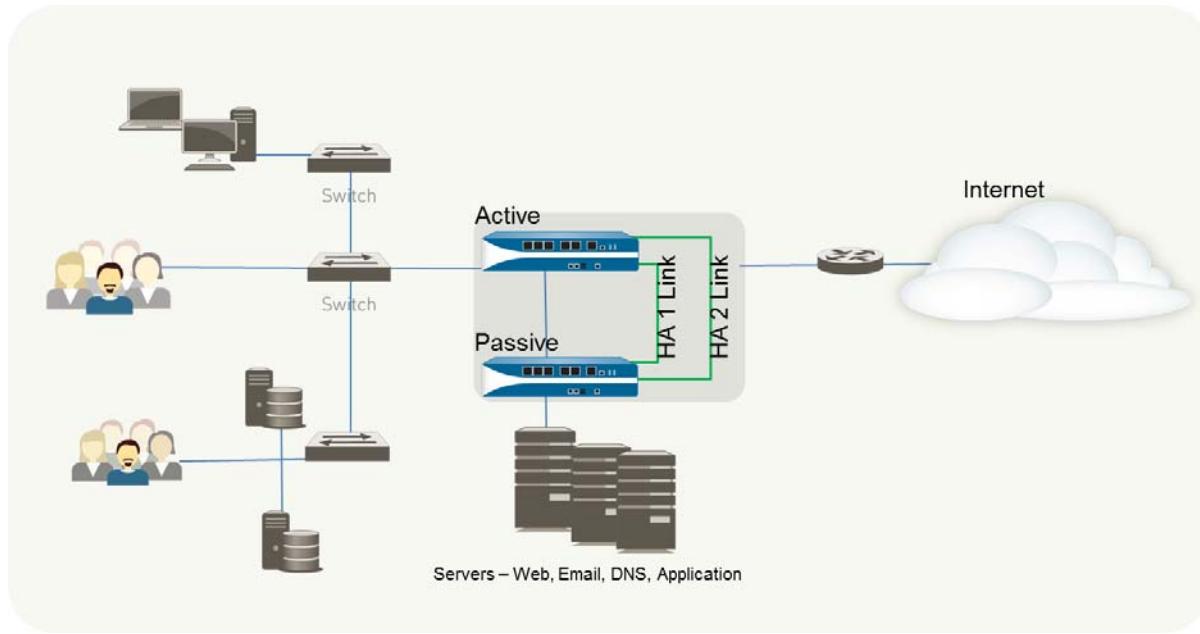
Identical Configuration Settings on PeerA and PeerB
<ul style="list-style-type: none"><li>• HA must be enabled on both firewalls.</li><li>• Both firewalls must have the same Group ID value. The Group ID value is used to create a virtual MAC address for all the configured interfaces. The format of the virtual MAC is 00-1B-17:00: xx: yy where 00-1B-17: vendor ID; 00: fixed; xx: HA group ID; yy: interface ID. When a new active firewall takes over, Gratuitous ARP messages are sent from each of the connected interfaces of the new active member to inform the connected Layer 2 switches of the virtual MAC address' new location.</li><li>• If using in-band ports, the interfaces for the HA1 and HA2 links must be set to type HA.</li><li>• The HA mode must be set to Active Passive.</li><li>• If required, preemption must be enabled on both firewalls. The device priority value, however, must not be identical.</li><li>• If required, encryption on the HA1 link (for communication between the HA peers) must be configured on both firewalls.</li><li>• Based on the combination of HA1 and HA1 Backup ports you are using, use the following recommendations to decide whether you should enable heartbeat backup:<ul style="list-style-type: none"><li>• HA1: Dedicated HA1 port HA1 Backup: In-band port Recommendation: Enable Heartbeat Backup</li><li>• HA1: Dedicated HA1 port HA1 Backup: Management port Recommendation: Do not enable Heartbeat Backup</li><li>• HA1: In-band port HA1 Backup: In-band port Recommendation: Enable Heartbeat Backup</li><li>• HA1: Management port HA1 Backup: In-band port Recommendation: Do not enable Heartbeat Backup</li></ul></li></ul>

The following table lists the settings that must be configured independently on each firewall:

Independent Configuration Settings	PeerA	PeerB
Control Link	IP address of the HA1 link configured on this firewall (PeerA).	IP address of the HA1 link configured on this firewall (PeerB).
	For firewalls without dedicated HA ports, use the management port IP address for the control link.	
Data Link The data link information is synchronized between the firewalls after HA is enabled and the control link is established between the firewalls.	By default, the HA2 link uses Ethernet/Layer 2. If using a Layer 3 connection, configure the IP address for the data link on this firewall (PeerA).	By default, the HA2 link uses Ethernet/Layer 2. If using a Layer 3 connection, configure the IP address for the data link on this firewall (PeerB).
Device Priority (required, if preemption is enabled)	The firewall you plan to make active must have a lower numerical value than its peer. So, if Peer A is to function as the active firewall, keep the default value of 100 and increment the value on PeerB.	If PeerB is passive, set the device priority value to a number larger than that on PeerA. For example, set the value to 110.
Link Monitoring— Monitor one or more physical interfaces that handle vital traffic on this firewall and define the failure condition.	Select the physical interfaces on the firewall that you would like to monitor and define the failure condition (all or any) to trigger a failover.	Pick a similar set of physical interfaces that you would like to monitor on this firewall and define the failure condition (all or any) to trigger a failover.
Path Monitoring— Monitor one or more destination IP addresses that the firewall can use ICMP pings to ascertain responsiveness.	Define the failure condition (all or any), ping interval and the ping count. This is particularly useful for monitoring the availability of other interconnected networking devices. For example, monitor the availability of a router that connects to a server, connectivity to the server itself, or some other vital device that is in the flow of traffic.  Make sure that the node/device that you are monitoring is not likely to be unresponsive, especially when it comes under load, as this could cause a path monitoring failure and trigger a failover.	Pick a similar set of devices or destination IP addresses that can be monitored for determining the failover trigger for PeerB. Define the failure condition (all or any), ping interval and the ping count.

## Configure Active/Passive HA

The following procedure shows how to configure a pair of firewalls in an active/passive deployment as depicted in the following example topology.



### Connect and Configure the Firewalls

**Step 1** Connect the HA ports to set up a physical connection between the firewalls.

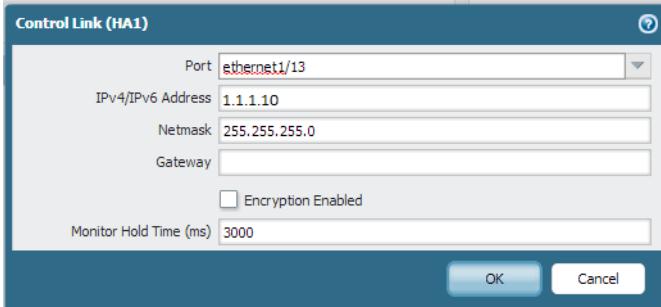
- For firewalls with dedicated HA ports, use an Ethernet cable to connect the dedicated HA1 ports and the HA2 ports on peers. Use a crossover cable if the peers are directly connected to each other.
  - For firewalls without dedicated HA ports, select two data interfaces for the HA2 link and the backup HA1 link. Then, use an Ethernet cable to connect these in-band HA interfaces across both firewalls.
- Use the management port for the HA1 link and ensure that the management ports can connect to each other across your network.

Pick a firewall in the pair and complete the following steps:

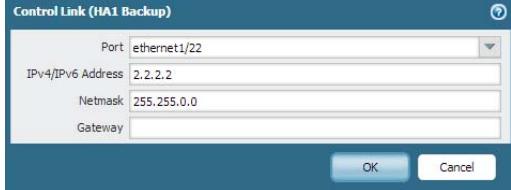
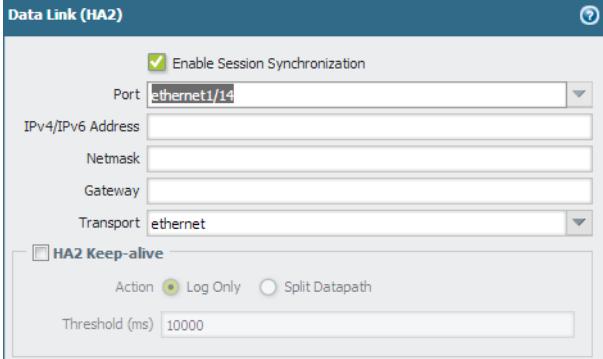
**Step 2** Enable ping on the management port.  
Enabling ping allows the management port to exchange heartbeat backup information.

- Select **Device > Setup > Management** and then click the Edit icon in the Management Interface Settings section of the screen.
- Select **Ping** as a service that is permitted on the interface.

### Connect and Configure the Firewalls (Continued)

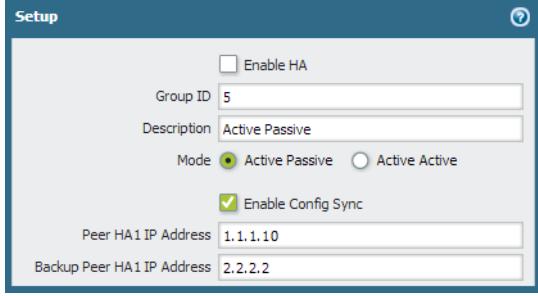
<p><b>Step 3</b> If the firewall does not have dedicated HA ports, set up the data ports to function as HA ports.</p> <p>For firewalls with dedicated HA ports continue to the next step.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces</b>.</li> <li>2. Confirm that the link is up on the ports that you want to use.</li> <li>3. Select the interface and set <b>Interface Type</b> to <b>HA</b>.</li> </ol> <table border="1" data-bbox="824 369 1460 454"> <thead> <tr> <th>Interface</th><th>Interface Type</th><th>Management Profile</th><th>Link State</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>ether1/1</td><td>HA</td><td></td><td>Up</td><td>none</td></tr> </tbody> </table> <ol style="list-style-type: none"> <li>4. Set the <b>Link Speed</b> and <b>Link Duplex</b> settings, as appropriate.</li> </ol>	Interface	Interface Type	Management Profile	Link State	IP Address	ether1/1	HA		Up	none
Interface	Interface Type	Management Profile	Link State	IP Address							
ether1/1	HA		Up	none							
<p><b>Step 4</b> Set the HA mode and group ID.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; High Availability &gt; General</b> and edit the Setup section.</li> <li>2. Set a <b>Group ID</b> and optionally a <b>Description</b> for the pair. The Group ID uniquely identifies each HA pair on your network. If you have multiple HA pairs that share the same broadcast domain you must set a unique Group ID for each pair.</li> <li>3. Set the mode to <b>Active Passive</b>.</li> </ol>										
<p><b>Step 5</b> Set up the control link connection.</p> <p>This example shows an in-band port that is set to interface type HA.</p> <p>For firewalls that use the management port as the control link, the IP address information is automatically pre-populated.</p>	<ol style="list-style-type: none"> <li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Control Link (HA1) section.</li> <li>2. Select the <b>Port</b> that you have cabled for use as the HA1 link.</li> <li>3. Set the <b>IPv4/IPv6 Address</b> and <b>Netmask</b>.</li> </ol> <p>If the HA1 interfaces are on separate subnets, enter the IP address of the <b>Gateway</b>. Do not add a gateway address if the firewalls are directly connected</p> 										
<p><b>Step 6</b> (Optional) Enable encryption for the control link connection.</p> <p>This is typically used to secure the link if the two firewalls are not directly connected, that is if the ports are connected to a switch or a router.</p>	<ol style="list-style-type: none"> <li>1. Export the HA key from one firewall and import it into the peer firewall.             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; Certificates</b>.</li> <li>b. Select <b>Export HA key</b>. Save the HA key to a network location that the peer can access.</li> <li>c. On the peer firewall, select <b>Device &gt; Certificate Management &gt; Certificates</b>, and select <b>Import HA key</b> to browse to the location that you saved the key and import it in to the peer.</li> </ol> </li> <li>2. Select <b>Device &gt; High Availability &gt; General</b>, edit the Control Link (HA1) section.</li> <li>3. Select <b>Encryption Enabled</b>.</li> </ol>										

### Connect and Configure the Firewalls (Continued)

<p><b>Step 7</b> Set up the backup control link connection.</p>	<ol style="list-style-type: none"> <li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Control Link (HA1 Backup) section.</li> <li>2. Select the HA1 backup interface and set the <b>IPv4/IPv6 Address</b> and <b>Netmask</b>.</li> </ol> 
<p><b>Step 8</b> Set up the data link connection (HA2) and the backup HA2 connection between the firewalls.</p>	<ol style="list-style-type: none"> <li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Data Link (HA2) section.</li> <li>2. Select the <b>Port</b> to use for the data link connection.</li> <li>3. Select the <b>Transport</b> method. The default is <b>ethernet</b>, and will work when the HA pair is connected directly or through a switch. If you need to route the data link traffic through the network, select <b>IP</b> or <b>UDP</b> as the transport mode.</li> <li>4. If you use IP or UDP as the transport method, enter the <b>IPv4/IPv6 Address</b> and <b>Netmask</b>.</li> </ol>  <p>5. Verify that <b>Enable Session Synchronization</b> is selected.</p> <p>6. Select <b>HA2 Keep-alive</b> to enable monitoring on the HA2 data link between the HA peers. If a failure occurs based on the threshold that is set (default is 10000 ms), the defined action will occur. For active/passive configuration, a critical system log message is generated when an HA2 keep-alive failure occurs.</p> <p> You can configure the HA2 keep-alive option on both firewalls, or just one firewall in the HA pair. If the option is only enabled on one firewall, only that firewall will send the keep-alive messages. The other firewall will be notified if a failure occurs.</p> <p>7. Edit the <b>Data Link (HA2 Backup)</b> section, select the interface, and add the <b>IPv4/IPv6 Address</b> and <b>Netmask</b>.</p>

Connect and Configure the Firewalls (Continued)	
<p><b>Step 9</b> Enable heartbeat backup if your control link uses a dedicated HA port or an in-band port.</p> <p>You do not need to enable heartbeat backup if you are using the management port for the control link.</p>	<ol style="list-style-type: none"><li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Election Settings.</li><li>2. Select <b>Heartbeat Backup</b>.</li></ol> <p>To allow the heartbeats to be transmitted between the firewalls, you must verify that the management port across both peers can route to each other.</p> <p> Enabling heartbeat backup also allows you to prevent a split-brain situation. Split brain occurs when the HA1 link goes down causing the firewall to miss heartbeats, although the firewall is still functioning. In such a situation, each peer believes that the other is down and attempts to start services that are running, thereby causing a split brain. When the heartbeat backup link is enabled, split brain is prevented because redundant heartbeats and hello messages are transmitted over the management port.</p>
<p><b>Step 10</b> Set the device priority and enable preemption.</p> <p>This setting is only required if you wish to make sure that a specific firewall is the preferred active firewall. For information, see <a href="#">Device Priority and Preemption</a>.</p>	<ol style="list-style-type: none"><li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Election Settings.</li><li>2. Set the numerical value in <b>Device Priority</b>. Make sure to set a lower numerical value on the firewall that you want to assign a higher priority to.  If both firewalls have the same device priority value, the firewall with the lowest MAC address on the HA1 control link will become the active firewall.</li><li>3. Select <b>Preemptive</b>.</li></ol> <p>You must enable preemptive on both the active firewall and the passive firewall.</p>
<p><b>Step 11</b> (Optional) Modify the failover timers.</p> <p>By default, the HA timer profile is set to the <b>Recommended</b> profile and is suited for most HA deployments.</p>	<ol style="list-style-type: none"><li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Election Settings.</li><li>2. Select the <b>Aggressive</b> profile for triggering failover faster; select <b>Advanced</b> to define custom values for triggering failover in your set up.  To view the preset value for an individual timer included in a profile, select <b>Advanced</b> and click <b>Load Recommended</b> or <b>Load Aggressive</b>. The preset values for your hardware model will be displayed on screen.</li></ol>

### Connect and Configure the Firewalls (Continued)

<p><b>Step 12</b> (Optional, only configured on the passive firewall) Modify the link status of the HA ports on the passive firewall.</p> <p> The passive link state is <b>shutdown</b>, by default. After you enable HA, the link state for the HA ports on the active firewall will be green and those on the passive firewall will be down and display as red.</p>	<p>Setting the link state to <b>Auto</b> allows for reducing the amount of time it takes for the passive firewall to take over when a failover occurs and it allows you to monitor the link state.</p> <p>To enable the link status on the passive firewall to stay up and reflect the cabling status on the physical interface:</p> <ol style="list-style-type: none"> <li>1. In <b>Device &gt; High Availability &gt; General</b>, edit the Active Passive Settings.</li> <li>2. Set the <b>Passive Link State</b> to <b>Auto</b>.</li> </ol> <p>The auto option decreases the amount of time it takes for the passive firewall to take over when a failover occurs.</p> <p> Although the interface displays green (as cabled and up) it continues to discard all traffic until a failover is triggered.</p> <p>When you modify the passive link state, make sure that the adjacent devices do not forward traffic to the passive firewall based only on the link status of the firewall.</p>
<p><b>Step 13</b> Enable HA.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; High Availability &gt; General</b> and edit the Setup section.</li> <li>2. Select <b>Enable HA</b>.</li> <li>3. Select <b>Enable Config Sync</b>. This setting enables the synchronization of the configuration settings between the active and the passive firewall.</li> <li>4. Enter the IP address assigned to the control link of the peer in <b>Peer HA1 IP Address</b>.</li> </ol>  <p>For firewalls without dedicated HA ports, if the peer uses the management port for the HA1 link, enter the management port IP address of the peer.</p> <ol style="list-style-type: none"> <li>5. Enter the <b>Backup HA1 IP Address</b>.</li> </ol>
<p><b>Step 14</b> Save your configuration changes.</p>	<p>Click <b>Commit</b>.</p>
<p><b>Step 15</b> Complete <a href="#">Step 2</a> through <a href="#">Step 14</a> on the other firewall in the HA pair.</p>	

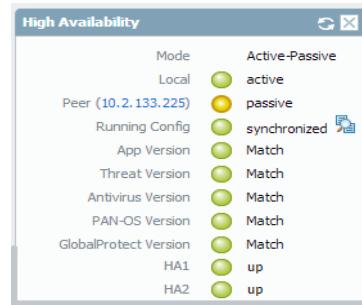
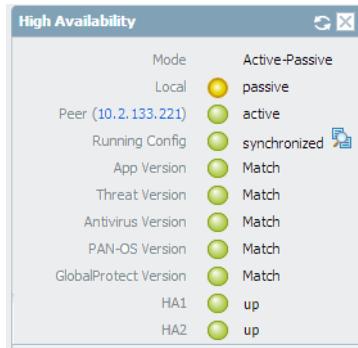
**Connect and Configure the Firewalls (Continued)**

**Step 16** After you finish configuring both firewalls, verify that the firewalls are paired in active/passive HA.

1. Access the **Dashboard** on both firewalls, and view the High Availability widget.
2. On the active firewall, click the **Sync to peer** link.
3. Confirm that the firewalls are paired and synced, as shown below:

On the passive firewall: the state of the local firewall should display **passive** and the Running Config should show as **synchronized**.

On the active firewall: The state of the local firewall should display **active** and the Running Config should show as **synchronized**.



## Define HA Failover Conditions

### Configure the Failover Triggers

<p><b>Step 1</b> To configure link monitoring, define the interfaces that you would like to monitor. A change in the link state of these interface will trigger a failover.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; High Availability &gt; Link and Path Monitoring</b> and <b>Add</b> a Link Group.</li> <li>2. Name the <b>Link Group</b>, <b>Add</b> the interfaces to monitor, and select the <b>Failure Condition</b> for the group. The Link group you define is added to the <b>Link Group</b> section.</li> </ol>
---	---

Link Group				
	Name	Enabled	Group Failure Condition	Interfaces
<input checked="" type="checkbox"/>	Main	<input checked="" type="checkbox"/>	any	ethernet1/11 ethernet1/15 ethernet1/21
<b>[+ Add] [Delete]</b>				

<p><b>Step 2</b> (Optional) Modify the failure condition for the Link Groups that you configured (in the preceding step) on the firewall. By default, the firewall will trigger a failover when any monitored link fails.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Link Monitoring</b> section.</li> <li>2. Set the <b>Failure Condition</b> to <b>All</b>. The default setting is <b>Any</b>.</li> </ol>																												
<p><b>Step 3</b> To configure path monitoring, define the destination IP addresses that the firewall should ping to verify network connectivity.</p>	<ol style="list-style-type: none"> <li>1. In the <b>Path Group</b> section of the <b>Device &gt; High Availability &gt; Link and Path Monitoring</b> tab, pick the <b>Add option for your set up</b>: Virtual Wire, VLAN, or Virtual Router.</li> <li>2. Select the appropriate item from the drop-down for the <b>Name</b> and <b>Add</b> the IP addresses (source and/or destination, as prompted) that you wish to monitor. Then select the <b>Failure Condition</b> for the group. The path group you define is added to the <b>Path Group</b> section.</li> </ol>																												
	<table border="1"> <thead> <tr> <th colspan="7">Path Group</th> </tr> <tr> <th></th> <th>Name</th> <th>Type</th> <th>Enabled</th> <th>Failure Condition</th> <th>Source IP</th> <th>Destination IP</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td><td>VR.2</td><td>virtual-router</td><td><input checked="" type="checkbox"/></td><td>all</td><td></td><td>10.2.2.5 10.2.2.2 10.2.2.3 10.2.2.4</td></tr> <tr> <td colspan="4"><b>[+ Add Virtual Wire Path] [+ Add VLAN Path] [+ Add Virtual Router Path] [Delete]</b></td><td></td><td></td><td></td></tr> </tbody> </table>	Path Group								Name	Type	Enabled	Failure Condition	Source IP	Destination IP	<input checked="" type="checkbox"/>	VR.2	virtual-router	<input checked="" type="checkbox"/>	all		10.2.2.5 10.2.2.2 10.2.2.3 10.2.2.4	<b>[+ Add Virtual Wire Path] [+ Add VLAN Path] [+ Add Virtual Router Path] [Delete]</b>						
Path Group																													
	Name	Type	Enabled	Failure Condition	Source IP	Destination IP																							
<input checked="" type="checkbox"/>	VR.2	virtual-router	<input checked="" type="checkbox"/>	all		10.2.2.5 10.2.2.2 10.2.2.3 10.2.2.4																							
<b>[+ Add Virtual Wire Path] [+ Add VLAN Path] [+ Add Virtual Router Path] [Delete]</b>																													
<p><b>Step 4</b> (Optional) Modify the failure condition for all Path Groups configured on the firewall. By default, the firewall will trigger a failover when any monitored path fails.</p>	<p>Set the <b>Failure Condition</b> to <b>All</b>. The default setting is <b>Any</b>.</p>																												
<p><b>Step 5</b> Save your changes.</p>	<p>Click <b>Commit</b>.</p>																												

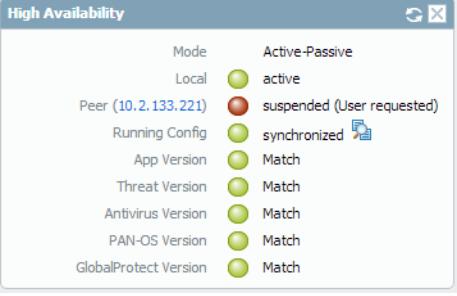


If you are using SNMPv3 to monitor the firewalls, note that the SNMPv3 Engine ID is unique to each firewall; the EngineID is not synchronized between the HA pair and, therefore, allows you to independently monitor each firewall in the HA pair. For information on setting up SNMP, see [Forward Traps to an SNMP Manager](#).

Because the EngineID is generated using the firewall serial number, on the VM-Series firewall you must apply a valid license in order to obtain a unique EngineID for each firewall.

## Verify Failover

To test that your HA configuration works properly, trigger a manual failover and verify that the firewalls transition states successfully.

<b>Verify Failover</b>	
<b>Step 1</b> Suspend the active firewall.	Select <b>Device &gt; High Availability &gt; Operational Commands</b> and click the <b>Suspend local device</b> link.
<b>Step 2</b> Verify that the passive firewall has taken over as active.	On the <b>Dashboard</b> , verify that the state of the passive firewall changes to <b>active</b> in the High Availability widget.
<b>Step 3</b> Restore the suspended firewall to a functional state. Wait for a couple minutes, and then verify that preemption has occurred, if preemptive is enabled.	<p>1. On the firewall you previously suspended, select <b>Device &gt; High Availability &gt; Operational Commands</b> and click the <b>Make local device functional</b> link.</p>  <p>2. In the High Availability widget on the <b>Dashboard</b>, confirm that the firewall has taken over as the active firewall and that the peer is now in a passive state.</p> 

## Reference: HA Synchronization

If you have enabled configuration synchronization on both peers in an HA pair, most of the configuration settings you configure on one peer will automatically sync to the other peer upon commit. To avoid configuration conflicts, always make configuration changes on the active (active/passive) or active-primary (active/active) peer and wait for the changes to sync to the peer before making any additional configuration changes.

The following topics identify what portions of a firewall configuration must be configured on each device independently (rather than synchronized from the HA peer).

- ▲ [What Settings Don't Sync in Active/Passive HA?](#)
- ▲ [What Settings Don't Sync in Active/Active HA?](#)
- ▲ [Synchronization of System Runtime Information](#)

### What Settings Don't Sync in Active/Passive HA?

You must configure the following settings on each firewall in an HA pair in an active/passive deployment. These settings do not sync from one peer to another:

Configuration Item	What Doesn't Sync in Active/Passive?
Management Interface Settings	<p>All management configuration settings must be configured individually on each device, including:</p> <ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Management &gt; General Settings</b>—Hostname, Domain, Login Banner, Time Zone, Locale, Date, Time, Latitude, Longitude</li> <li>• <b>Device &gt; Setup &gt; Management Interface Settings</b>—IP Address, Netmask, Default Gateway, IPv6 Address/Prefix Length, Default IPv6 Gateway, Speed, MTU, and Services (HTTP, HTTP OCSP, HTTPS, Telnet, SSH, Ping, SNMP, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP)</li> </ul>
Multi-vsyst Capability	<p>To enable multi-vsyst you must activate the Virtual Systems license (required to enable support for multiple virtual systems on PA-2000 Series and PA-3000 Series firewalls or to increase the number of virtual systems beyond the base number provided by default on PA-4000 Series, PA-5000 Series, and PA-7000 Series firewalls) on each firewall in the pair.</p> <p>In addition, you must also enable <b>Multi Virtual System Capability</b> on each firewall (<b>Device &gt; Setup &gt; Management &gt; General Settings</b>).</p>
Administrator Authentication Settings	<p>You must define the authentication profile and certificate profile for administrative access to the firewall locally on each firewall (<b>Device &gt; Setup &gt; Management &gt; Authentication</b>).</p>
Panorama Settings	<p>Set the following Panorama settings on each firewall (<b>Device &gt; Setup &gt; Management &gt; Panorama Settings</b>).</p> <ul style="list-style-type: none"> <li>• <b>Panorama Servers</b></li> <li>• <b>Disable Panorama Policy and Objects</b> and <b>Disable Device and Network Template</b></li> </ul>

Configuration Item	What Doesn't Sync in Active/Passive?
SNMP	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Operations &gt; SNMP Setup</b></li> </ul>
Statistics Collection	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Operations &gt; Statistics Service Setup</b></li> </ul>
Services	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Services</b></li> </ul>
Global Service Routes	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Services &gt; Service Route Configuration</b></li> </ul>
Data Protection	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Content-ID &gt; Manage Data Protection</b></li> </ul>
Jumbo Frames	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Session &gt; Session Settings &gt; Enable Jumbo Frame</b></li> </ul>
Forward Proxy Server Certificate Settings	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Session &gt; Decryption Settings &gt; SSL Forward Proxy Settings</b></li> </ul>
Master Key Secured by HSM	<ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; HSM &gt; Hardware Security Module Provider &gt; Master Key Secured by HSM</b></li> </ul>
Log Export Settings	<ul style="list-style-type: none"> <li>• <b>Device &gt; Scheduled Log Export</b></li> </ul>
Software Updates	<p>With software updates, you can either download and install them separately on each device, or download them on one peer and sync the update to the other peer. You must install the update on each peer.</p> <ul style="list-style-type: none"> <li>• <b>Device &gt; Software</b></li> </ul>
GlobalProtect Agent Package	<p>With GlobalProtect client updates, you can either download and install them separately on each device, or download them to one peer and sync the update to the other peer. You must activate separately on each peer.</p> <ul style="list-style-type: none"> <li>• <b>Device &gt; GlobalProtect Client</b></li> </ul>
Content Updates	<p>With content updates, you can either download and install them separately on each device, or download them on one peer and sync the update to the other peer. You must install the update on each peer.</p> <ul style="list-style-type: none"> <li>• <b>Device &gt; Dynamic Updates</b></li> </ul>
Licenses/Subscriptions	<ul style="list-style-type: none"> <li>• <b>Device &gt; Licenses</b></li> </ul>
Support Subscription	<ul style="list-style-type: none"> <li>• <b>Device &gt; Support</b></li> </ul>
Master Key	<p>The master key must be identical on each firewall in the HA pair, but you must manually enter it on each device (<b>Device &gt; Master Key and Diagnostics</b>).</p> <p>Before changing the master key, you must disable config sync on both peers (<b>Device &gt; High Availability &gt; General &gt; Setup</b> and clear the <b>Enable Config Sync</b> check box) and then re-enable it after you change the keys.</p>
Reports, logs, and Dashboard Settings	<p>Log data, reports, and Dashboard data and settings (column display, widgets) are not synced between peers. Report configuration settings, however, are synced.</p>

## What Settings Don't Sync in Active/Active HA?

You must configure the following settings on each firewall in an HA pair in an active/active deployment. These settings do not sync from one peer to another:

Configuration Item	What Doesn't Sync?
Management Interface Settings	All management configuration settings must be configured individually on each device, including: <ul style="list-style-type: none"> <li>• <b>Device &gt; Setup &gt; Management &gt; General Settings</b>—Hostname, Domain, Login Banner, Time Zone, Locale, Date, Time, Latitude, Longitude</li> <li>• <b>Device &gt; Setup &gt; Management &gt; Management Interface Settings</b>—IP Address, Netmask, Default Gateway, IPv6 Address/Prefix Length, Default IPv6 Gateway, Speed, MTU, and Services (HTTP, HTTPS, OCSP, Telnet, SSH, Ping, SNMP, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP)</li> </ul>
Multi-vsyst Capability	To enable multi-vsyst you must activate the Virtual Systems license (required to enable support for multiple virtual systems on PA-2000 Series and PA-3000 Series firewalls or to increase the number of virtual systems beyond the base number provided by default on PA-4000 Series, PA-5000 Series, and PA-7000 Series firewalls) on each firewall in the pair. In addition, you must also enable <b>Multi Virtual System Capability</b> on each firewall ( <b>Device &gt; Setup &gt; Management &gt; General Settings</b> ).
Administrator Authentication Settings	You must define the authentication profile and certificate profile for administrative access to the firewall locally on each firewall ( <b>Device &gt; Setup &gt; Management &gt; Authentication</b> ).
Panorama Settings	Set the following Panorama settings on each firewall ( <b>Device &gt; Setup &gt; Management &gt; Panorama Settings</b> ). <ul style="list-style-type: none"> <li>• <b>Panorama Servers</b></li> <li>• <b>Disable Panorama Policy and Objects</b> and <b>Disable Device and Network Template</b></li> </ul>
SNMP	• <b>Device &gt; Setup &gt; Operations &gt; SNMP Setup</b>
Statistics Collection	• <b>Device &gt; Setup &gt; Operations &gt; Statistics Service Setup</b>
Services	• <b>Device &gt; Setup &gt; Services</b>
Global Service Routes	• <b>Device &gt; Setup &gt; Services &gt; Service Route Configuration</b>
Data Protection	• <b>Device &gt; Setup &gt; Content-ID &gt; Manage Data Protection</b>
Jumbo Frames	• <b>Device &gt; Setup &gt; Session &gt; Session Settings &gt; Enable Jumbo Frame</b>
Forward Proxy Server Certificate Settings	• <b>Device &gt; Setup &gt; Session &gt; Decryption Settings &gt; SSL Forward Proxy Settings</b>
HSM Configuration	• <b>Device &gt; Setup &gt; HSM</b>
Log Export Settings	• <b>Device &gt; Scheduled Log Export</b>

Configuration Item	What Doesn't Sync?
Software Updates	With software updates, you can either download and install them separately on each device, or download them on one peer and sync the update to the other peer. You must install the update on each peer. • <b>Device &gt; Software</b>
GlobalProtect Agent Package	With GlobalProtect client updates, you can either download and install them separately on each device, or download them to one peer and sync the update to the other peer. You must activate separately on each peer. • <b>Device &gt; GlobalProtect Client</b>
Content Updates	With content updates, you can either download and install them separately on each device, or download them on one peer and sync the update to the other peer. You must install the update on each peer. • <b>Device &gt; Dynamic Updates</b>
Licenses/Subscriptions	• <b>Device &gt; Licenses</b>
Support Subscription	• <b>Device &gt; Support</b>
Ethernet Interface IP Addresses	All Ethernet interface configuration settings sync except for the IP address ( <b>Network &gt; Interface &gt; Ethernet</b> ).
Loopback Interface IP Addresses	All Loopback interface configuration settings sync except for the IP address ( <b>Network &gt; Interface &gt; Loopback</b> ).
Tunnel Interface IP Addresses	All Tunnel interface configuration settings sync except for the IP address ( <b>Network &gt; Interface &gt; Tunnel</b> ).
LACP System Priority	Each peer must have a unique LACP System ID in an active/active deployment ( <b>Network &gt; Interface &gt; Ethernet &gt; Add Aggregate Group &gt; System Priority</b> ).
VLAN Interface IP Address	All VLAN interface configuration settings sync except for the IP address ( <b>Network &gt; Interface &gt; VLAN</b> ).
Virtual Routers	Virtual router configuration synchronizes only if you have enabled VR Sync ( <b>Device &gt; High Availability &gt; Active/Active Config &gt; Packet Forwarding</b> ). Whether or not to do this depends on your network design, including whether you have asymmetric routing.
IPSec Tunnels	IPSec tunnel configuration synchronization is dependent on whether you have configured the Virtual Addresses to use Floating IP addresses ( <b>Device &gt; High Availability &gt; Active/Active Config &gt; Virtual Address</b> ). If you have configured a floating IP address, these settings sync automatically. Otherwise, you must configure these settings independently on each peer.
GlobalProtect Portal Configuration	GlobalProtect portal configuration synchronization is dependent on whether you have configured the Virtual Addresses to use Floating IP addresses ( <b>Network &gt; GlobalProtect &gt; Portals</b> ). If you have configured a floating IP address, the GlobalProtect portal configuration settings sync automatically. Otherwise, you must configure the portal settings independently on each peer.

Configuration Item	What Doesn't Sync?
GlobalProtect Gateway Configuration	GlobalProtect gateway configuration synchronization is dependent on whether you have configured the Virtual Addresses to use Floating IP addresses ( <b>Network &gt; GlobalProtect &gt; Gateways</b> ). If you have configured a floating IP address, the GlobalProtect gateway configuration settings sync automatically. Otherwise, you must configure the gateway settings independently on each peer.
QoS	QoS configuration synchronizes only if you have enabled <b>QoS Sync (Device &gt; High Availability &gt; Active/Active Config &gt; Packet Forwarding)</b> . You might choose not to sync QoS setting if, for example, you have different bandwidth on each link or different latency through your service providers.
LLDP	No LLDP state or individual firewall data is synchronized in an active/active configuration ( <b>Network &gt; LLDP</b> ).
IKE Gateways	IKE gateway configuration synchronization is dependent on whether you have configured the Virtual Addresses to use floating IP addresses ( <b>Network &gt; IKE Gateways</b> ). If you have configured a floating IP address, the IKE gateway configuration settings sync automatically. Otherwise, you must configure the IKE gateway settings independently on each peer.
Master Key	The master key must be identical on each firewall in the HA pair, but you must manually enter it on each device ( <b>Device &gt; Master Key and Diagnostics</b> ). Before changing the master key, you must disable config sync on both peers ( <b>Device &gt; High Availability &gt; General &gt; Setup</b> and clear the <b>Enable Config Sync</b> check box) and then re-enable it after you change the keys.
Reports, logs, and Dashboard Settings	Log data, reports, and dashboard data and settings (column display, widgets) are not synced between peers. Report configuration settings, however, are synced.

## Synchronization of System Runtime Information

Runtime Information	Config Synced?		HA Link	Details
	A/P	A/A		
<b>Management Plane</b>				
User to Group Mappings	Yes	Yes	HA1	
DHCP Lease (as server)	Yes	Yes	HA1	
DNS Cache	No	No	N/A	
FQDN Refresh	No	No	N/A	
IKE Keys (phase 2)	Yes	Yes	HA1	
BrightCloud URL Database	No	No	N/A	

Runtime Information	Config Synced?		HA Link	Details
	A/P	A/A		
BrightCloud URL Cache	No	No	N/A	This feature is disabled by default and must be enabled separately on each HA peer.
BrightCloud Bloom Filter	No	No	N/A	This feature is disabled by default and must be enabled separately on each HA peer.
PAN-DB URL Cache	Yes	No	HA1	This is synchronized upon database backup to disk (every eight hours, when URL database version updates), or when the firewall reboots.
Content (manual sync)	Yes	Yes	HA1	
PPPoE, PPPoE Lease	Yes	Yes	HA1	
DHCP Client Settings and Lease	Yes	Yes	HA1	
SSL VPN Logged in User List	Yes	Yes	HA1	
Forward Information Base (FIB)	Yes	Yes	HA1	
<b>Dataplane</b>				
Session Table	Yes	Yes	HA2	<ul style="list-style-type: none"> <li>Active/passive peers do not sync ICMP or host session information.</li> <li>Active/active peers do not sync host session or multicast session information.</li> </ul>
ARP Table	Yes	No	HA2	
Neighbor Discovery (ND) Table	Yes	No	HA2	
MAC Table	Yes	No	HA2	
IPSec Sequence Number (anti-replay)	Yes	Yes	HA2	
DoS Protection	Yes	Yes	HA2	
User to IP Address Mappings	Yes	Yes	HA2	
Virtual MAC	Yes	Yes	HA2	

## HA Resources

For more information on HA, refer to the following sources:

- [Active/Active HA](#)
- [High Availability Failover Optimization](#)
- [Upgrading an HA pair](#)
- [Examples: Deploying HA](#)





# Monitoring

---

To forestall potential issues, and accelerate incidence response when needed, the firewall provides intelligence on traffic and user patterns and customizable and informative reports. The dashboard, Application Command Center (ACC), reports, and logs on the firewall allow you to monitor activity on your network. You can monitor the logs and filter the information to generate reports with predefined or customized views. You can, for example, use the predefined templates to generate reports on user activities, or analyze the reports and logs to interpret unusual behavior on your network and generate a custom report on the traffic pattern. For a visually engaging presentation of network activity, the dashboard and the ACC include widgets, charts, and tables that you can interact with to find information that you care about. In addition, you can configure the firewall to forward monitored information as email notifications, syslog messages, SNMP traps, and NetFlow records to external services.

- ▲ [Use the Dashboard](#)
- ▲ [Use the Application Command Center](#)
- ▲ [App Scope](#)
- ▲ [Use the Automated Correlation Engine](#)
- ▲ [Take Packet Captures](#)
- ▲ [Monitor Applications and Threats](#)
- ▲ [Monitor and Manage Logs](#)
- ▲ [Manage Reporting](#)
- ▲ [Use External Services for Monitoring](#)
- ▲ [Configure Log Forwarding](#)
- ▲ [Configure Email Alerts](#)
- ▲ [Use Syslog for Monitoring](#)
- ▲ [SNMP Monitoring and Traps](#)
- ▲ [NetFlow Monitoring](#)

## Use the Dashboard

The **Dashboard** tab widgets show general device information, such as the software version, the operational status of each interface, resource utilization, and up to 10 of the most recent entries in the threat, configuration, and system logs. All of the available widgets are displayed by default, but each administrator can remove and add individual widgets, as needed. Click the refresh icon  to update the dashboard or an individual widget. To change the automatic refresh interval, select an interval from the drop-down (**1 min**, **2 mins**, **5 mins**, or **Manual**). To add a widget to the dashboard, click the widget drop-down, select a category and then the widget name. To delete a widget, click  in the title bar. The following table describes the dashboard widgets.

Dashboard Charts	Descriptions
Top Applications	Displays the applications with the most sessions. The block size indicates the relative number of sessions (mouse-over the block to view the number), and the color indicates the security risk—from green (lowest) to red (highest). Click an application to view its application profile.
Top High Risk Applications	Similar to Top Applications, except that it displays the highest-risk applications with the most sessions.
General Information	Displays the device name, model, PAN-OS software version, the application, threat, and URL filtering definition versions, the current date and time, and the length of time since the last restart.
Interface Status	Indicates whether each interface is up (green), down (red), or in an unknown state (gray).
Threat Logs	Displays the threat ID, application, and date and time for the last 10 entries in the Threat log. The threat ID is a malware description or URL that violates the URL filtering profile.
Config Logs	Displays the administrator username, client (Web or CLI), and date and time for the last 10 entries in the Configuration log.
Data Filtering Logs	Displays the description and date and time for the last 60 minutes in the Data Filtering log.
URL Filtering Logs	Displays the description and date and time for the last 60 minutes in the URL Filtering log.
System Logs	Displays the description and date and time for the last 10 entries in the System log.  A config installed entry indicates configuration changes were committed successfully.
System Resources	Displays the Management CPU usage, Data Plane usage, and the Session Count, which displays the number of sessions established through the firewall.
Logged In Admins	Displays the source IP address, session type (Web or CLI), and session start time for each administrator who is currently logged in.
ACC Risk Factor	Displays the average risk factor (1 to 5) for the network traffic processed over the past week. Higher values indicate higher risk.
High Availability	If high availability (HA) is enabled, indicates the HA status of the local and peer device—green (active), yellow (passive), or black (other). For more information about HA, see <a href="#">High Availability</a> .
Locks	Shows configuration locks taken by administrators.

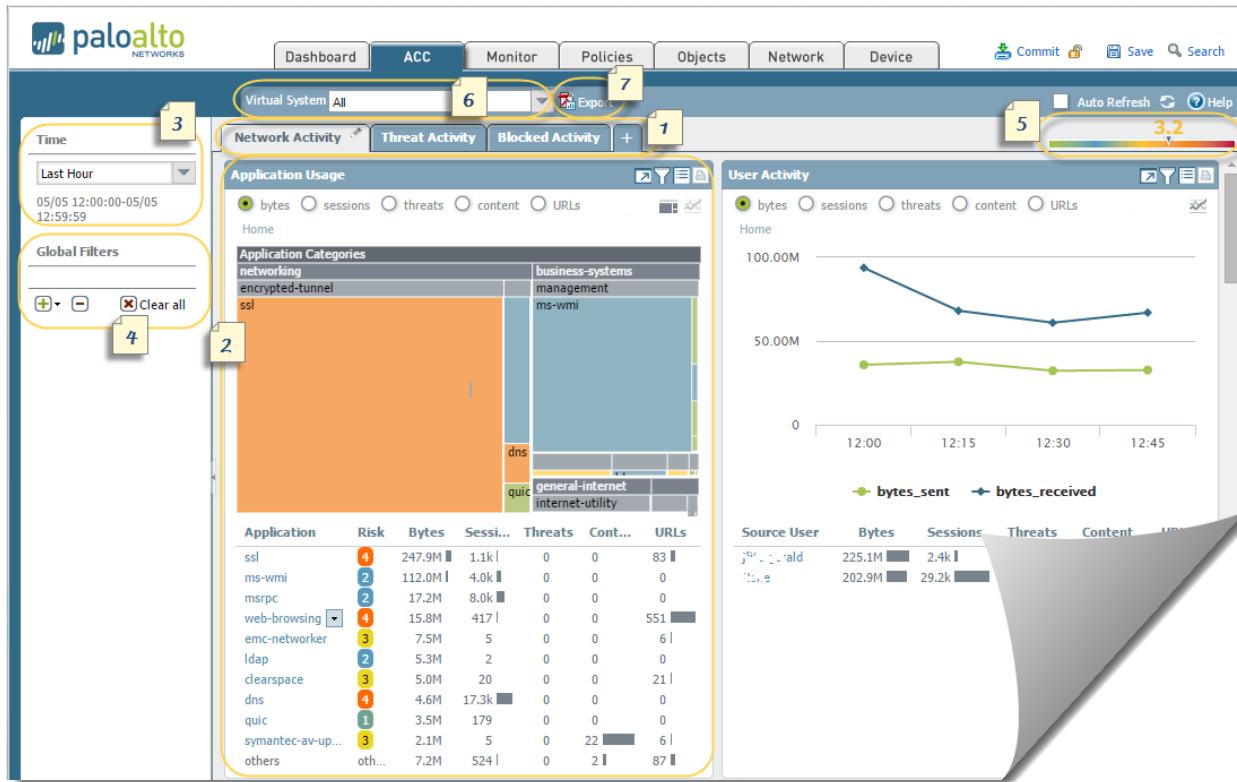
## Use the Application Command Center

The Application Command Center (ACC) is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing your network. The ACC uses the firewall logs to provide visibility into traffic patterns and actionable information on threats. The ACC layout includes a tabbed view of network activity, threat activity, and blocked activity and each tab includes pertinent widgets for better visualization of network traffic. The graphical representation allows you to interact with the data and visualize the relationships between events on the network, so that you can uncover anomalies or find ways to enhance your network security rules. For a personalized view of your network, you can also add a custom tab and include widgets that allow you to drill down into the information that is most important to you.

- ▲ [ACC—First Look](#)
- ▲ [ACC Tabs](#)
- ▲ [ACC Widgets \(Widget Descriptions\)](#)
- ▲ [ACC Filters](#)
- ▲ [Interact with the ACC](#)
- ▲ [Use Case: ACC—Path of Information Discovery](#)

## ACC—First Look

Take a quick tour of the ACC.



### ACC—First Look

	<b>Tabs</b>	The ACC includes three predefined tabs that provide visibility into network traffic, threat activity, and blocked activity. For information on each tab, see <a href="#">ACC Tabs</a> .
	<b>Widgets</b>	<p>Each tab includes a default set of widgets that best represent the events/trends associated with the tab. The widgets allow you to survey the data using the following filters:</p> <ul style="list-style-type: none"> <li>• bytes (in and out)</li> <li>• sessions</li> <li>• content (files and data)</li> <li>• URL categories</li> <li>• threats (and count)</li> </ul> <p>For information on each widget, see <a href="#">ACC Widgets</a>.</p>

### ACC—First Look (Continued)

	<b>Time</b>	The charts or graphs in each widget provide a summary and historic view. You can choose a custom range or use the predefined time periods that range from the last 15 minutes up to the last 30 days or last 30 calendar days. The selected time period applies across all tabs in the ACC.  The time period used to render data, by default, is the <b>Last Hour</b> updated in 15 minute intervals. The date and time interval are displayed onscreen, for example at 11:40, the time range is 01/12 10:30:00-01/12 11:29:59.
	<b>Global Filters</b>	The Global Filters allow you to set the filter across all widgets and all tabs. The charts/graphs apply the selected filters before rendering the data. For information on using the filters, see <a href="#">ACC Filters</a> .
	<b>Risk Factor</b>	The risk factor (1=lowest to 5=highest) indicates the relative risk based on the applications used on your network. The risk factor uses a variety of factors to assess the associated risk levels, such as whether the application can share files, is it prone to misuse or does it try to evade firewalls, it also factors in the threat activity and malware as seen through the number of blocked threats, compromised hosts or traffic to malware hosts/domains.
	<b>Source</b>	The data segment used for the display. The options vary on the firewall and on Panorama.  On the firewall, if enabled for multiple virtual systems, you can use the <b>Virtual System</b> drop-down to change the ACC display to include all virtual systems or just a selected virtual system.  On Panorama, you can select the <b>Device Group</b> drop-down to change the ACC display to include all device groups or just a selected device group.  Additionally, on Panorama, you can change the <b>Data Source</b> as <b>Panorama</b> data or <b>Remote Device Data</b> . <b>Remote Device Data</b> is only available when all the managed firewalls are on PAN-OS 7.0.0 or later. When you filter the display for a specific device group, <b>Panorama</b> data is used as the data source.
	<b>Export</b>	You can export the widgets displayed in the currently selected tab as a PDF. The PDF is downloaded and saved to the downloads folder associated with your web browser, on your computer.

## ACC Tabs

The ACC includes the following predefined tabs for viewing network activity, threat activity, and blocked activity.

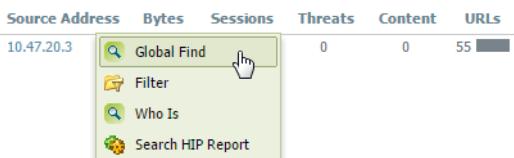
Tab	Description
<b>Network Activity</b>	<p>Displays an overview of traffic and user activity on your network including:</p> <ul style="list-style-type: none"><li>• Top applications in use</li><li>• Top users who generate traffic (with a drill down into the bytes, content, threats or URLs accessed by the user)</li><li>• Most used security rules against which traffic matches occur</li></ul> <p>In addition, you can also view network activity by source or destination zone, region, or IP address, ingress or egress interfaces, and GlobalProtect host information such as the operating systems of the devices most commonly used on the network.</p>
<b>Threat Activity</b>	<p>Displays an overview of the threats on the network, focusing on the top threats: vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top WildFire submissions by file type and application, and applications that use non-standard ports. The Compromised Hosts widget in this tab (the widget is supported on some platforms only), supplements detection with better visualization techniques; it uses the information from the correlated events tab (<b>Automated Correlation Engine &gt; Correlated Events</b>) to present an aggregated view of compromised hosts on your network by source users/IP addresses and sorted by severity.</p>
<b>Blocked Activity</b>	<p>Focuses on traffic that was prevented from coming into the network. The widgets in this tab allow you to view activity denied by application name, username, threat name, blocked content—files and data that were blocked by a file blocking profile. It also lists the top security rules that were matched on to block threats, content, and URLs.</p>

You can also [Interact with the ACC](#) to create customized tabs with custom layout and widgets that meet your network monitoring needs.

## ACC Widgets

The widgets on each tab are interactive; you can set the [ACC Filters](#) and drill down into the details for each table or graph, or customize the widgets included in the tab to focus on the information you need. For details on what each widget displays, see [Widget Descriptions](#).



Widgets		
 3	<b>Table</b>	<p>The detailed view of the data used to render the graph is provided in a table below the graph. You can interact with the table in several ways:</p> <ul style="list-style-type: none"> <li>Click and set a local filter for an attribute in the table. The graph is updated and the table is sorted using the local filter. The information displayed in the graph and the table are always synchronized.</li> <li>Hover over the attribute in the table and use the options available in the drop-down.</li> </ul> 
 4	<b>Actions</b>	<ul style="list-style-type: none"> <li><b>Maximize view</b>—Allows you enlarge the widget and view the table in a larger screen space and with more viewable information.</li> <li><b>Set up local filters</b>—Allows you to add <a href="#">ACC Filters</a> to refine the display within the widget. Use these filters to customize the widgets; these customizations are retained between logins.</li> <li><b>Jump to logs</b>—Allows you to directly navigate to the logs (<a href="#">Monitor &gt; Logs &gt; Log type</a> tab). The logs are filtered using the time period for which the graph is rendered. If you have set local and global filters, the log query concatenates the time period and the filters and only displays logs that match the combined filter set.</li> <li><b>Export</b>—Allows you to export the graph as a PDF. The PDF is downloaded and saved on your computer. It is saved in the Downloads folder associated with your web browser.</li> </ul>

## Widget Descriptions

Each tab on the ACC includes a different set of widgets.

Widget	Description
<b>Network Activity</b> —Displays an overview of traffic and user activity on your network.	
<b>Application Usage</b>	<p>The table displays the top ten applications used on your network, all the remaining applications used on the network are aggregated and displayed as other. The graph displays all applications by application category, sub category, and application. Use this widget to scan for applications being used on the network, it informs you about the predominant applications using bandwidth, session count, file transfers, triggering the most threats, and accessing URLs.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: treemap, area, column, line (the charts vary by the sort by attribute selected)</p>
<b>User Activity</b>	<p>Displays the top ten most active users on the network who have generated the largest volume of traffic and consumed network resources to obtain content. Use this widget to monitor top users on usage sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: area, column, line (the charts vary by the sort by attribute selected)</p>
<b>Source IP Activity</b>	<p>Displays the top ten IP addresses or hostnames of the devices that have initiated activity on the network. All other devices are aggregated and displayed as other.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: area, column, line (the charts vary by the sort by attribute selected)</p>
<b>Destination IP Activity</b>	<p>Displays the IP addresses or hostnames of the top ten destinations that were accessed by users on the network.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: area, column, line (the charts vary by the sort by attribute selected)</p>
<b>Source Regions</b>	<p>Displays the top ten regions (built-in or custom defined regions) around the world from where users initiated activity on your network.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: map, bar</p>
<b>Destination Regions</b>	<p>Displays the top ten destination regions (built-in or custom defined regions) on the world map from where content is being accessed by users on the network.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: map, bar</p>

Widget	Description
<b>GlobalProtect Host Information</b>	<p>Displays information on the state of the hosts on which the GlobalProtect agent is running; the host system is a GlobalProtect client. This information is sourced from entries in the HIP match log that are generated when the data submitted by the GlobalProtect agent matches a HIP object or a HIP profile you have defined on the firewall. If you do not have HIP Match logs, this widget is blank. To learn how to create HIP objects and HIP profiles and use them as policy match criteria, see <a href="#">Configure HIP-Based Policy Enforcement</a>.</p> <p>Sort attributes: profiles, objects, operating systems Charts available: bar</p>
<b>Rule Usage</b>	<p>Displays the top ten rules that have allowed the most traffic on the network. Use this widget to view the most commonly used rules, monitor the usage patterns, and to assess whether the rules are effective in securing your network.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: line</p>
<b>Ingress Interfaces</b>	<p>Displays the firewall interfaces that are most used for allowing traffic into the network.</p> <p>Sort attributes: bytes, bytes sent, bytes received Charts available: line</p>
<b>Egress Interfaces</b>	<p>Displays the firewall interfaces that are most used by traffic exiting the network.</p> <p>Sort attributes: bytes, bytes sent, bytes received Charts available: line</p>
<b>Source Zones</b>	<p>Displays the zones that are most used for allowing traffic into the network.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: line</p>
<b>Destination Zones</b>	<p>Displays the zones that are most used by traffic going outside the network.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: line</p>

**Threat Activity**—Displays an overview of the threats on the network

<b>Compromised Hosts</b>	<p>Displays the hosts that are likely compromised on your network. This widget summarizes the events from the correlation logs. For each source user/IP address, it includes the correlation object that triggered the match and the match count, which is aggregated from the match evidence collated in the correlated events logs. For details see <a href="#">Use the Automated Correlation Engine</a>.</p> <p>Available on the PA-3000 Series, PA-5000 Series, PA-7000 Series, and Panorama.</p> <p>Sort attributes: severity (by default)</p>
<b>Hosts Visiting Malicious URLs</b>	<p>Displays the frequency with which hosts (IP address/hostnames) on your network have accessed malicious URLs. These URLs are known to be malware based on categorization in PAN-DB.</p> <p>Sort attributes: count Charts available: line</p>

Widget	Description
<b>Hosts Resolving Malicious Domains</b>	<p>Displays the top hosts matching DNS signatures; hosts on the network that are attempting to resolve the hostname or domain of a malicious URL. This information is gathered from an analysis of the DNS activity on your network. It utilizes passive DNS monitoring, DNS traffic generated on the network, activity seen in the sandbox if you have configured DNS sinkhole on the firewall, and DNS reports on malicious DNS sources that are available to Palo Alto Networks customers.</p> <p>Sort attributes: count Charts available: line</p>
<b>Threat Activity</b>	<p>Displays the threats seen on your network. This information is based on signature matches in Antivirus, Anti-Spyware, and Vulnerability Protection profiles and viruses reported by WildFire.</p> <p>Sort attributes: threats Charts available: bar, area, column</p>
<b>WildFire Activity by Application</b>	<p>Displays the applications that generated the most WildFire submissions. This widget uses the malicious and benign verdict from the WildFire Submissions log.</p> <p>Sort attributes: malicious, benign Charts available: bar, line</p>
<b>WildFire Activity by File Type</b>	<p>Displays the threat vector by file type. This widget displays the file types that generated the most WildFire submissions and uses the malicious and benign verdict from the WildFire Submissions log. If this data is unavailable, the widget is empty.</p> <p>Sort attributes: malicious, benign Charts available: bar, line</p>
<b>Applications using Non Standard Ports</b>	<p>Displays the applications that are entering your network on non-standard ports. If you have migrated your firewall rules from a port-based firewall, use this information to craft policy rules that allow traffic only on the default port for the application. Where needed, make an exception to allow traffic on a non-standard port or create a custom application.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: treemap, line</p>
<b>Rules Allowing Applications On Non Standard Ports</b>	<p>Displays the security policy rules that allow applications on non-default ports. The graph displays all the rules, while the table displays the top ten rules and aggregates the data from the remaining rules as other.</p> <p>This information helps you identify gaps in network security by allowing you to assess whether an application is hopping ports or sneaking into your network. For example, you can validate whether you have a rule that allows traffic on any port except the default port for the application. Say for example, you have a rule that allows DNS traffic on its <i>application-default</i> port (port 53 is the standard port for DNS). This widget will display any rule that allows DNS traffic into your network on any port except port 53.</p> <p>Sort attributes: bytes, sessions, threats, content, URLs Charts available: treemap, line</p>

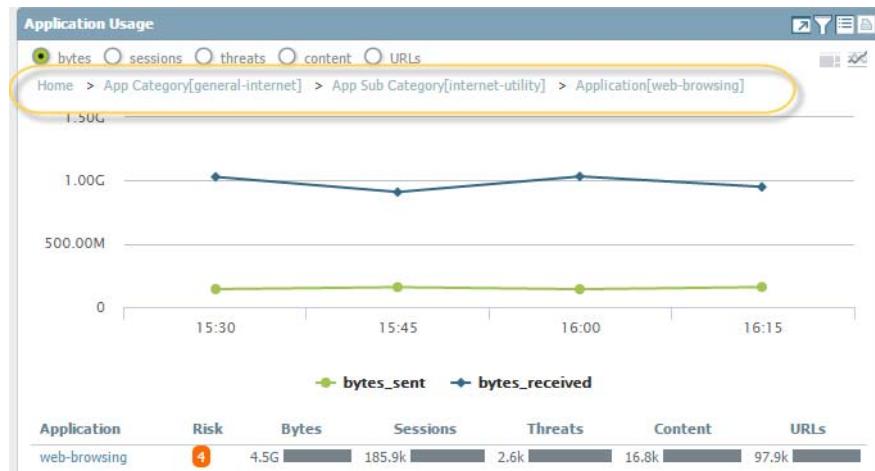
**Blocked Activity**—Focuses on traffic that was prevented from coming into the network

Widget	Description
<b>Blocked Application Activity</b>	<p>Displays the applications that were denied on your network, and allows you to view the threats, content, and URLs that you kept out of your network.</p> <p>Sort attributes: threats, content, URLs Charts available: treemap, area, column</p>
<b>Blocked User Activity</b>	<p>Displays user requests that were blocked by a match on an antivirus, anti-spyware, file blocking or url filtering profile attached to security policy.</p> <p>Sort attributes: threats, content, URLs Charts available: bar, area, column</p>
<b>Blocked Threats</b>	<p>Displays the threats that were successfully denied on your network. These threats were matched on antivirus signatures, vulnerability signatures, and DNS signatures available through the dynamic content updates on the firewall.</p> <p>Sort attributes: threats Charts available: bar, area, column</p>
<b>Blocked Content</b>	<p>Displays the files and data that was blocked from entering the network. The content was blocked because security policy denied access based on criteria defined in a File Blocking security profile or a Data Filtering security profile.</p> <p>Sort attributes: files, data Charts available: bar, area, column</p>
<b>Security Policies Blocking Activity</b>	<p>Displays the security policy rules that blocked or restricted traffic into your network. Because this widget displays the threats, content, and URLs that were denied access into your network, you can use it to assess the effectiveness of your policy rules. This widget does not display traffic that blocked because of deny rules that you have defined in policy.</p> <p>Sort attributes: threats, content, URLs Charts available: bar, area, column</p>

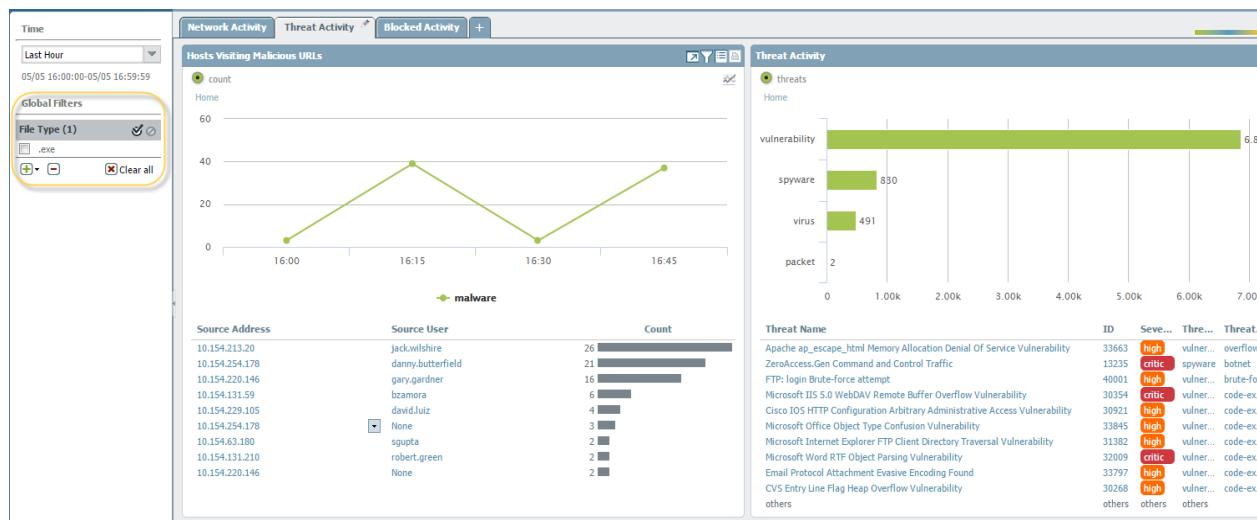
## ACC Filters

The graphs and tables on the ACC widgets allow you to use filters to narrow the scope of data that is displayed, so that you can isolate specific attributes and analyze information you want to view in greater detail. The ACC supports the simultaneous use of widget and global filters.

- **Widget Filters**—Apply a widget filter, which is a filter that is *local* to a specific widget. A widget filter allows you to interact with the graph and customize the display so that you can drill down in to the details and access the information you want to monitor on a specific widget. To create a widget filter that is persistent across reboots, you must use the **Set Local Filter** option.



- **Global filters**—Apply global filters across all the tabs in the ACC. A global filter allows you to pivot the display around the details you care about right now and exclude the unrelated information from the current display. For example, to view all events relating to a specific user and application, you can apply the username and the application as a global filter and view only information pertaining to the user and the application through all the tabs and widgets on the ACC. Global filters are not persistent.



You can apply global filters in three ways:

- **Set a global filter from a table**—Select an attribute from a table in any widget and apply the attribute as a global filter.
- **Promote a widget filter to be a global filter**—Promote a value in a table or a graph to a global filter by using the dropdown menu next to the value. This option allows you to elevate a local filter used in a widget, and apply the attribute globally to update the display across all the tabs on the ACC.
- **Define a global filter**—Define a filter using the **Global Filters** pane on the ACC.

See [Interact with the ACC](#) for details on using these filters.

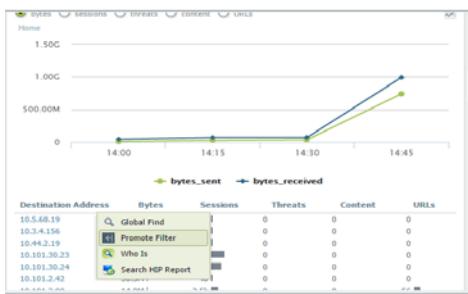
## Interact with the ACC

To customize and refine the ACC display, you can add and delete tabs, add and delete widgets, set local and global filters, and interact with the widgets.

Work with the Tabs and Widgets	
<ul style="list-style-type: none"> <li>Add a tab.</li> </ul>	<ol style="list-style-type: none"> <li>Select the  icon along the list of tabs.</li> <li>Add a <b>View Name</b>. This name will be used as the name for the tab. You can add up to five tabs.</li> </ol>
<ul style="list-style-type: none"> <li>Edit a tab.</li> </ul>	<p>Select the tab, and click the pencil icon next to the tab name, to edit the tab. For example .</p> <p>Editing a tab allow you to add or delete or reset the widgets that are displayed in the tab. You can also change the widget layout in the tab.</p>
<ul style="list-style-type: none"> <li>See what widgets are included in a tab.</li> </ul>	<ol style="list-style-type: none"> <li>Select the tab, and click on the pencil icon to edit it.</li> <li>Select the <b>Add Widgets</b> drop-down and verify the widgets that have the check boxes selected.</li> </ol>
<ul style="list-style-type: none"> <li>Add a widget or a widget group.</li> </ul>	<ol style="list-style-type: none"> <li>Add a new tab or edit a predefined tab.</li> <li>Select <b>Add Widget</b>, and then select the check box that corresponds to the widget you want to add. You can select up to a maximum of 12 widgets.</li> <li>(Optional) To create a 2-column layout, select <b>Add Widget Group</b>. You can drag and drop widgets into the 2-column display. As you drag the widget into the layout, a placeholder will display for you to drop the widget.</li> </ol> <p> You cannot name a widget group.</p>
<ul style="list-style-type: none"> <li>Delete a tab or a widget group/ widget.</li> </ul>	<ol style="list-style-type: none"> <li>To delete a custom tab, select the tab and click the X icon. </li> <li> You cannot delete a predefined tab.</li> <li>To delete a widget group/widget, edit the tab and in the workspace section, click the [X] icon on the right. You cannot undo a deletion.</li> </ol>
<ul style="list-style-type: none"> <li>Reset the default widgets in a tab.</li> </ul>	<p>On a predefined tab, such as the <b>Blocked Activity</b> tab, you can delete one or more widgets. If you want to reset the layout to include the default set of widgets for the tab, edit the tab and click <b>Reset View</b>.</p>
<ul style="list-style-type: none"> <li>Zoom in on the details in an area, column, or line graph.</li> </ul> <p><a href="#">Watch</a> how the zoom-in capability works.</p>	<p>Click and drag an area in the graph to zoom in. For example, when you zoom into a line graph, it triggers a re-query and the firewall fetches the data for the selected time period. It is not a mere magnification.</p>

## Work with the Tabs and Widgets (Continued)

- Use the table drop-down to find more information on an attribute.



- Hover over an attribute in a table to see the drop-down.
- Click into the drop-down to view the available options.
- Global Find**—Use **Global Find** allows you to find references to the attribute (username/IP address, object name, policy rule name, threat ID, or application name) anywhere in the candidate configuration on the firewall.
- Promote Filter**—Sets the attribute as a global filter. This allows you to filter all the views in the ACC based on the filters you have applied.
- Value**—Displays the details of the threat ID, or application name, or address object.
- Who Is**—Performs a domain name (*WHOIS*) lookup for the IP address. The lookup queries databases that store the registered users or assignees of an Internet resource.
- Search HIP Report**—Uses the username or IP address to find matches in a HIP Match report.

- Set a widget filter.



You can also click an attribute in the table (below the graph) to apply it as a widget filter.

- Select a widget and click the  icon.
- Click the  icon to add the filters you want to apply.
- Click **Apply**. These filters are persistent across reboots.



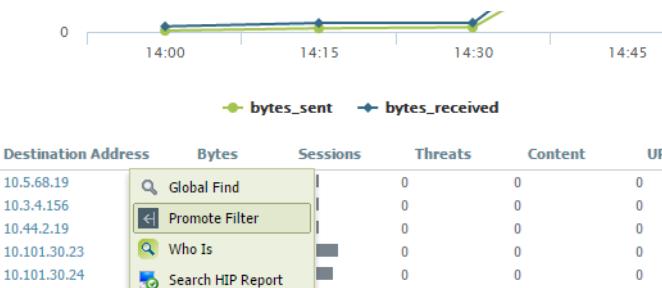
The active widget filters are indicated next to the widget name.

- Negate a widget filter

- Click the  icon to display the Setup Local Filters dialog.
- Add a filter, and then click the  negate icon.

- Set a global filter from a table.

- Hover over an attribute in the table below the chart, and click the drop-down.
- Click **Promote Filter** to add the attribute as a global filter.



- Set a global filter using the Global Filters pane.

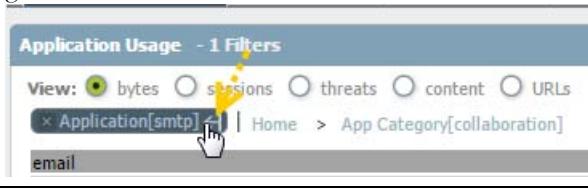
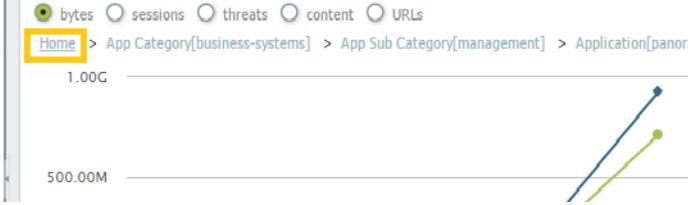
[Watch](#) global filters in action.

- Locate the **Global Filters** pane on the left side of the ACC.



- Click the  icon to view the list of filters you can apply.

### Work with the Tabs and Widgets (Continued)

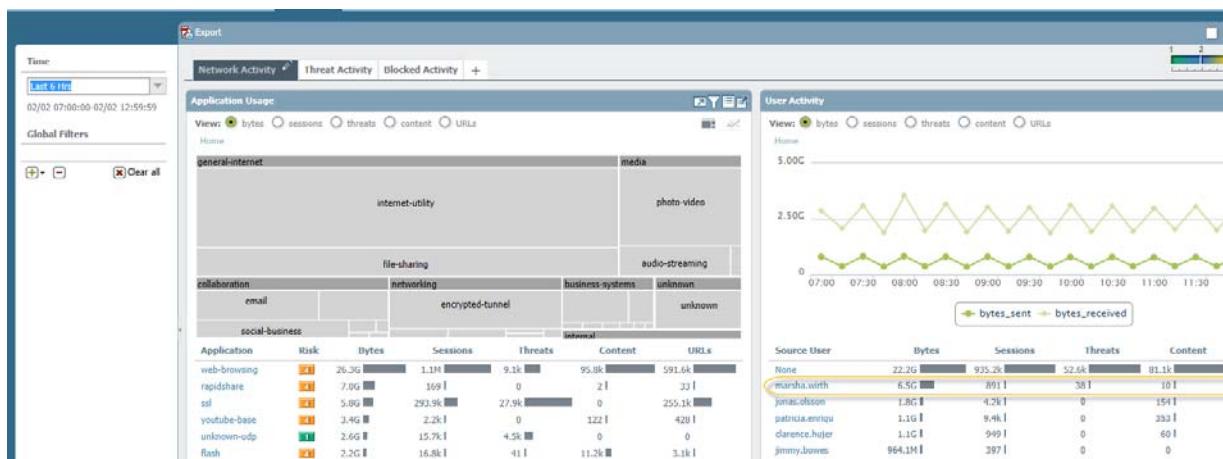
<ul style="list-style-type: none"> <li>Promote a widget filter to a global filter.</li> </ul>	<ol style="list-style-type: none"> <li>On any table in a widget, click the link for an attribute. This sets the attribute as a widget filter.</li> <li>To promote the filter to be a global filter, select the arrow to the right of the filter.</li> </ol> 
<ul style="list-style-type: none"> <li>Remove a filter.</li> </ul>	<p>Click the  icon to remove a filter.</p> <ul style="list-style-type: none"> <li>For global filters: It is located in the Global Filters pane.</li> <li>For widget filters: Click the  icon to display the Setup Local Filters dialog, then select the filter, and click the  icon.</li> </ul> 
<ul style="list-style-type: none"> <li>Clear all filters.</li> </ul>	<ul style="list-style-type: none"> <li>For global filters: Click the <b>Clear All</b> button under Global Filters.</li> <li>For widget filters: Select a widget and click the  icon. Then click the <b>Clear All</b> button in the Setup Local Filters dialog.</li> </ul>
<ul style="list-style-type: none"> <li>See what filters are in use.</li> </ul>	<ul style="list-style-type: none"> <li>For global filters: The number of global filters applied are displayed on the left pane under Global Filters.</li> <li>For widget filters: The number of widget filters applied on a widget are displayed next to the widget name. To view the filters, click the  icon.</li> </ul>
<ul style="list-style-type: none"> <li>Reset the display on a widget.</li> </ul>	<ul style="list-style-type: none"> <li>If you set a widget filter or drill into a graph, click the <b>Home</b> link to reset the display in the widget.</li> </ul> 

## Use Case: ACC—Path of Information Discovery

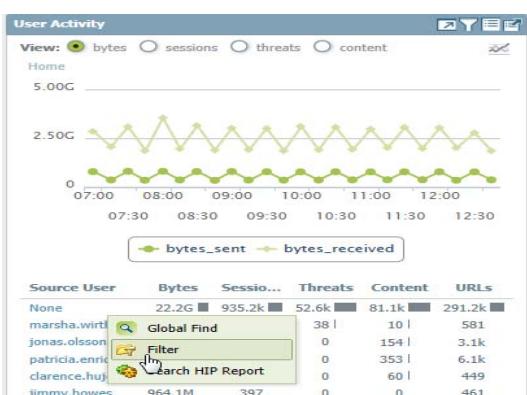
The ACC has a wealth of information that you can use as a starting point for analyzing network traffic. Let's look at an example on using the ACC to uncover events of interest. This example illustrates how you can use the ACC to ensure that legitimate users can be held accountable for their actions, detect and track unauthorized activity, and detect and diagnose compromised hosts and vulnerable systems on your network.

The widgets and filters in the ACC give you the capability to analyze the data and filter the views based on events of interest or concern. You can trace events that pique your interest, directly export a PDF of a tab, access the raw logs, and save a personalized view of the activity that you want to track. These capabilities make it possible for you to monitor activity and develop policies and countermeasures for fortifying your network against malicious activity. In this section, you will [Interact with the ACC](#) widgets across different tabs, drill down using widget filters, and pivot the ACC views using global filters, and export a PDF for sharing with incidence response or IT teams.

At first glance, you see the Application Usage and User Activity widgets in the **ACC > Network Activity** tab. The User Activity widget shows that user Marsha Wirth has transferred 718 Megabytes of data during the last hour. This volume is nearly six times more than any other user on the network. To see the trend over the past few hours, expand the **Time** period to the **Last 6 Hrs**, and now Marsha's activity has been 6.5 Gigabytes over 891 sessions and has triggered 38 threats signatures.



Because Marsha has transferred a large volume of data, apply her username as a global filter ([ACC Filters](#)) and pivot all the views in the ACC to Marsha's traffic activity.

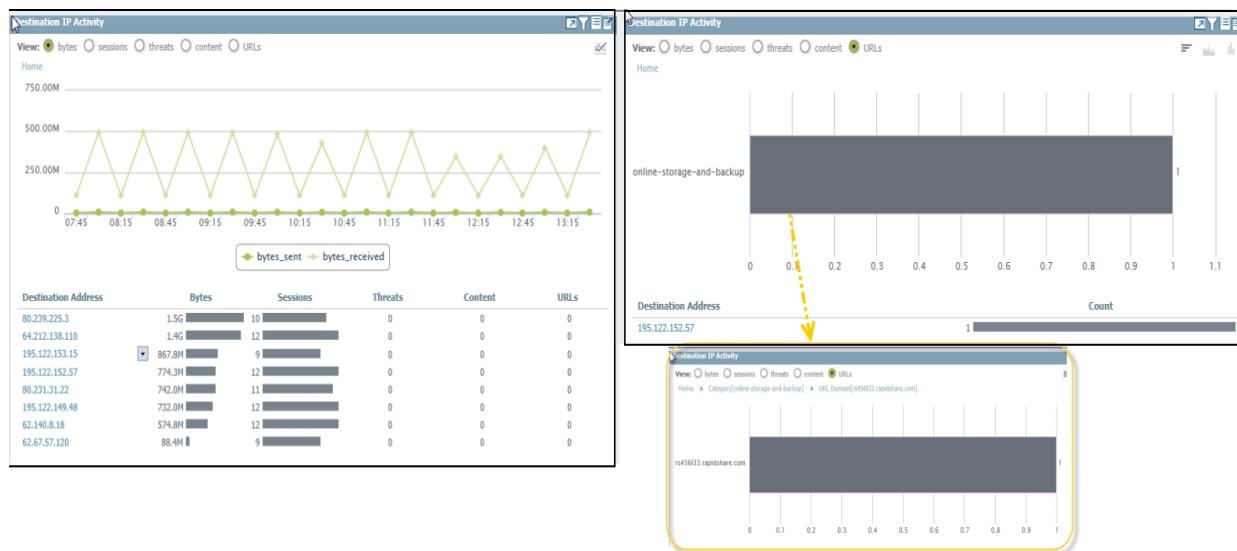


The Application Usage tab now shows that the top application that Martha used was rapidshare, a Swiss-owned file-hosting site that belongs to the file-sharing URL category. For further investigation, add rapidshare as a global filter, and view Marsha's activity in the context of rapidshare.

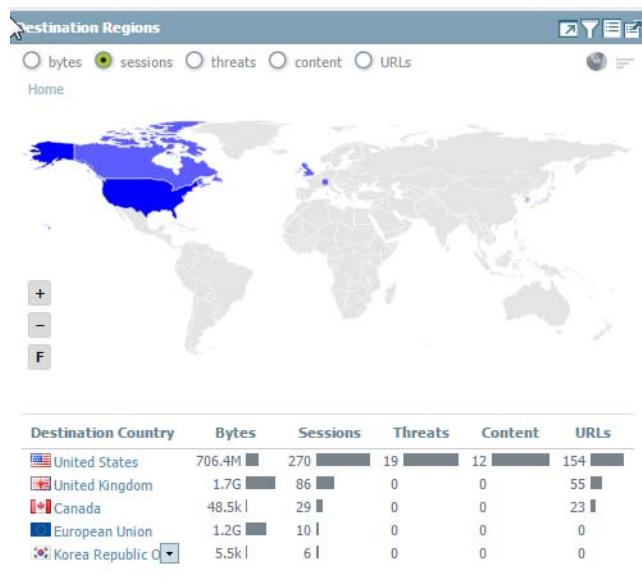


Consider whether you want to sanction rapidshare for company use. Should you allow uploads to this site and do you need a QoS policy to limit bandwidth?

To view which IP addresses Marsha has communicated with, check the **Destination IP Activity** widget, and view the data by bytes and by URLs.



To know which countries Marsha communicated with, sort on **sessions** in the **Destination Regions** widget.



From this data, you can confirm that Marsha, a user on your network, has established sessions in Korea and the European Union, and she logged 19 threats in her sessions within the United States.

To look at Marsha's activity from a threat perspective, remove the global filter for rapidshare. In the **Threat Activity** widget on the **Threat Activity** tab, view the threats. The widget displays that her activity had triggered a match for 26 vulnerabilities in the overflow, DoS and code-execution threat category. Several of these vulnerabilities are of critical severity.



To further drill-down into each vulnerability, click into the graph and narrow the scope of your investigation. Each click automatically applies a local filter on the widget.



To investigate each threat by name, you can create a global filter for say, **Microsoft Works File Converter Field Length Remote Code Execution Vulnerability**. Then, view the **User Activity** widget in the **Network Activity** tab. The tab is automatically filtered to display threat activity for Marsha (notice the global filters in the screenshot).

The screenshot shows the Application Command Center interface. In the top navigation bar, the 'Network Activity' tab is selected. On the left, a sidebar displays 'Global Filters' with two items selected: 'Source User (1)' and 'Threat Name (1)'. The main area shows a 'User Activity' card with a single entry: 'collaboration' under 'View: threats'. Below this is a table with columns 'Application', 'Risk', and 'Count'. One row shows 'imap' with a risk level of 8 and a count of 20.

Notice that this Microsoft code-execution vulnerability was triggered over email, by the imap application. You can now establish that Marsha has IE vulnerabilities and email attachment vulnerabilities, and perhaps her computer needs to be patched. You can now either navigate to the **Blocked Threats** widget in the **Blocked Activity** tab to check how many of these vulnerabilities were blocked.

Or, you can check the **Rule Usage** widget on the **Network Activity** tab to discover how many vulnerabilities made it into your network and which security rule allowed this traffic, and navigate directly to the security rule using the **Global Find** capability.

The screenshot shows the Application Command Center interface with the 'Rule Usage' widget selected. The left panel shows a chart for 'vulnerability' with a count of 15. The right panel shows a table of security rules:

Name	Location Type	Location
Security Rule (1)	VSYS	vsys1

Details for the rule 'HighRiskApps-Standard Ports' are shown:

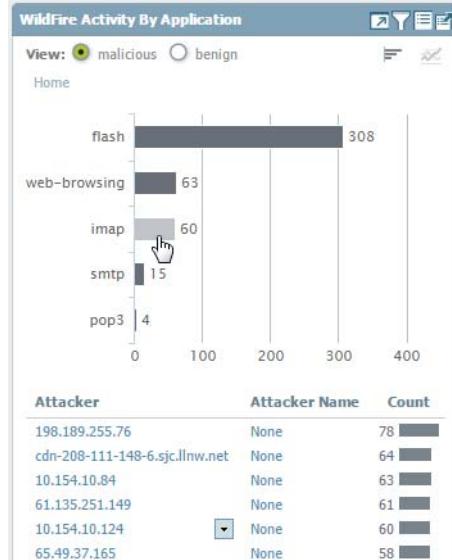
- Name: HighRiskApps-Standard Ports
- Tags: none
- Type: universal
- Zone: TAP-138
- Address: any
- User: any
- HIP Profile: any
- Zone: TAP-138
- Address: any
- Application: HighRiskApps
- Service: application-default
- Action: Allow
- Profile: (multiple icons)
- Options: (multiple icons)

A yellow arrow points from the 'Count' bar for this rule to a 'Global Find' button at the bottom of the right panel. Another yellow arrow points from the 'Rule' section to the same 'Global Find' button.

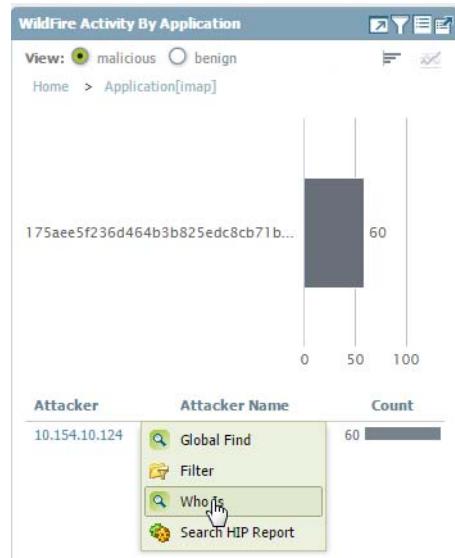
Then, drill into why imap used a non-standard port 43206 instead of port 143, which is the default port for the application. Consider modifying the security policy rule to allow applications to only use the default port for the application, or assess whether this port should be an exception on your network.



To review if any threats were logged over imap, check Marsha's activity in the **WildFire Activity by Application** widget in the **Threat Activity** tab. You can confirm that Marsha had no malicious activity, but to verify that no other user was compromised by the imap application, negate Marsha as a global filter and look for other users who triggered threats over imap.



Click into the bar for imap in the graph and drill into the inbound threats associated with the application. To find out who an IP address is registered to, hover over the attacker IP address and select the **Who Is** link in the drop-down.



Because the session count from this IP address is high, check the **Blocked Content** and **Blocked Threats** widgets in the **Blocked Activity** tab for events related to this IP address. The **Blocked Activity** tab allows you to validate whether or not your policy rules are effective in blocking content or threats when a host on your network is compromised.

Use the **Export PDF** capability on the ACC to export the current view (create a snapshot of the data) and send it to an incidence response team. To view the threat logs directly from the widget, you can also click the  icon to jump to the logs; the query is generated automatically and only the relevant logs are displayed onscreen (for example in **Monitor > Logs > Threat Logs**).



Receive Time	Type	Name	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
02/02 15:37:32	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical
02/02 15:07:49	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical
02/02 14:07:56	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical
02/02 13:07:20	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical
02/02 11:07:30	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical
02/02 10:37:29	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical
02/02 10:07:30	vulnerability	Microsoft Works File Converter Field Length Remote Code Execution Vulnerability	10.154.10.58	pancademo\mar...	66.1.1.8	43206	imap	drop	critical

You have now used the ACC to review network data/trends to find which applications or users are generating the most traffic, and how many application are responsible for the threats seen on the network. You were able to identify which application(s), user(s) generated the traffic, determine whether the application was on the default port, and which policy rule(s) allowed the traffic into the network, and determine whether the threat is spreading laterally on the network. You also identified the destination IP addresses, geo-locations with which hosts on the network are communicating with. Use the conclusions from your investigation to craft goal-oriented policies that can secure users and your network.

## App Scope

The App Scope reports provide visibility and analysis tools to help pinpoint problematic behavior, helping you understand changes in application usage and user activity, users and applications that take up most of the network bandwidth, and identify network threats.

With the App Scope reports, you can quickly see if any behavior is unusual or unexpected. Each report provides a dynamic, user-customizable window into the network; hovering the mouse over and clicking either the lines or bars on the charts opens detailed information about the specific application, application category, user, or source on the ACC. The App Scope charts on **Monitor > App Scope** give you the ability to:

- Toggle the attributes in the legend to only view chart details that you want to review. The ability to include or exclude data from the chart allows you to change the scale and review details more closely.
- Click into an attribute in a bar chart and drill down to the related sessions in the ACC. Click into an Application name, Application Category, Threat Name, Threat Category, Source IP address or Destination IP address on any bar chart to filter on the attribute and view the related sessions in the ACC.
- Export a chart or map to PDF or as an image. For portability and offline viewing, you can Export charts and maps as PDFs or PNG images.

The following App Scope reports are available:

- ▲ [Summary Report](#)
- ▲ [Change Monitor Report](#)
- ▲ [Threat Monitor Report](#)
- ▲ [Threat Map Report](#)
- ▲ [Network Monitor Report](#)
- ▲ [Traffic Map Report](#)

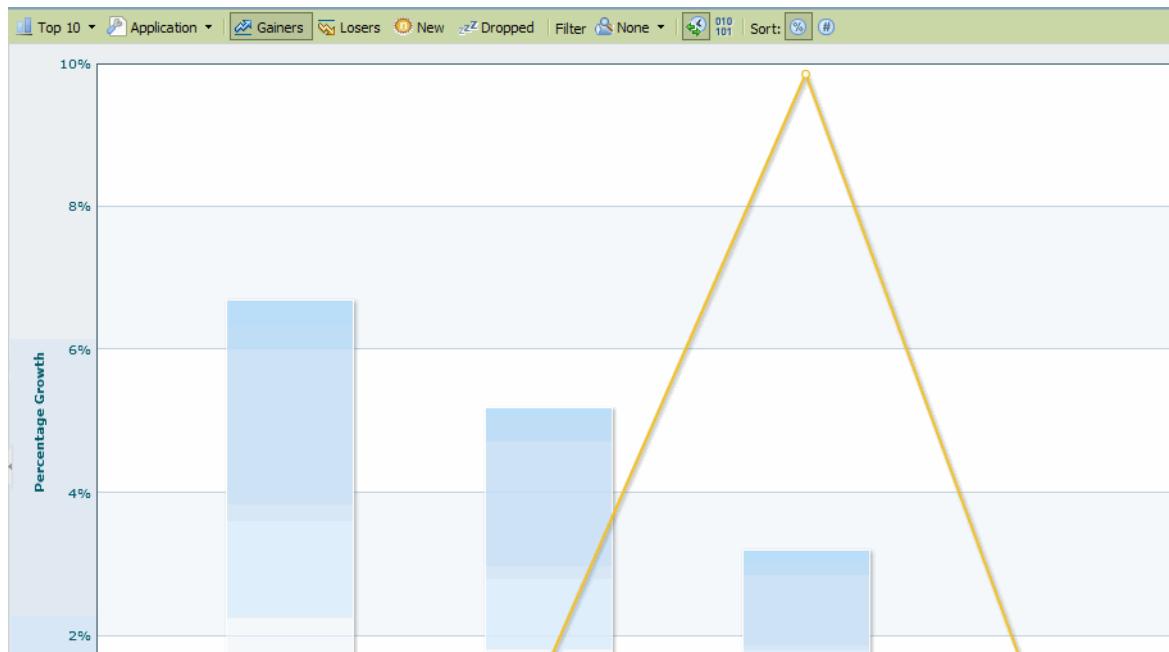
## Summary Report

The App Scope Summary report (**Monitor > App Scope > Summary**) displays charts for the top five gainers, losers, and bandwidth consuming applications, application categories, users, and sources.



## Change Monitor Report

The App Scope Change Monitor report (**Monitor > App Scope > Change Monitor**) displays changes over a specified time period. For example, the following chart displays the top applications that gained in use over the last hour as compared with the last 24-hour period. The top applications are determined by session count and sorted by percent.



The Change Monitor Report contains the following buttons and options.

Button	Description
Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
Application ▾	Determines the type of item reported: Application, Application Category, Source, or Destination.
Gainers	Displays measurements of items that have increased over the measured period.
Losers	Displays measurements of items that have decreased over the measured period.
New	Displays measurements of items that were added over the measured period.
Dropped	Displays measurements of items that were discontinued over the measured period.

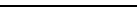
Button	Description
 None ▾	Applies a filter to display only the selected item. <b>None</b> displays all entries.
	Determines whether to display session or byte information.
 Sort: % #	Determines whether to sort entries by percentage or raw growth.
 Export:	Exports the graph as a .png image or as a PDF.
Compare last hour ▾ to the same period ending 24 hours ▾ ago	Specifies the period over which the change measurements are taken.

# Threat Monitor Report

The App Scope Threat Monitor report (**Monitor > App Scope > Threat Monitor**) displays a count of the top threats over the selected time period. For example, the following figure shows the top 10 threat types over the last 6 hours.



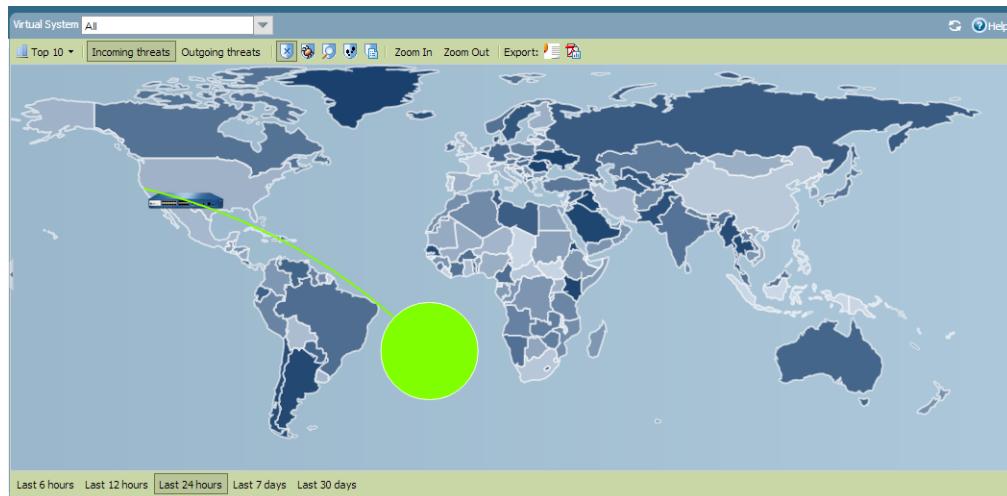
Each threat type is color-coded as indicated in the legend below the chart. The Threat Monitor report contains the following buttons and options.

Button	Description
 Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
 Threats ▾	Determines the type of item measured: Threat, Threat Category, Source, or Destination.
 Filter     	Applies a filter to display only the selected type of items.
	Determines whether the information is presented in a stacked column chart or a stacked area chart.
	Exports the graph as a .png image or as a PDF.
<a href="#">Last 6 hours</a> <a href="#">Last 12 hours</a> <a href="#">Last 24 hours</a> <a href="#">Last 7 days</a> <a href="#">Last 30 days</a>	Specifies the period over which the measurements are taken.

## Threat Map Report

The App Scope Threat Map report (**Monitor > App Scope > Threat Map**) shows a geographical view of threats, including severity. Each threat type is color-coded as indicated in the legend below the chart.

The firewall uses geolocation for creating threat maps. The firewall is placed at the bottom of the threat map screen, if you have not specified the geolocation coordinates (**Device > Setup > Management**, General Settings section) on the firewall.



The Threat Map report contains the following buttons and options.

Button	Description
Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
Incoming threats	Displays incoming threats.
Outgoing threats	Displays outgoing threats.
Filter	Applies a filter to display only the selected type of items.
Zoom In Zoom Out	Zoom in and zoom out of the map.
Export:	Exports the graph as a .png image or as a PDF.
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	Indicates the period over which the measurements are taken.

## Network Monitor Report

The App Scope Network Monitor report (**Monitor > App Scope > Network Monitor**) displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded as indicated in the legend below the chart. For example, the image below shows application bandwidth for the past 7 days based on session information.



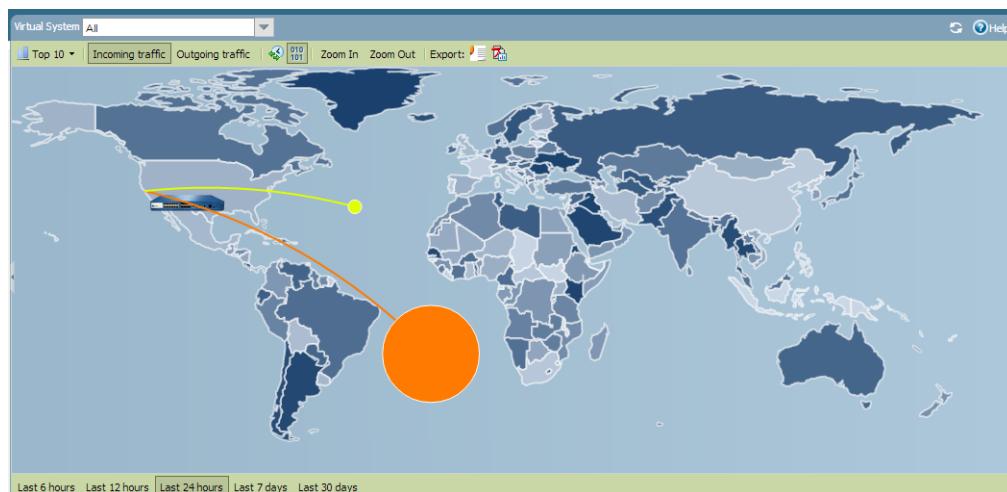
The Network Monitor report contains the following buttons and options.

Button	Description
Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
Application ▾	Determines the type of item reported: Application, Application Category, Source, or Destination.
Filter  None ▾	Applies a filter to display only the selected item. <b>None</b> displays all entries.
	Determines whether to display session or byte information.
Export:	Exports the graph as a .png image or as a PDF.
	Determines whether the information is presented in a stacked column chart or a stacked area chart.
Last 6 hours <input checked="" type="checkbox"/> Last 12 hours <input type="checkbox"/> Last 24 hours <input type="checkbox"/> Last 7 days <input type="checkbox"/> Last 30 days	Indicates the period over which the change measurements are taken.

## Traffic Map Report

The App Scope Traffic Map (**Monitor > App Scope > Traffic Map**) report shows a geographical view of traffic flows according to sessions or flows.

The firewall uses geolocation for creating traffic maps. The firewall is placed at the bottom of the traffic map screen, if you have not specified the geolocation coordinates (**Device > Setup > Management**, General Settings section) on the firewall.



Each traffic type is color-coded as indicated in the legend below the chart. The Traffic Map report contains the following buttons and options.

Buttons	Description
Top 10 ▾	Determines the number of records with the highest measurement included in the chart.
Incoming threats	Displays incoming threats.
Outgoing threats	Displays outgoing threats.
010 101	Determines whether to display session or byte information.
Zoom In   Zoom Out	Zoom in and zoom out of the map.
Export:	Exports the graph as a .png image or as a PDF.
Last 6 hours   Last 12 hours   Last 24 hours   Last 7 days   Last 30 days	Indicates the period over which the change measurements are taken.

# Use the Automated Correlation Engine

The automated correlation engine is an analytics tool that uses the logs on the firewall to detect actionable events on your network. The engine correlates a series of related threat events that, when combined, indicate a likely compromised host on your network or some other higher level conclusion. It pinpoints areas of risk, such as compromised hosts on the network, allows you to assess the risk and take action to prevent exploitation of network resources. The automated correlation engine uses *correlation objects* to analyze the logs for patterns and when a match occurs, it generates a *correlated event*.



The automated correlation engine is supported on the following platforms:

- Panorama—M-Series appliance and the virtual appliance
- PA-7000 Series firewall
- PA-5000 Series firewall
- PA-3000 Series firewall

- ▲ [Automated Correlation Engine Concepts](#)
- ▲ [View the Correlated Objects](#)
- ▲ [Interpret Correlated Events](#)
- ▲ [Use the Compromised Hosts Widget in the ACC](#)

## Automated Correlation Engine Concepts

The automated correlation engine uses *correlation objects* to analyze the logs for patterns and when a match occurs, it generates a *correlated event*.

- ▲ [Correlation Object](#)
- ▲ [Correlated Events](#)

### Correlation Object

A correlation object is a definition file that specifies patterns to match against, the data sources to use for the lookups, and time period within which to look for these patterns. A pattern is a boolean structure of conditions that queries the following data sources (or logs) on the firewall: application statistics, traffic, traffic summary, threat summary, threat, data filtering, and URL filtering. Each pattern has a severity rating, and a threshold for the number of times the pattern match must occur within a defined time limit to indicate malicious activity. When the match conditions are met, a correlated event is logged.

A correlation object can connect isolated network events and look for patterns that indicate a more significant event. These objects identify suspicious traffic patterns and network anomalies, including suspicious IP activity, known command-and-control activity, known vulnerability exploits, or botnet activity that, when correlated, indicate with a high probability that a host on the network has been compromised. Correlation objects are defined and developed by the Palo Alto Networks Threat Research team, and are delivered with the weekly dynamic updates to the firewall and Panorama. To obtain new correlation objects, the firewall must have a Threat Prevention license. Panorama requires a support license to get the updates.

The patterns defined in a correlation object can be static or dynamic. Correlated objects that include patterns observed in WildFire are dynamic, and can correlate malware patterns detected by WildFire with command-and-control activity initiated by a host that was targeted with the malware on your network. For example, when a host submits a file to the WildFire cloud and the verdict is malicious, the correlation object looks for other hosts or clients on the network that exhibit the same behavior seen in the cloud. If the malware sample had performed a DNS query and browsed to a malware domain, the correlation object will parse the logs for a similar event. When the activity on a host matches the analysis in the cloud, a high severity correlated event is logged.

### Correlated Events

A correlated event is logged when the patterns and thresholds defined in a correlation object match the traffic patterns on your network. To [Interpret Correlated Events](#) and to view a graphical display of the events, see [Use the Compromised Hosts Widget in the ACC](#).

## View the Correlated Objects

### View the Correlation Objects Available on the Firewall

- Step 1** To view the correlation objects that are currently available, select **Monitor > Automated Correlation Engine > Correlation Objects**. All the objects in the list are enabled by default.

Name	ID	Title	Category	State	Description
attack-lifecycle	6003	Compromise Lifecycle	compromised-host	active	This correlation object detects a host involved in a complete attack lifecycle, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
c2-detected	6002	C2 Detected	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
beacon-heuristics	6005	Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
worm-activity	6004	Worm Activity	compromised-host	active	This correlation object detects a worm spreading throughout the network by identifying hosts that are targeted by an exploit, perform command-and-control communications, and finally download a known malware variant.
wf-corr-c2	6001	WildFire Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire, and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.

- Step 2** View the details on each correlation object. Each object provides the following information:

- **Name** and **Title**—The name and title indicate the type of activity that the correlation object detects. The name column is hidden from view, by default. To view the definition of the object, unhide the column and click the name link.
- **ID**—A unique number that identifies the correlation object; this column is also hidden by default. The IDs are in the 6000 series.
- **Category**—A classification of the kind of threat or harm posed to the network, user, or host. For now, all the objects identify compromised hosts on the network.
- **State**—Indicates whether the correlation object is enabled (active) or disabled (inactive). All the objects in the list are enabled by default, and are hence active. Because these objects are based on threat intelligence data and are defined by the Palo Alto Networks Threat Research team, keep the objects active in order to track and detect malicious activity on your network.
- **Description**—Specifies the match conditions for which the firewall or Panorama will analyze logs. It describes the sequence of conditions that are matched on to identify acceleration or escalation of malicious activity or suspicious host behavior. For example, the **Compromise Lifecycle** object detects a host involved in a complete attack lifecycle in a three-step escalation that starts with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.

For more information, see [Automated Correlation Engine Concepts](#) and [Use the Automated Correlation Engine](#).

## Interpret Correlated Events

You can view and analyze the logs generated for each correlated event in the **Monitor > Automated Correlation Engine > Correlated Events** tab.

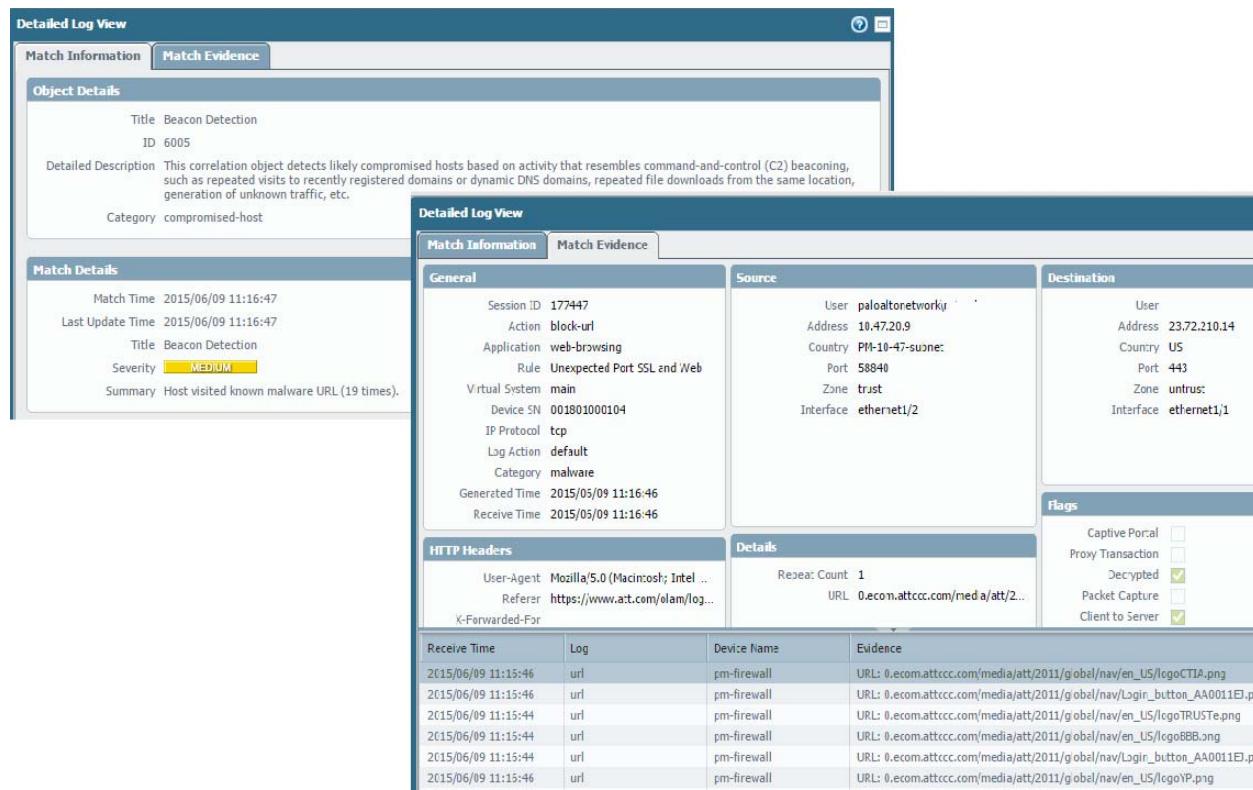
Match Time	Update Time	Object Name	Source address	Source User	Severity	Summary
2015/02/04 11:20:35	2015/02/04 11:41:10	C2 Detected	192.168.61.51	panq\aa...	high	Host visited 101 URLs including: hawet.zapt0.org/hawet.zapt...
2015/02/03 21:35:47	2015/02/04 09:17:39	Compromise Lifecycle	192.168.61.51	panq\aa...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/02/03 21:43:44	2015/02/04 09:17:29	Beacon Detection	192.168.61.51	panq\aa...	high	Host repeatedly visited malware domains (100).
2015/01/28 17:17:02	2015/01/28 17:25:06	Compromise Lifecycle	192.168.61.51	panq\yos...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/01/28 17:16:35	2015/01/28 17:16:35	Compromise Lifecycle	192.168.61.51	panq\yos...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/01/28 16:31:25	2015/01/28 17:14:11	Beacon Detection	192.168.61.51	panq\lin...	high	Host repeatedly visited malware domains (100).
2015/01/28 16:21:49	2015/01/28 16:21:49	Compromise Lifecycle	192.168.61.51	panq\jkn...	critical	Host appears to be compromised based on a sequence of recent threat log activity.
2015/01/28 14:54:44	2015/01/28 15:24:11	Beacon Detection	192.168.61.51	panq\jim...	high	Host repeatedly visited malware domains (100).
2015/01/28 13:55:25	2015/01/28 14:53:00	Beacon Detection	192.168.61.51	panq\do...	high	Host repeatedly visited malware domains (100).
2015/01/28 11:15:54	2015/01/28 11:20:10	C2 Detected	192.168.61.51	panq\do...	high	Host visited 102 URLs including: hawet.zapt0.org/hawet.zapt...
2015/01/22 15:41:25	2015/01/28 10:51:15	C2 Detected	192.168.61.51	panq\pla...	high	Host visited 101 URLs including: hawet.zapt0.org/hawet.zapt...
2015/01/26 17:40:56	2015/01/26 23:10:00	Beacon Detection	134.154.10.201		low	Host is generating unknown TCP or UDP network traffic.
2015/01/26 23:09:57	2015/01/26 23:09:57	Beacon Detection	134.154.254.64		low	Host is generating unknown TCP or UDP network traffic.

Correlated Events includes the following details:

Field	Description
<b>Match Time</b>	The time the correlation object triggered a match.
<b>Update Time</b>	The time when the event was last updated with evidence on the match. As the firewall collects evidence on pattern or sequence of events defined in a correlation object, the time stamp on the correlated event log is updated.
<b>Object Name</b>	The name of the correlation object that triggered the match.
<b>Source Address</b>	The IP address of the user/device on your network from whom which the traffic originated.
<b>Source User</b>	The user and user group information from the directory server, if <b>User-ID</b> is enabled.

Field	Description
<b>Severity</b>  To configure the firewall or Panorama to send alerts using email, SNMP or syslog messages for a desired severity level, see <a href="#">Use External Services for Monitoring</a> .	<p>A rating that indicates the urgency and impact of the match. The severity level indicates the extent of damage or escalation pattern, and the frequency of occurrence. Because correlation objects are primarily for detecting threats, the correlated events typically relate to identifying compromised hosts on the network and the severity implies the following:</p> <ul style="list-style-type: none"> <li>• <b>Critical</b>—Confirms that a host has been compromised based on correlated events that indicate an escalation pattern. For example, a critical event is logged when a host that received a file with a malicious verdict by WildFire exhibits the same command-and-control activity that was observed in the WildFire sandbox for that malicious file.</li> <li>• <b>High</b>—Indicates that a host is very likely compromised based on a correlation between multiple threat events, such as malware detected anywhere on the network that matches the command-and-control activity generated by a particular host.</li> <li>• <b>Medium</b>—Indicates that a host is likely compromised based on the detection of one or multiple suspicious events, such as repeated visits to known malicious URLs, which suggests a scripted command-and-control activity.</li> <li>• <b>Low</b>—Indicates that a host is possibly compromised based on the detection of one or multiple suspicious events, such as a visit to a malicious URL or a dynamic DNS domain.</li> <li>• <b>Informational</b>—Detects an event that may be useful in aggregate for identifying suspicious activity, but the event is not necessarily significant on its own.</li> </ul>
<b>Summary</b>	A description that summarizes the evidence gathered on the correlated event.

Click the  icon to see the detailed log view, which includes all the evidence on a match:



The screenshot shows the 'Match Evidence' tab selected in the 'Detailed Log View' interface. The interface is divided into several sections:

- Object Details:** Displays information about the correlation object, including Title (Beacon Detection), ID (6005), and Detailed Description (This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.).
- Match Details:** Shows Match Time (2015/06/09 11:16:47), Last Update Time (2015/06/09 11:16:47), Title (Beacon Detection), Severity (MEDIUM), and Summary (Host visited known malware URL (19 times)).
- Detailed Log View:** This main section contains tabs for 'Match Information' and 'Match Evidence'. The 'Match Evidence' tab is active, displaying detailed log entries. It includes sections for General, Source, Destination, HTTP Headers, and Details.
- General:** Lists session details: Session ID (177447), Action (block-url), Application (web-browsing), Rule (Unexpected Port SSL and Web), Virtual System (main), Device SN (001801000104), IP Protocol (tcp), Log Action (default), Category (malware), Generated Time (2015/05/09 11:16:46), and Receive Time (2015/05/09 11:16:46).
- Source:** Lists user (paloaltnetworkup), address (10.47.20.9), country (PM-10-47-sudone), port (58840), zone (trust), and interface (ethernet1/2).
- Destination:** Lists user (User), address (23.72.210.14), country (US), port (443), zone (untrust), and interface (ethernet1/1).
- HTTP Headers:** Lists User-Agent (Mozilla/5.0 (Macintosh; Intel ...), Referer (https://www.att.com/elam/log...), and X-Forwarded-For.
- Details:** Shows Reuse Count (1) and URL (0.ecom.attccc.com/media/att/2...).
- Flags:** Includes checkboxes for Captive Portal (unchecked), Proxy Transaction (unchecked), Decrypted (checked), Packet Capture (unchecked), and Client to Server (checked).
- Evidence:** A table listing receive time, log, device name, and evidence URL for each event. The table has 6 rows of data.

Tab	Description
<b>Match Information</b>	Object Details: Presents information on the <a href="#">Correlation Object</a> that triggered the match.
	Match Details: A summary of the match details that includes the match time, last update time on the match evidence, severity of the event, and an event summary.
<b>Match Evidence</b>	Presents all the evidence that corroborates the correlated event. It lists detailed information on the evidence collected for each session.

## Use the Compromised Hosts Widget in the ACC

The compromised hosts widget on **ACC > Threat Activity**, aggregates the **Correlated Events** and sorts them by severity. It displays the source IP address/user who triggered the event, the correlation object that was matched and the number of times the object was matched. Use the match count link to jump to the match evidence details.

Severity	Host	User	Matching Objects	Match Count
CRITICAL	192.168.61.51	kingsbeach	Beacon Detection Compromise Lifecycle	2
CRITICAL	192.168.61.51	yosemite	Compromise Lifecycle	1
CRITICAL	192.168.61.51	yosemitae	Compromise Lifecycle	1
HIGH	192.168.61.51	donnerlake	Beacon Detection C2 Detected	1
HIGH	192.168.61.51	placerville	C2 Detected	1
LOW	134.154.10.201		Beacon De	1

This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.

For more details, see [Use the Automated Correlation Engine](#) and [Use the Application Command Center](#).

## Take Packet Captures

All Palo Alto Networks firewalls allow you to take packet captures (pcaps) of traffic that traverses the management interface and network interfaces on the firewall. When taking packet captures on the dataplane, you may need to [Disable Hardware Offload](#) to ensure that the firewall captures all traffic.



Packet capture can be very CPU intensive and can degrade firewall performance. Only use this feature when necessary and make sure you turn it off after you have collected the required packets.

There are four different types of packet captures you can enable, depending on what you need to do:

- **Custom Packet Capture**—The firewall captures packets for all traffic or for specific traffic based on filters that you define. For example, you can configure the firewall to only capture packets to and from a specific source and destination IP address or port. You then use the packet captures for troubleshooting network-related issues or for gathering application attributes to enable you to write custom application signatures or to request an application signature from Palo Alto Networks. See [Take a Custom Packet Capture](#).
- **Threat Packet Capture**—The firewall captures packets when it detects a virus, spyware, or vulnerability. You enable this feature in Antivirus, Anti-Spyware, and Vulnerability Protection security profiles. A link to view or export the packet captures will appear in the second column of the Threat log. These packet captures provide context around a threat to help you determine if an attack is successful or to learn more about the methods used by an attacker. You can also submit this type of pcap to Palo Alto Networks to have a threat re-analyzed if you feel its a false-positive or false-negative. See [Take a Threat Packet Capture](#).
- **Application Packet Capture**—The firewall captures packets based on a specific application and filters that you define. A link to view or export the packet captures will appear in the second column of the Traffic logs for traffic that matches the packet capture rule. See [Take an Application Packet Capture](#).
- **Management Interface Packet Capture**—The firewall captures packets on the management interface (MGT). The packet captures are useful when troubleshooting services that traverse the interface, such as device management authentication to external servers (LDAP and RADIUS for example), software and content updates, log forwarding, communication with SNMP servers, and authentication requests for GlobalProtect and Captive Portal. See [Take a Packet Capture on the Management Interface](#).

## Disable Hardware Offload

Packet captures on a Palo Alto Networks firewall are performed in the dataplane CPU, unless you configure the firewall to [Take a Packet Capture on the Management Interface](#), in which case the packet capture is performed on the management plane. When a packet capture is performed on the dataplane, during the ingress stage, the firewall performs packet parsing checks and discards any packets that do not match the packet capture filter. Any traffic that is offloaded to the field-programmable gate array (FPGA) offload processor is also excluded, unless you turn off hardware offload. For example, encrypted traffic (SSL/SSH), network protocols (OSPF, BGP, RIP), application overrides, and terminating applications can be offloaded to the FPGA and therefore are excluded from packet captures by default. Some types of sessions will never be offloaded, such as ARP, all non-IP traffic, IPSec, VPN sessions, SYN, FIN, and RST packets.



Hardware offload is supported on the following firewalls: PA-2000 Series, PA-3050, PA-3060, PA-4000 Series, PA-5000 Series, and PA-7000 Series firewall.



Disabling hardware offload increases the dataplane CPU usage. If dataplane CPU usage is already high, you may want to schedule a maintenance window before disabling hardware offload.

Enable/Disable Hardware Offload	
<b>Step 1</b>	Disable hardware offload by running the following CLI command:  <code>admin@PA-7050&gt; set session offload no</code>
<b>Step 2</b>	After the firewall captures the required traffic, enable hardware offload by running the following CLI command:  <code>admin@PA-7050&gt; set session offload yes</code>

## Take a Custom Packet Capture

Custom packet captures allow you to define the traffic that the firewall will capture. To ensure that you capture all traffic, you may need to [Disable Hardware Offload](#).

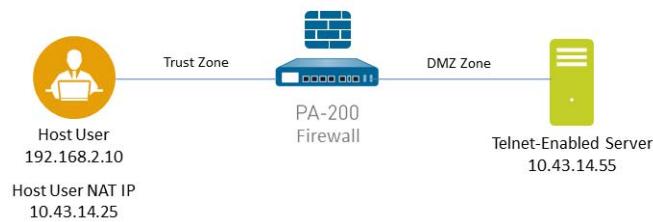
## Take a Custom Packet Capture

**Step 1** Before you start a packet capture, identify the attributes of the traffic that you want to capture.

For example, to determine the source IP address, source NAT IP address, and the destination IP address for traffic between two systems, perform a ping from the source system to the destination system. After the ping is complete, go to **Monitor > Traffic** and locate the traffic log for the two systems. Click the **Detailed Log View** icon located in the first column of the log and note the source address, source NAT IP, and the destination address.

Detailed Log View		
General	Source	Destination
Session ID 27949 Action allow Action Source from-policy Application ping Rule rule1 Session End Reason n/a Category any Virtual System	User Address 192.168.2.10 Country 192.168.0.0-192.168.255.255 Port 0 Zone I3-vlan-trust Interface vlan.1 NAT IP 10.43.14.25 NAT Port 0	User Address 10.43.14.55 Country 10.0.0.0-10.255.255.255 Port 0 Zone I3-untrust Interface ethernet1/1 NAT IP 10.43.14.55 NAT Port 0

In the example that follows, we will use a packet capture to troubleshoot a Telnet connectivity issue from a user in the Trust zone to a server in the DMZ zone.



### Take a Custom Packet Capture (Continued)

- Step 2** Set packet capture filters, so the firewall only captures traffic you are interested in.

Filters will make it easier for you to locate the information you need in the packet capture and will reduce the processing power required by the firewall to take the packet capture. To capture all traffic, do not define filters and leave the filter option off.

For example, if you configured NAT on the firewall, you will need to apply two filters. The first one filters on the pre-NAT source IP address to the destination IP address and the second one filters traffic from the destination server to the source NAT IP address.

1. Select **Monitor > Packet Capture**.
2. Click **Clear All Settings** at the bottom of the window to clear any existing capture settings.
3. Click **Manage Filters** and click **Add**.
4. Select **Id 1** and in the **Source** field enter the source IP address you are interested in and in the **Destination** field enter a destination IP address.

For example, enter the source IP address 192.168.2.10 and the destination IP address 10.43.14.55. To further filter the capture, set **Non-IP** to **exclude** non-IP traffic, such as broadcast traffic.

5. **Add** the second filter and select **Id 2**.

For example, in the **Source** field enter 10.43.14.55 and in the **Destination** field enter 10.43.14.25. In the **Non-IP** drop-down menu select **exclude**.



6. Click **OK**.

- Step 3** Set **Filtering** to **On**.

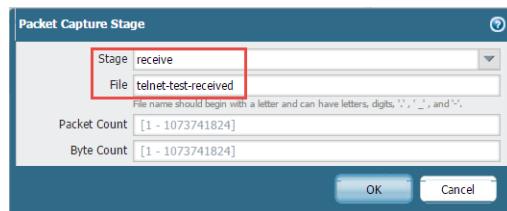
### Take a Custom Packet Capture (Continued)

- Step 4** Specify the traffic stage(s) that trigger the packet capture and the filename(s) to use to store the captured content. For a definition of each stage, click the **Help** icon on the packet capture page.

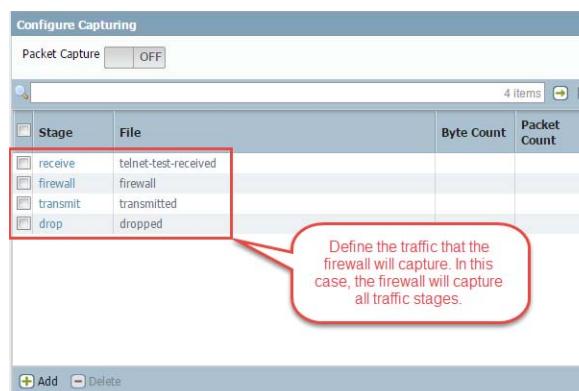
For example, to configure all packet capture stages and define a filename for each stage, perform the following procedure:

1. Add a **Stage** to the packet capture configuration and define a **File** name for the resulting packet capture.

For example, select **receive** as the **Stage** and set the **File** name to **telnet-test-received**.

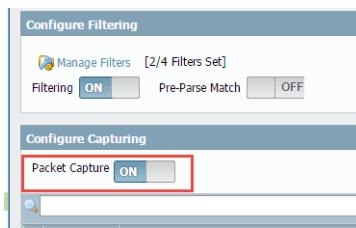


2. Continue to Add each **Stage** you want to capture (**firewall**, **transmit**, and **drop**) and set a unique **File** name for each stage.



- Step 5** Set **Packet Capture** to **ON**.

Note the warning that system performance can be degraded and then click **OK**. If you define filters, the packet capture should have little impact on performance, but you should always turn **Off** packet capture after the firewall captures the data that you want to analyze.



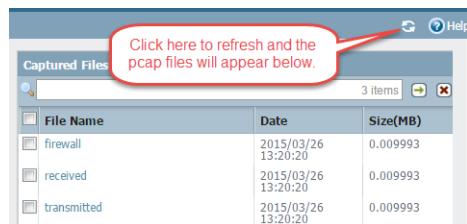
**Take a Custom Packet Capture (Continued)**

- Step 6** Generate traffic that matches the filters that you defined.

For this example, generate traffic from the source system to the Telnet-enabled server by running the following command from the source system (192.168.2.10):

```
telnet 10.43.14.55
```

- Step 7** Turn packet capture **OFF** and then click the refresh icon to see the packet capture files.



Notice that in this case, there were no dropped packets, so the firewall did not create a file for the drop stage.

- Step 8** Download the packet captures by clicking the filename in the File Name column.



- Step 9** View the packet capture files using a network packet analyzer, such as Wireshark.

In this example, the received.pcap packet capture shows a failed Telnet session from the source system at 192.168.2.10 to the Telnet-enabled server at 10.43.14.55. The source system sent the Telnet request to the server, but the server did not respond. In this example, the server may not have Telnet enabled, so check the server.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.10	10.43.14.55	TCP	66	49525 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	3.002415	192.168.2.10	10.43.14.55	TCP	66	49525 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	9.008679	192.168.2.10	10.43.14.55	TCP	62	49525 > telnet [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

- Step 10** Enable the Telnet service on the destination server (10.43.14.55) and turn on packet capture to take a new packet capture.

- Step 11** Generate traffic that will trigger the packet capture.

Run the Telnet session again from the source system to the Telnet-enabled server

```
telnet 10.43.14.55
```

### Take a Custom Packet Capture (Continued)

#### Step 12 Download and open the received.pcap file and view it using a network packet analyzer.

The following packet capture now shows a successful Telnet session from the host user at 192.168.2.10 to the Telnet-enabled server at 10.43.14.55. Note that you also see the NAT address 10.43.14.25. When the server responds, it does so to the NAT address. You can see the session is successful as indicated by the three-way handshake between the host and the server and then you see Telnet data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.10	10.43.14.55	TCP	66	61.214 > telnet [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000661	10.43.14.55	10.43.14.25	TCP	66	telnet > 59293 [SYN, ACK] seq=0 Ack=0 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	0.001144	192.168.2.10	10.43.14.55	TCP	66	61.214 > telnet [ACK] Seq=1 Ack=1 win=65536 Len=0
		10.43.14.55	10.43.14.25	TELNET	69	Telnet data ...
		192.168.2.10	10.43.14.55	TELNET	60	Telnet data ...
		10.43.14.55	10.43.14.25	TCP	54	telnet > 59293 [ACK] Seq=16 Ack=6 win=14720 Len=0
		192.168.2.10	10.43.14.55	TELNET	57	Telnet data ...
		10.43.14.55	10.43.14.25	TCP	6	6 Telnet data ...
		192.168.2.10	10.43.14.55	TELNET	4	4 telnet > 59293 [ACK] Seq=32 Ack=16 win=14720 Len=0
		10.43.14.55	10.43.14.25	TCP	3	3 Telnet data ...
		192.168.2.10	10.43.14.55	TELNET	6	6 Telnet data ...
		10.43.14.55	10.43.14.25	TCP	60	Telnet data ...
11	0.064820	10.43.14.55	10.43.14.25	TELNET		
12	0.065304	192.168.2.10	10.43.14.55	TELNET		

### Take a Threat Packet Capture

To configure the firewall to take a packet capture (pcap) when it detects a threat, enable packet capture on Antivirus, Anti-Spyware, and Vulnerability Protection security profiles.

#### Take a Threat Packet Capture

##### Step 1 Enable the packet capture option in the security profile.

Some security profiles allow you to define a single-packet capture, or extended-capture. If you choose extended-capture, define the capture length. This will allow the firewall to capture more packets to provide additional context related to the threat.



The firewall can only capture packets if the action for a given threat is set to allow or alert.

##### 1. Select **Objects > Security Profiles** and enable the packet capture option for the supported profiles as follows:

- **Antivirus**—Select a custom antivirus profile and in the **Antivirus** tab select the **Packet Capture** check box.
- **Anti-Spyware**—Select a custom Anti-Spyware profile, click the **DNS Signatures** tab and in the **Packet Capture** drop-down, select **single-packet** or **extended-capture**.
- **Vulnerability Protection**—Select a custom Vulnerability Protection profile and in the **Rules** tab, click **Add** to add a new rule, or select an existing rule. Set **Packet Capture** to **single-packet** or **extended-capture**. Note that if the profile has signature exceptions defined, click the **Exceptions** tab and in the **Packet Capture** column for a signature, set **single-packet** or **extended-capture**.

##### 2. (Optional) If you selected **extended-capture** for any of the profiles, define the extended packet capture length.

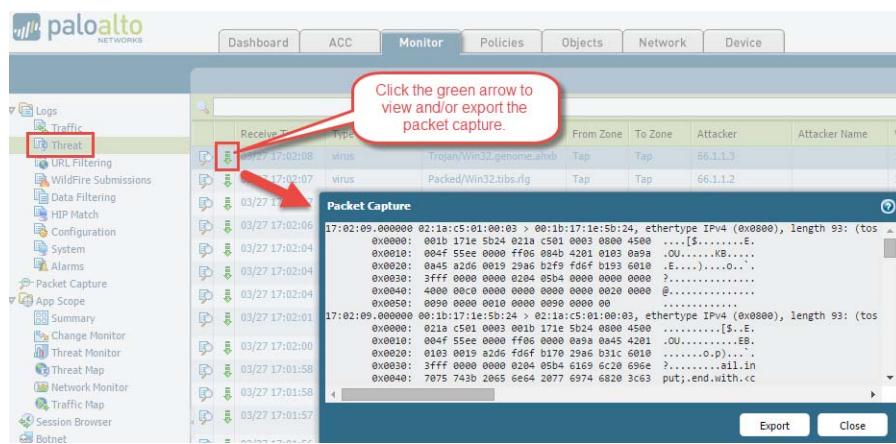
- Select **Device > Setup > Content-ID** and edit the Content-ID Settings.
- In the **Extended Packet Capture Length (packets)** section, specify the number of packets that the firewall will capture (range is 1-50; default is 5).
- Click **OK**.

### Take a Threat Packet Capture (Continued)

- |  |   |
|--|---|
| <b>Step 2</b> Add the security profile (with packet capture enabled) to a <b>Security Policy</b> rule. | <ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b> and select a rule.</li> <li>2. Select the <b>Actions</b> tab.</li> <li>3. In the Profile Settings section, select a profile that has packet capture enabled.</li> </ol> <p>For example, click the <b>Antivirus</b> drop-down and select a profile that has packet capture enabled.</p> |
|--|---|

- Step 3** View/export the packet capture from the Threat logs.

1. Select **Monitor > Logs > Threat**.
2. In the log entry that you are interested in, click the green packet capture icon in the second column. View the packet capture directly or **Export** it to your system.



### Take an Application Packet Capture

The following topics describe two ways that you can configure the firewall to take application packet captures:

- ▲ [Take a Packet Capture for Unknown Applications](#)
- ▲ [Take a Custom Application Packet Capture](#)

### Take a Packet Capture for Unknown Applications

Palo Alto Networks firewalls automatically generate a packet capture for sessions that contain an application that it cannot identify. Typically, the only applications that are classified as unknown traffic—tcp, udp or non-syn-tcp—are commercially available applications that do not yet have App-ID signatures, are internal or custom applications on your network, or potential threats. You can use these packet captures to gather more context related to the unknown application or use the information to analyze the traffic for potential threats. You can also [Manage Custom or Unknown Applications](#) by controlling them through security policy or by

writing a custom application signature and creating a security rule based on the custom signature. If the application is a commercial application, you can submit the packet capture to Palo Alto Networks to have an App-ID signature created.

### Identify Unknown Applications in Traffic Logs and View Packet Captures

**Step 1** Verify that unknown application packet capture is enabled. This option is on by default.

1. To view the unknown application capture setting, run the following CLI command:  
`admin@PA-200> show running application setting | match "Unknown capture"`
2. If the unknown capture setting option is off, enable it:  
`admin@PA-200> set application dump-unknown yes`

**Step 2** Locate unknown application by filtering the traffic logs.

1. Select **Monitor > Logs > Traffic**.
2. Click **Add Filter** and select the filters as shown in the following example.

The screenshot shows the 'Logs' section of the Palo Alto Networks interface. On the left, there's a sidebar with various monitoring and reporting options like Threat, URL Filtering, and Traffic. The 'Traffic' section is selected. In the center, a 'Logs' table displays network traffic. Above the table, a 'Log Filter' dialog is open. The search bar contains '(app eq unknown-tcp)'. The 'Add Filter' and 'Apply Filter' buttons are highlighted with red boxes.

3. Click **Add** and **Apply Filter**.

**Step 3** Click the packet capture icon to view the packet capture or **Export** it to your local system.

The screenshot shows the 'Logs' section with the 'Traffic' filter applied. The 'Logs' table now shows only traffic for 'unknown-tcp'. A 'Packet Capture' window is open, displaying a list of captured packets. The 'Receive Time' and 'Application' columns are highlighted with red boxes. A red arrow points from the 'Packet capture download icons' label to the icons in the table header. The 'Export' button is also highlighted with a red box.

## Take a Custom Application Packet Capture

You can configure a Palo Alto Networks firewall to take a packet capture based on an application name and filters that you define. You can then use the packet capture to troubleshoot issues with controlling an application. When configuring an application packet capture, you must use the application name defined in the App-ID database. You can view a list of all App-ID applications using [Applipedia](#) or from the web interface on the firewall in **Objects > Applications**.

### Take a Custom Application Packet Capture

**Step 1** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

**Step 2** Turn on the application packet capture and define filters.

```
admin@PA-200> set application dump on application <application-name> rule <rule-name>
```

For example, to capture packets for the facebook-base application that matches the security rule named rule1, run the following CLI command:

```
admin@PA-200> set application dump on application facebook-base rule rule1
```



You can also apply other filters, such as source IP address and destination IP address.

**Take a Custom Application Packet Capture (Continued)**

**Step 3** View the output of the packet capture settings to ensure that the correct filters are applied. The output appears after enabling the packet capture.

In the following output, you see that application filtering is now on based on the facebook-base application for traffic that matches rule1.

```
Application setting:  
Application cache : yes  
Supernode : yes  
Heuristics : yes  
Cache Threshold : 16  
Bypass when exceeds queue limit: no  
Traceroute appid : yes  
Traceroute TTL threshold : 30  
Use cache for appid : no  
Unknown capture : on  
Max. unknown sessions : 5000  
Current unknown sessions : 0  
Application capture : on  
Max. application sessions : 5000  
Current application sessions : 0  
Application filter setting:  
  Rule : rule1  
  From : any  
  To : any  
  Source : any  
  Destination : any  
  Protocol : any  
  Source Port : any  
  Dest. Port : any  
  Application : facebook-base  
Current APPID Signature  
  Signature Usage : 21 MB (Max. 32 MB)  
    TCP 1 C2S : 15503 states  
    TCP 1 S2C : 5070 states  
    TCP 2 C2S : 2426 states  
    TCP 2 S2C : 702 states  
    UDP 1 C2S : 11379 states  
    UDP 1 S2C : 2967 states  
    UDP 2 C2S : 755 states  
    UDP 2 S2C : 224 states
```

**Step 4** To turn off application packet capture after the traffic you are interested in has traversed the firewall:

```
admin@PA-200> set application dump off
```

## Take a Custom Application Packet Capture (Continued)

**Step 5** View/export the packet capture.

1. Log in to the web interface on the firewall and select **Monitor > Logs > Traffic**.
2. In the log entry that you are interested in, click the green packet capture icon  in the second column.



Receive Time	From Zone	To Zone	Source	S... U...	To Port	Application	Action	Rule	Session End Reason	Byt...
04/09 09:52:29	end	I3-vlan-trust	I3-untrust	192.168.2.10	443	facebook-base	allow	rule1	tcp-rst-from-client	36.1k
04/09 09:52:29	end	I3-vlan-trust	I3-untrust	192.168.2.10	443	facebook-base	allow	rule1	tcp-fin	5.1k
04/09 09:52:29	end	I3-vlan-trust	I3-untrust	192.168.2.10	443	facebook-base	allow	rule1	tcp-fin	16.8k
04/09 09:52:25	end	I3-vlan-trust	I3-untrust	192.168.2.10	389	ldap	allow	rule1	aged-out	435

3. View the packet capture directly or **Export** it to your local system. The following screen capture shows the facebook-base packet capture.



## Take a Packet Capture on the Management Interface

The `tcpdump` CLI command enables you to capture packets that traverse the management interface (MGT) on a Palo Alto Networks firewall.



Each platform has a default number of bytes that `tcpdump` captures. The PA-200, PA-500, and PA-2000 Series firewalls capture 68 bytes of data from each packet and anything over that is truncated. The PA-3000, PA-4000, PA-5000 Series, the PA-7000 Series firewalls, and VM-Series firewalls capture 96 bytes of data from each packet. To define the number of packets that `tcpdump` will capture, use the `snaplen` (snap length) option (range 0-65535). Setting the `snaplen` to 0 will cause the firewall to use the maximum length required to capture whole packets.

## Take a Management Interface Packet Capture

**Step 1** Using a terminal emulation application, such as PuTTY, launch an SSH session to the firewall.

## Take a Management Interface Packet Capture (Continued)

- Step 2** To start a packet capture on the MGT interface, run the following command:

```
admin@PA-200> tcpdump filter "<filter-option> <IP-address>" snaplen length
```

For example, to capture the traffic that is generated when an administrator authenticates to the firewall using RADIUS, filter on the destination IP address of the RADIUS server (10.5.104.99 in this example):

```
admin@PA-200> tcpdump filter "dst 10.5.104.99" snaplen 0
```

You can also filter on src (source IP address), host, net, and you can exclude content. For example, to filter on a subnet and exclude all SCP, SFTP, and SSH traffic (which uses port 22), run the following command:

```
admin@PA-200> tcpdump filter "net 10.5.104.0/24 and not port 22" snaplen 0
```



Each time `tcpdump` takes a packet capture, it stores the content in a file named `mgmt.pcap`. This file is overwritten each time you run `tcpdump`.

- Step 3** After the traffic you are interested in has traversed the MGT interface, press `ctrl + c` to stop the capture.

- Step 4** View the packet capture by running the following command:

```
admin@PA-200> view-pcap mgmt-pcap mgmt.pcap
```

The following output shows the packet capture from the MGT port (10.5.104.98) to the RADIUS server (10.5.104.99):

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, Access Request (1), id: 0x00 length: 89
09:55:29.144354 arp reply 10.5.104.98 is-at 00:25:90:23:94:98 (oui Unknown)
09:55:29.379290 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, Access Request (1), id: 0x00 length: 70
09:55:34.379262 arp who-has 10.5.104.99 tell 10.5.104.98
```

- Step 5** (Optional) Export the packet capture from the firewall using SCP (or TFTP). For example, to export the packet capture using SCP, run the following command:

```
admin@PA-200> scp export mgmt-pcap from mgmt.pcap to username@host:path
```

For example, to export the pcap to an SCP enabled server at 10.5.5.20 to a temp folder named `temp-SCP`, run the following CLI command:

```
admin@PA-200> scp export mgmt-pcap from mgmt.pcap to admin@10.5.5.20:c:/temp-SCP
```

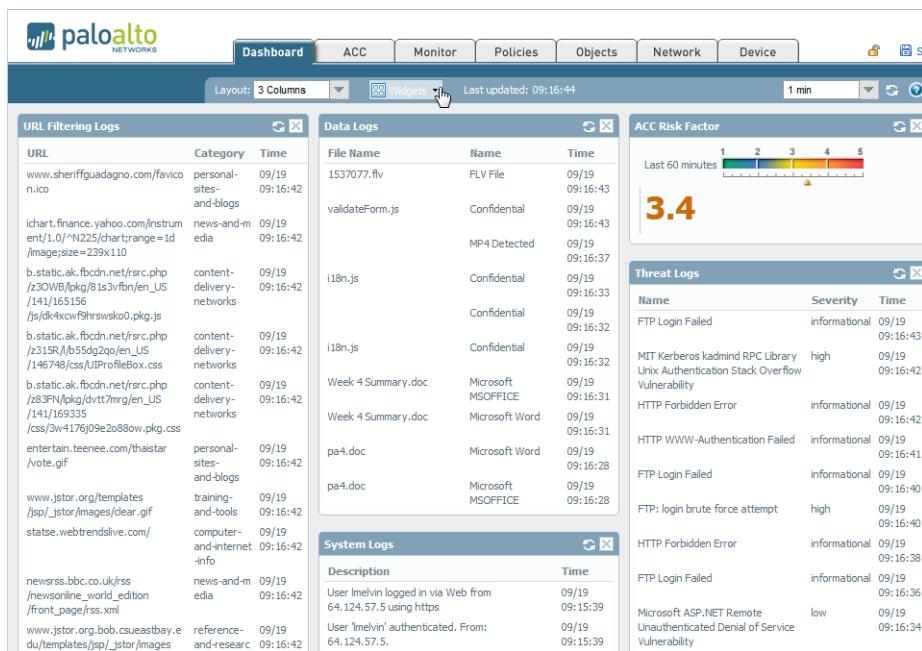
Enter the login name and password for the account on the SCP server and the firewall will copy the packet capture to the SCP enabled server to `c:\temp-SCP`.

- Step 6** You can now view the packet capture files using a network packet analyzer, such as Wireshark.

# Monitor Applications and Threats

All Palo Alto Networks next-generation firewalls come equipped with the [App-ID](#) technology, which identifies the applications traversing your network, irrespective of protocol, encryption, or evasive tactic. You can then [Use the Application Command Center](#) to monitor the applications. The ACC graphically summarizes the data from a variety of log databases to highlight the applications traversing your network, who is using them, and their potential security impact. ACC is dynamically updated, using the continuous traffic classification that App-ID performs; if an application changes ports or behavior, App-ID continues to see the traffic, displaying the results in ACC. Additional visibility into URL categories, threats, and data provides a complete and well-rounded picture of network activity. With ACC, you can very quickly learn more about the traffic traversing the network and then translate that information into a more informed security policy.

You can also [Use the Dashboard](#) to monitor the network.



## Monitor and Manage Logs

All Palo Alto Networks next-generation firewalls can generate log files that provide an audit trail of the activities and events on the firewall. There are separate logs for separate types of activities and events. For example, the Threat logs record all traffic that causes the firewall to generate a security alarm, URL Filtering logs record all traffic that matches a URL Filtering profile attached to a security rule, and Config logs record all changes to the firewall configuration. The firewall uses log data to generate reports (**Monitor > Reports**), which display the data in a tabular or graphical format. See [Manage Reporting](#) for details.

The following topics describe how to view logs locally on the firewall. You can also [Use External Services for Monitoring](#) logs.

- ▲ [View the Log Files](#)
- ▲ [Filter Log Data](#)
- ▲ [Configure Log Storage Quotas and Expiration Periods](#)
- ▲ [Log Severity Levels and WildFire Verdicts](#)
- ▲ [Schedule Log Exports to an SCP or FTP Server](#)

## View the Log Files

The firewall maintains logs for WildFire, configurations, system events, alarms, traffic flows, threats, URL filtering, data filtering, and Host Information Profile (HIP) matches. You can view the current logs at any time. To locate specific entries, you can apply filters to most of the log fields.



The firewall displays the information in logs so that role-based administration permissions are respected. When you display logs, only the information that you have permission to see is included. For information on administrator permissions, see [Administrative Roles](#).

By default all log files are generated and stored locally on the firewall. You can view these log files in the **Monitor > Logs** pages:

	Receive Time	Type	Name	From Zone	To Zone	Attacker
	03/26 14:42:44	spyware	Sip vicious.sundayddr User-Agent Traffic	TAP-138	TAP-138	202.103.52.147
	03/26 14:42:33	vulnerability	FTP: login Brute-force attempt	TAP-138	TAP-138	61.136.188.83
	03/26 14:42:31	vulnerability	FTP: login Brute-force attempt	TAP-138	TAP-138	61.136.188.83
	03/26 14:42:29	vulnerability	FTP: login Brute-force attempt	TAP-138	TAP-138	61.136.188.83
	03/26 14:42:25	vulnerability	FTP: login Brute-force	TAP-138	TAP-138	61.136.188.83

To display additional details, click the spyglass icon for an entry.

Related Logs (+/- 24 Hours)											
PCAP	Receive Time	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL/...
2014/03/25 11:02:58	TRAFFIC	end	incomplete	allow	rule1		134	2		any	

The following table includes information on each log type:

Log Description Charts	Description
Traffic	<p>Displays an entry for the start and end of each session. Each entry includes the date and time, source and destination zones, addresses and ports, application name, security rule name applied to the flow, rule action (<b>allow</b>, <b>deny</b>, or <b>drop</b>), ingress and egress interface, number of bytes, and session end reason.</p> <p>Click  next to an entry to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (the <b>Count</b> value will be greater than one).</p> <p>The <b>Type</b> column indicates whether the entry is for the start or end of the session, or whether the session was denied or dropped. A <b>drop</b> indicates that the security rule that blocked the traffic specified <b>any</b> application, while a <b>deny</b> indicates the rule identified a specific application.</p> <p>If traffic is dropped before the application is identified, such as when a rule drops all traffic for a specific service, the application is shown as <b>not-applicable</b>.</p>
Threat	<p>Displays an entry when traffic matches a Security Profile (Antivirus, Anti-Spyware, Vulnerability, URL Filtering, File Blocking, Data Filtering, or DoS Protection) that is attached to a security rule on the firewall. Each entry includes the date and time, a threat name or URL, the source and destination zones, addresses, and ports, the application name, and the alarm action (<b>allow</b> or <b>block</b>) and severity.</p> <p>Click  next to an entry to view additional details about the threat, such as whether the entry aggregates multiple threats of the same type between the same source and destination (the <b>Count</b> value will be greater than one).</p> <p>The <b>Type</b> column indicates the type of threat, such as “virus” or “spyware.” The Name column is the threat description or URL, and the <b>Category</b> column is the threat category (such as “keylogger”) or URL category.</p> <p>If local packet captures are enabled, click  next to an entry to access the captured packets. To enable local packet captures, see <a href="#">Take Packet Captures</a>.</p> <p>For details on threat severity levels, see <a href="#">Log Severity Levels and WildFire Verdicts</a>.</p>
URL Filtering	<p>Displays logs for all traffic that matches a URL Filtering profile attached to a security rule. For example, if rule blocks access to specific web sites and web site categories or if rule is configured to generate an alert when a web site is accessed. For information on defining URL filtering profiles, see <a href="#">URL Filtering</a>.</p>
WildFire Submissions	<p>Displays logs for files that are uploaded and analyzed by the WildFire cloud; log data is sent back to the device after analysis, along with the analysis results.</p> <p>For details on WildFire verdicts (benign or malicious), see <a href="#">Log Severity Levels and WildFire Verdicts</a>.</p>

Log Description Charts	Description
Data Filtering	<p>Displays logs for the security rules that help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall. See <a href="#">Set Up Data Filtering</a> for information on defining data filtering profiles.</p> <p>This log also shows information for file-blocking profiles. For example, if you are blocking .exe files, the log will show the files that were blocked. If you forward files to WildFire, you will see the results of that action. In this case, if you are forwarding PE files to WildFire, for example, the log will show that the file was forwarded and will also show the status on whether or not it was uploaded to WildFire successfully.</p>
Configuration	<p>Displays an entry for each configuration change. Each entry includes the date and time, the administrator username, the IP address from where the change was made, the type of client (XML, Web or CLI), the type of command executed, whether the command succeeded or failed, the configuration path, and the values before and after the change.</p>
System	<p>Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.</p> <p>For details on System log severity levels, see <a href="#">Log Severity Levels and WildFire Verdicts</a>.</p>
HIP Match	<p>Displays traffic flows that match a <a href="#">HIP Object</a> or <a href="#">HIP Profile</a> that you have configured.</p>

## Filter Log Data

Each log page has a filter area at the top of the page.



Use the filter area as follows:

- Click any of the underlined links in the log listing to add that item as a log filter option. For example, if you click the **Host** link in the log entry for 10.0.0.252 and **Web Browsing**, both items are added, and the search will find entries that match both (AND search).
- To define other search criteria, click **Add Log Filter**. Select the type of search (and/or), the attribute to include in the search, the matching operator, and the values for the match, if appropriate. Click **Add** to add the criterion to the filter area on the log page, and then click **Close** to close the pop-up window. Click **Apply Filter** to display the filtered list.



If the **Value** string matches an **Operator** (such as **has** or **in**), enclose the string in quotation marks to avoid a syntax error. For example, if you filter by destination country and use **IN** as a **Value** to specify INDIA, enter the filter as `( dstloc eq "IN" )`.

You can combine filter expressions added on the log page with those you define in the Add Log Filter dialog. The filter field on the log page displays each filter as an entry.

If you add a **Receive Time** filter with the **Operator** set to **in** and the **Value** set to **Last 60 seconds**, some of the page links on the log viewer might not show results because the number of pages might grow or shrink due to the dynamic nature of the selected time.

- To clear filters and redisplay the unfiltered list, click **Clear Filter**.
- To save your selections as a new filter, click **Save Filter**, enter a name for the filter, and click **OK**.
- To export the current log listing (as shown on the page, including any applied filters) click **Save Filter**. Select whether to open the file or save it to disk, and select the check box if you want to always use the same option. Click **OK**.
- To export the current log listing in CSV Format, select the **Export to CSV** icon. By default, exporting the log listing to CSV format generates a CSV report with up to 2,000 rows of logs. To change the limit for rows displayed in CSV reports, use the **Max Rows in CSV Export** field on the **Log Export and Reporting** tab (select **Device > Setup > Management > Logging and Reporting Settings**).

To change the automatic refresh interval, select an interval from the drop-down (**1 min**, **30 seconds**, **10 seconds**, or **Manual**).

To change the number of log entries per page, select the number of rows from the **Rows** drop-down.

Log entries are retrieved in blocks of 10 pages. Use the paging controls at the bottom of the page to navigate through the log list. Select the **Resolve Hostname** check box to begin resolving external IP addresses to domain names.

## Configure Log Storage Quotas and Expiration Periods

The firewall automatically deletes logs that exceed the expiration period. When the firewall reaches the storage quota for a log type, it automatically deletes older logs of that type to create space even if you don't set an expiration period.



If you want to manually delete logs, select **Device > Log Settings** and, in the Manage Logs section, click the links to clear logs by type.

### Configure Log Storage Quotas and Expiration Periods

- Step 1 Select **Device > Setup > Management** and edit the Logging and Reporting Settings.
- Step 2 In the **Log Storage** tab, select the **Log Storage** check box and enter the **Quota (%)** for each log type. When you change a percentage value, the dialog refreshes to display the corresponding absolute value (Quota GB/MB column).
- Step 3 Enter the **Max Days** (expiration period) for each log type (range is 1-2,000). The fields are blank by default, which means the logs never expire.



The firewall synchronizes expiration periods across high availability (HA) pairs. Because only the active HA peer generates logs, the passive peer has no logs to delete unless failover occurs and it starts generating logs.

- Step 4 Click **OK** and **Commit**.

## Log Severity Levels and WildFire Verdicts

The following table summarizes the Threat severity levels:

Severity	Description
<b>Critical</b>	Serious threats, such as those that affect default installations of widely deployed software, result in root compromise of servers, and the exploit code is widely available to attackers. The attacker usually does not need any special authentication credentials or knowledge about the individual victims and the target does not need to be manipulated into performing any special functions.
<b>High</b>	Threats that have the ability to become critical but have mitigating factors; for example, they may be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool.
<b>Medium</b>	Minor threats in which impact is minimized, such as DoS attacks that do not compromise the target or exploits that require an attacker to reside on the same LAN as the victim, affect only non-standard configurations or obscure applications, or provide very limited access. In addition, WildFire Submissions log entries with a malware verdict are logged as Medium.
<b>Low</b>	Warning-level threats that have very little impact on an organization's infrastructure. They usually require local or physical system access and may often result in victim privacy or DoS issues and information leakage. Data Filtering profile matches are logged as Low.
<b>Informational</b>	Suspicious events that do not pose an immediate threat, but that are reported to call attention to deeper problems that could possibly exist. URL Filtering log entries and WildFire Submissions log entries with a benign verdict are logged as Informational.

The following table summarizes the System log severity levels. For a partial list of System log messages and their corresponding severity levels, refer to [System Log Events](#).

Severity	Description
<b>Critical</b>	Hardware failures, including HA failover and link failures.
<b>High</b>	Serious issues, including dropped connections with external devices, such as LDAP and RADIUS servers.
<b>Medium</b>	Mid-level notifications, such as antivirus package upgrades.
<b>Low</b>	Minor severity notifications, such as user password changes.
<b>Informational</b>	Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.

The following table summarizes the Correlation log severity levels:

Severity	Description
<b>Critical</b>	Confirms that a host has been compromised based on correlated events that indicate an escalation pattern. For example, a critical event is logged when a host that received a file with a malicious verdict by WildFire, exhibits the same command-and control activity that was observed in the WildFire sandbox for that malicious file.

Severity	Description
<b>High</b>	Indicates that a host is very likely compromised based on a correlation between multiple threat events, such as malware detected anywhere on the network that matches the command and control activity being generated from a particular host.
<b>Medium</b>	Indicates that a host is likely compromised based on the detection of one or multiple suspicious events, such as repeated visits to known malicious URLs that suggests a scripted command-and-control activity.
<b>Low</b>	Indicates that a host is possibly compromised based on the detection of one or multiple suspicious events, such as a visit to a malicious URL or a dynamic DNS domain.
<b>Informational</b>	Detects an event that may be useful in aggregate for identifying suspicious activity; each event is not necessarily significant on its own.

The following table summarizes the WildFire verdicts:

Severity	Description
<b>Benign</b>	Indicates that the entry received a WildFire analysis verdict of benign. Files categorized as benign are safe and do not exhibit malicious behavior.
<b>Grayware</b>	Indicates that the entry received a WildFire analysis verdict of grayware. Files categorized as grayware do not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware can include, adware, spyware, and Browser Helper Objects (BHOs).
<b>Malware</b>	Indicates that the entry received a WildFire analysis verdict of malware. Files categorized as malware are malicious in intent or nature and can pose a security threat. Malware can include viruses, worms, Trojans, Remote Access Tools (RATs), rootkits, and botnets. For files that are identified as malware, a signature is generated and distributed by the WildFire cloud to prevent against future exposure.

## Schedule Log Exports to an SCP or FTP Server

You can schedule exports of Traffic, Threat, URL Filtering, Data Filtering, HIP Match, and WildFire Submission logs to a Secure Copy (SCP) server or File Transfer Protocol (FTP) server. Perform this task for each log type you want to export.



You can [use Secure Copy \(SCP\) commands from the CLI](#) to export the entire log database to an SCP server and import it to another firewall. Because the log database is too large for an export or import to be practical on the following platforms, they do not support these options: PA-7000 Series firewalls (all PAN-OS releases), Panorama virtual appliance running Panorama 6.0 or later releases, and Panorama M-Series appliances (all Panorama releases).

### Schedule Log Exports to an SCP or FTP Server

**Step 1** Select **Device > Scheduled Log Export** and click **Add**.

**Step 2** Enter a **Name** for the scheduled log export and **Enable** it.

**Step 3** Select the **Log Type** to export.

**Step 4** Select the daily **Scheduled Export Start Time**. The options are in 15-minute increments for a 24-hour clock (00:00 - 23:59).

**Step 5** Select the **Protocol** to export the logs: **SCP** (secure) or **FTP**.

**Step 6** Enter the **Hostname** or IP address of the server.

**Step 7** Enter the **Port** number. By default, FTP uses port 21 and SCP uses port 22.

**Step 8** Enter the **Path** or directory in which to save the exported logs.

**Step 9** Enter the **Username** and, if necessary, the **Password** (and **Confirm Password**) to access the server.

**Step 10** (FTP only) Select the **Enable FTP Passive Mode** check box if you want to use FTP passive mode, in which the firewall initiates a data connection with the FTP server. By default, the firewall uses FTP active mode, in which the FTP server initiates a data connection with the firewall. Choose the mode based on what your FTP server supports and on your network requirements.

**Step 11** (SCP only) Click **Test SCP server connection**. Before establishing a connection, the firewall must accept the host key for the SCP server.



If you use a Panorama template to configure the log export schedule, you must perform this step after committing the template configuration to the firewalls. After the template commit, log in to each firewall, open the log export schedule, and click **Test SCP server connection**.

**Step 12** Click **OK** and **Commit**.

# Manage Reporting

The reporting capabilities on the firewall allow you to keep a pulse on your network, validate your policies, and focus your efforts on maintaining network security for keeping your users safe and productive.

- ▲ [Report Types](#)
- ▲ [View Reports](#)
- ▲ [Configure the Report Expiration Period](#)
- ▲ [Disable Predefined Reports](#)
- ▲ [Generate Custom Reports](#)
- ▲ [Generate Botnet Reports](#)
- ▲ [Manage PDF Summary Reports](#)
- ▲ [Generate User/Group Activity Reports](#)
- ▲ [Manage Report Groups](#)
- ▲ [Schedule Reports for Email Delivery](#)

## Report Types

The firewall includes predefined reports that you can use as-is, or you can build custom reports that meet your needs for specific data and actionable tasks, or you can combine predefined and custom reports to compile information you need. The firewall provides the following types of reports:

- **Predefined Reports**—Allow you to view a quick summary of the traffic on your network. A suite of predefined reports are available in four categories—Applications, Traffic, Threat, and URL Filtering. See [View Reports](#).
- **User or Group Activity Reports**—Allow you to schedule or create an on-demand report on the application use and URL activity for a specific user or for a user group. The report includes the URL categories and an estimated browse time calculation for individual users. See [Generate User/Group Activity Reports](#).
- **Custom Reports**—Create and schedule custom reports that show exactly the information you want to see by filtering on conditions and columns to include. You can also include query builders for more specific drill down on report data. See [Generate Custom Reports](#).
- **PDF Summary Reports**—Aggregate up to 18 predefined or custom reports/graphs from Threat, Application, Trend, Traffic, and URL Filtering categories into one PDF document. See [Manage PDF Summary Reports](#).
- **Botnet Reports**—Allow you to use behavior-based mechanisms to identify potential botnet-infected hosts in the network. See [Generate Botnet Reports](#).
- **Report Groups**—Combine custom and predefined reports into report groups and compile a single PDF that is emailed to one or more recipients. See [Manage Report Groups](#).

Reports can be generated on demand, on a recurring schedule, and can be scheduled for email delivery.

## View Reports

The firewall provides an assortment of over 40 predefined reports that it generates every day. You can view these reports directly on the firewall. You can also view custom reports and summary reports.

About 200 MB of storage is allocated for saving reports on the firewall. You can't configure this limit but you can [Configure the Report Expiration Period](#): the firewall will automatically delete reports that exceed the period. Keep in mind that when the firewall reaches its storage limit, it automatically deletes older reports to create space even if you don't set an expiration period. Another way to conserve system resources on the firewall is to [Disable Predefined Reports](#). For long-term retention of reports, you can export the reports (as described below) or [Schedule Reports for Email Delivery](#).



Unlike other reports, you can't save User/Group Activity reports on the firewall. You must [Generate User/Group Activity Reports](#) on demand or schedule them for email delivery.

### View Reports

#### Step 1 Select **Monitor > Reports**.

The reports are chunked into sections on the right-hand side of the window: **Custom Reports, Application Reports, Traffic Reports, Threat Reports, URL Filtering Reports, and PDF Summary Reports**.

#### Step 2 Select a report to view. When you select a report, the previous day's report is displayed onscreen.

To view reports for any of the previous days, select an available date from the calendar at the bottom of the page and select a report within the same section. If you change sections, the time selection is reset.

#### Step 3 To view a report offline, you can export the report to PDF, CSV or to XML formats. Click **Export to PDF**, **Export to CSV**, or **Export to XML** at the bottom of the page. Then print or save the file.

## Configure the Report Expiration Period

When you set the **Report Expiration Period**, it applies to all [Report Types](#). The firewall automatically deletes reports that exceed the period.

### Configure Report Expiration Periods

**Step 1** Select **Device > Setup > Management**, edit the Logging and Reporting Settings, and select the **Log Export and Reporting** tab.

**Step 2** Enter the **Report Expiration Period** in days (range is 1-2000, default is no expiration).



You can't change the storage that the firewall allocates for saving reports: it is predefined at about 200 MB. When the firewall reaches the storage maximum, it automatically deletes older reports to create space even if you don't set a **Report Expiration Period**.

**Step 3** Click **OK** and **Commit**.

## Disable Predefined Reports

The firewall includes about 40 predefined reports that it automatically generates daily. If you do not use some or all of these, you can disable selected reports to conserve system resources on the firewall.

Make sure that no [report group](#) or [PDF summary report](#) includes the predefined reports you will disable. Otherwise, the firewall will render the PDF summary report or report group without any data.

### Disable Predefined Reports

**Step 1** Select **Device > Setup > Management** and edit the Logging and Reporting Settings.

**Step 2** Select the **Pre-Defined Reports** tab and clear the check box for each report you want to disable. To disable all predefined reports, click **Deselect All**.

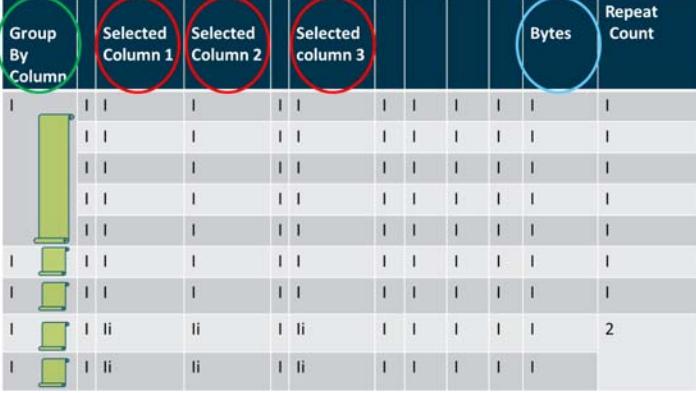


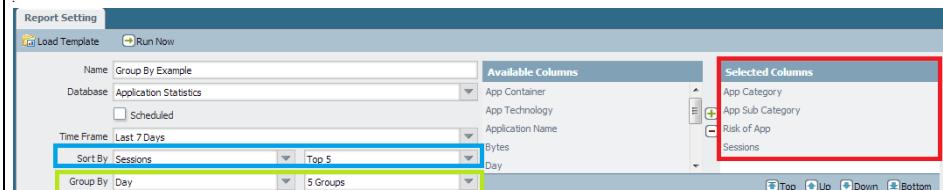
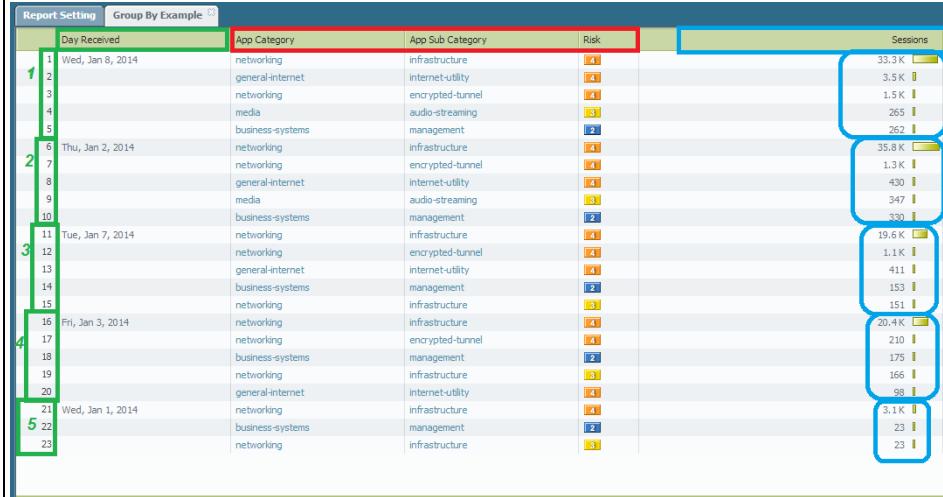
**Step 3** Click **OK** and **Commit**.

## Generate Custom Reports

In order to create purposeful custom reports, you must consider the attributes or key pieces of information that you want to retrieve and analyze. This consideration guides you in making the following selections in a custom report:

Selection	Description
Data Source	<p>The data file that is used to generate the report. The firewall offers two types of data sources—Summary databases and Detailed logs.</p> <ul style="list-style-type: none"> <li>Summary databases are available for traffic, threat, and application statistics. The firewall aggregates the detailed logs on traffic, application, and threat at 15-minute intervals. The data is condensed—duplicate sessions are grouped together and incremented with a repeat counter, and some attributes (or columns) are not included in the summary—to allow faster response time when generating reports.</li> <li>Detailed logs are itemized and are a complete listing of all the attributes (or columns) that pertain to the log entry. Reports based on detailed logs take much longer to run and are not recommended unless absolutely necessary.</li> </ul>
Attributes	<p>The columns that you want to use as the match criteria. The attributes are the columns that are available for selection in a report. From the list of <b>Available Columns</b>, you can add the selection criteria for matching data and for aggregating the details (the <b>Selected Columns</b>).</p>
Sort By/ Group By	<p>The <b>Sort By</b> and the <b>Group By</b> criteria allow you to organize/segment the data in the report; the sorting and grouping attributes available vary based on the selected data source.</p> <p>The Sort By option specifies the attribute that is used for aggregation. If you do not select an attribute to sort by, the report will return the first N number of results without any aggregation.</p> <p>The Group By option allows you to select an attribute and use it as an anchor for grouping data; all the data in the report is then presented in a set of top 5, 10, 25 or 50 groups. For example, when you select Hour as the Group By selection and want the top 25 groups for a 24-hr time period, the results of the report will be generated on an hourly basis over a 24-hr period. The first column in the report will be the hour and the next set of columns will be the rest of your selected report columns.</p>

Selection	Description																																																																													
	<p>The following example illustrates how the <b>Selected Columns</b> and <b>Sort By/Group By</b> criteria work together when generating reports:</p>  <table border="1"> <thead> <tr> <th>Group By Column</th> <th>Selected Column 1</th> <th>Selected Column 2</th> <th>Selected column 3</th> <th></th> <th>Bytes</th> <th>Repeat Count</th> </tr> </thead> <tbody> <tr><td>I</td><td>I I</td><td>I</td><td>I I</td><td>I I</td><td>I</td><td>I</td></tr> <tr><td>I</td><td>I I</td><td>I I</td><td>I I</td><td>I I</td><td>I</td><td>2</td></tr> </tbody> </table> <p>The columns circled in red (above) depict the columns selected, which are the attributes that you match against for generating the report. Each log entry from the data source is parsed and these columns are matched on. If multiple sessions have the same values for the selected columns, the sessions are aggregated and the repeat count (or sessions) is incremented.</p> <p>The column circled in blue indicates the chosen sort order. When the sort order (<b>Sort By</b>) is specified, the data is sorted (and aggregated) by the selected attribute.</p> <p>The column circled in green indicates the <b>Group By</b> selection, which serves as an anchor for the report. The <b>Group By</b> column is used as a match criteria to filter for the top N groups. Then, for each of the top N groups, the report enumerates the values for all the other selected columns.</p>	Group By Column	Selected Column 1	Selected Column 2	Selected column 3		Bytes	Repeat Count	I	I I	I	I I	I I	I	I	I	I I	I	I I	I I	I	I	I	I I	I	I I	I I	I	I	I	I I	I	I I	I I	I	I	I	I I	I	I I	I I	I	I	I	I I	I	I I	I I	I	I	I	I I	I I	I I	I I	I	I	I	I I	I I	I I	I I	I	I	I	I I	I I	I I	I I	I	I	I	I I	I I	I I	I I	I	2
Group By Column	Selected Column 1	Selected Column 2	Selected column 3		Bytes	Repeat Count																																																																								
I	I I	I	I I	I I	I	I																																																																								
I	I I	I	I I	I I	I	I																																																																								
I	I I	I	I I	I I	I	I																																																																								
I	I I	I	I I	I I	I	I																																																																								
I	I I	I	I I	I I	I	I																																																																								
I	I I	I	I I	I I	I	I																																																																								
I	I I	I I	I I	I I	I	I																																																																								
I	I I	I I	I I	I I	I	I																																																																								
I	I I	I I	I I	I I	I	I																																																																								
I	I I	I I	I I	I I	I	2																																																																								

Selection	Description
	<p>For example, if a report has the following selections</p>  <p>The output will display as follows:</p>  <p>The report is anchored by <b>Day</b> and sorted by <b>Sessions</b>. It lists the 5 days (<b>5 Groups</b>) with maximum traffic in the <b>Last 7 Days</b> time frame. The data is enumerated by the <b>Top 5</b> sessions for each day for the selected columns—<b>App Category</b>, <b>App Subcategory</b> and <b>Risk</b>.</p>
Time Period	<p>The date range for which you want to analyze data. You can define a custom range or select a time period ranging from last 15 minutes to the last 30 days. The reports can be run on demand or scheduled to run at a daily or weekly cadence.</p>
Query Builder	<p>The query builder allows you to define specific queries to further refine the selected attributes. It allows you see just what you want in your report using <b>and</b> and <b>or</b> operators and a match criteria, and then include or exclude data that matches or negates the query in the report. Queries enable you to generate a more focused collation of information in a report.</p>

### Generate Custom Reports

Step 1 Select **Monitor > Manage Custom Reports**.

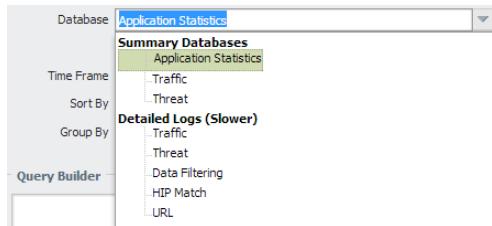
Step 2 Click **Add** and then enter a **Name** for the report.



To base a report on an predefined template, click **Load Template** and choose the template. You can then edit the template and save it as a custom report.

## Generate Custom Reports

- Step 3** Select the **Database** to use for the report.



 Each time you create a custom report, a **Log View** report is automatically created. This report shows the logs that were used to build the custom report. The log view report uses the same name as the custom report, but appends the phrase (Log View) to the report name.

When creating a report group, you can include the log view report with the custom report. For more information, see [Manage Report Groups](#).

- Step 4** Select the **Scheduled** check box to run the report each night. The report is then available for viewing in the **Reports** column on the side.

- Step 5** Define the filtering criteria. Select the **Time Frame**, the **Sort By** order, **Group By** preference, and select the columns that must display in the report.

- Step 6** (Optional) Select the **Query Builder** attributes if you want to further refine the selection criteria. To build a report query, specify the following and click **Add**. Repeat as needed to construct the full query.

- **Connector**—Choose the connector (and/or) to precede the expression you are adding.
- **Negate**—Select the check box to interpret the query as a negation. If, for example, you choose to match entries in the last 24 hours and/or are originating from the untrust zone, the negate option causes a match on entries that are not in the past 24 hours and/or are not from the untrust zone.
- **Attribute**—Choose a data element. The available options depend on the choice of database.
- **Operator**—Choose the criterion to determine whether the attribute applies (such as =). The available options depend on the choice of database.
- **Value**—Specify the attribute value to match.

For example, the following figure (based on the Traffic Log database) shows a query that matches if the traffic log entry was received in the past 24 hours and is from the “untrust” zone.

Connector	Attribute	Operator	Value
and	Zone	=	untrust
or	zone.src	≠	
<input type="checkbox"/> Negate	zone.dst		
<input type="button" value="Add"/>			

- Step 7** To test the report settings, select **Run Now**. Modify the settings as required to change the information that is displayed in the report.

- Step 8** Click **OK** to save the custom report.

## Generate Custom Reports

### Examples of Custom Reports

If you want to set up a simple report in which you use the traffic summary database from the last 30 days, and sort the data by the top 10 sessions and these sessions are grouped into 5 groups by day of the week. You would set up the custom report to look like this:



And the PDF output for the report would look as follows:

### Sample Report

Group By

Column

Selected Columns											Sort By Column
Day Received	Source Zone	Destination Zone	Application	Source address	Source host Name	Description address	Destination host Name	Risk	App Category	Sessions	Bytes
Mon, Dec 16, 2013	trust	untrust	dns	10.47.20.20	10.47.20.20	10.0.0.247	sj0t0vwf02p.paloaltonetworks.local	4	networking	11.26 k	5.41 M
	trust	untrust	dns	10.47.20.20	10.47.20.20	10.0.0.246	sj0t0vwf01p.paloaltonetworks.local	4	networking	11.26 k	6.40 M
	trust	untrust	dns	10.47.20.3	10.47.20.3	10.0.0.247	sj0t0vwf03p.paloaltonetworks.local	4	networking	5.83 k	3.44 M
	trust	untrust	dns	10.47.20.3	10.47.20.3	10.0.0.246	sj0t0vwf01p.paloaltonetworks.local	4	networking	5.83 k	3.48 M
	trust	untrust	dns	10.47.20.5	10.47.20.5	10.43.2.10	sj0t0vwf05p.paloaltonetworks.local	4	networking	1.76 k	414.15 k
	trust	untrust	syslog	10.47.20.20	10.47.20.20	10.2.133.73	10.2.133.73	2	business-systems	260	103.84 k
	trust	untrust	snmp-trap	10.47.20.20	10.47.20.20	10.2.133.73	10.2.133.73	3	networking	200	101.84 k
	trust	untrust	dns	10.47.20.5	10.47.20.5	10.44.2.10	sj0t0vwf05p.paloaltonetworks.local	4	networking	196	43.11 k
	trust	untrust	dnsbox	10.47.20.6	10.47.20.6	10.10.1.101.1234	10.10.1.101.234	4	general-internet	170	60.07 k
	trust	untrust	dns	10.47.20.6	10.47.20.6	10.0.0.246	sj0t0vwf06p.paloaltonetworks.local	4	networking	11.04 k	5.69 M
	trust	untrust	dns	10.47.20.7	10.47.20.7	10.0.0.247	sj0t0vwf07p.paloaltonetworks.local	4	networking	11.04 k	5.68 M
	trust	untrust	dns	10.47.20.7	10.47.20.7	10.0.0.247	sj0t0vwf07p.paloaltonetworks.local	4	networking	5.83 k	3.67 M
	trust	untrust	dns	10.47.20.7	10.47.20.7	10.43.2.10	sj0t0vwf07p.paloaltonetworks.local	4	networking	5.82 k	3.65 M
	trust	untrust	dns	10.47.20.7	10.47.20.7	10.10.1.2.00	sj0t0vwf07p.paloaltonetworks.local	4	networking	1.98 k	471.26 k
	trust	untrust	syslog	10.47.20.7	10.47.20.7	10.2.133.73	10.2.133.73	2	business-systems	278	104.10 k
	trust	untrust	snmp-trap	10.47.20.7	10.47.20.7	10.2.133.73	10.2.133.73	3	networking	278	183.38 k
	trust	untrust	dns	10.47.20.7	10.47.20.7	23.72.35.120	a23-72-35-120.deploy.static.akamaitechnologies.com	4	networking	101	937.11 k
	trust	untrust	web-browsing	10.47.20.7	10.47.20.7	21.27.164.28	21.27.164.28	4	general-internet	90	515.49 k
	trust	untrust	dns	10.47.20.7	10.47.20.7	10.0.0.246	sj0t0vwf07p.paloaltonetworks.local	4	networking	11.35 k	5.50 M
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.0.0.247	sj0t0vwf08p.paloaltonetworks.local	4	networking	11.34 k	5.48 M
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.0.0.246	sj0t0vwf08p.paloaltonetworks.local	4	networking	6.83 k	3.51 M
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.0.0.247	sj0t0vwf08p.paloaltonetworks.local	4	networking	6.82 k	3.53 M
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.43.2.10	sj0t0vwf08p.paloaltonetworks.local	4	networking	1.44 k	348.46 k
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.10.1.2.00	sj0t0vwf08p.paloaltonetworks.local	4	networking	482	24.22 M
	trust	untrust	snmp-trap	10.47.20.8	10.47.20.8	10.2.133.73	10.2.133.73	3	networking	280	190.20 k
	trust	untrust	syslog	10.47.20.8	10.47.20.8	10.2.133.73	10.2.133.73	2	business-systems	280	107.86 k
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.47.0.8	pm-firewall.paloaltonetworks.local	4	networking	222	3.79 M
	trust	untrust	dns	10.47.20.8	10.47.20.8	10.0.0.246	sj0t0vwf08p.paloaltonetworks.local	4	networking	188	41.94 k
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.0.0.247	sj0t0vwf09p.paloaltonetworks.local	4	networking	11.33 k	5.49 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.0.0.246	sj0t0vwf09p.paloaltonetworks.local	4	networking	11.32 k	5.50 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.0.0.247	sj0t0vwf09p.paloaltonetworks.local	4	networking	6.83 k	3.51 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.0.0.246	sj0t0vwf09p.paloaltonetworks.local	4	networking	6.82 k	3.53 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.43.2.10	sj0t0vwf09p.paloaltonetworks.local	4	networking	1.16 k	276.78 k
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.10.1.2.00	sj0t0vwf09p.paloaltonetworks.local	4	networking	496	54.20 M
	trust	untrust	snmp-trap	10.47.20.9	10.47.20.9	10.2.133.73	10.2.133.73	3	networking	280	190.83 k
	trust	untrust	syslog	10.47.20.9	10.47.20.9	10.2.133.73	10.2.133.73	2	business-systems	280	109.07 k
	trust	untrust	web-browsing	10.47.20.9	10.47.20.9	21.27.164.28	21.27.164.28	4	general-internet	220	54.16 k
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.0.0.246	sj0t0vwf09p.paloaltonetworks.local	4	networking	11.40 k	5.53 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.0.0.247	sj0t0vwf09p.paloaltonetworks.local	4	networking	11.39 k	5.51 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.43.2.10	sj0t0vwf09p.paloaltonetworks.local	4	networking	3.69 k	2.19 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.10.1.2.00	sj0t0vwf09p.paloaltonetworks.local	4	networking	3.69 k	2.19 M
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.10.1.2.00	sj0t0vwf09p.paloaltonetworks.local	4	networking	2.35 k	563.08 k
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.10.1.2.00	sj0t0vwf09p.paloaltonetworks.local	4	networking	649	64.13 M
	trust	untrust	snmp-trap	10.47.20.9	10.47.20.9	10.44.2.10	sj0t0vwf09p.paloaltonetworks.local	4	networking	417	99.08 k
	trust	untrust	syslog	10.47.20.9	10.47.20.9	10.2.133.73	10.2.133.73	3	networking	292	198.16 k
	trust	untrust	web-browsing	10.47.20.9	10.47.20.9	10.2.133.73	10.2.133.73	2	business-systems	292	110.95 k
	trust	untrust	dns	10.47.20.9	10.47.20.9	10.101.2.49	10.101.2.49	4	networking	130	5.88 M

## Generate Custom Reports

Now, if you want to use the query builder to generate a custom report that represents the top consumers of network resources within a user group, you would set up the report to look like this:

The report would display the top users in the product management user group sorted by bytes, as follows:

	Source Address	Source Host Name	Source User	Sessions	Bytes
1	10.1.16.35	10.1.16.35	paloaltonetwork\jacob	136	445.3 K
2	10.1.35.48	10.1.35.48	paloaltonetwork\jir	123	410.5 K
3	10.1.16.49	10.1.16.49	paloaltonetwork\louis.vira	103	360.4 K
4	10.1.13.23	10.1.13.23	paloaltonetwork\louis.vira	103	347.2 K
5	10.1.14.51	10.1.14.51	paloaltonetwork\louis.vira	103	334.9 K
6	10.1.11.55	10.1.11.55	paloaltonetwork\ari.pas	96	326.3 K
7	10.1.11.161	10.1.11.161	paloaltonetwork\jif...	84	306.7 K
8	10.1.16.42	pan...@hq.paloaltonetwork...	paloaltonetwork\ari.pas	49	232.2 K
9	10.1.14.145	pan...@hq.paloaltonetwork...	paloaltonetwork\louis.vira	65	201.2 K
10	10.1.1.42	10.1.1.42	paloaltonetwork\jir...	54	191.4 K
11	10.1.5.1.145	pa...@paloaltonetworks.lo...	paloaltonetwork\louis.vira	28	171.2 K
12	10.1.1.26	10.1.1.26	paloaltonetwork\jacob	32	110.0 K
13	10.1.1.74	10.1.1.74	paloaltonetwork\jir...	13	98.6 K

## Generate Botnet Reports

The botnet report enables you to use heuristic and behavior-based mechanisms to identify potential malware- or botnet-infected hosts in your network. To evaluate botnet activity and infected hosts, the firewall correlates user and network activity data in Threat, URL, and Data Filtering logs with the list of malware URLs in PAN-DB, known dynamic DNS domain providers, and domains registered within the last 30 days. You can configure the report to identify hosts that visited those sites, as well as hosts that communicated with Internet Relay Chat (IRC) servers or that used unknown applications. Malware often use dynamic DNS to avoid IP blacklisting, while IRC servers often use bots for automated functions.



The firewall requires Threat Prevention and URL Filtering licenses to use the botnet report. You can [Use the Automated Correlation Engine](#) to monitor suspicious activities based on additional indicators besides those that the botnet report uses. However, the botnet report is the only tool that uses newly registered domains as an indicator.

- ▲ [Configure a Botnet Report](#)
- ▲ [Interpret Botnet Report Output](#)

### Configure a Botnet Report

You can schedule a botnet report or run it on demand. The firewall generates scheduled botnet reports every 24 hours because behavior-based detection requires correlating traffic across multiple logs over that timeframe.

#### Configure a Botnet Report

**Step 1** Define the types of traffic that indicate possible botnet activity.

1. Select **Monitor > Botnet** and click **Configuration** on the right side of the page.
2. **Enable** and define the **Count** for each type of HTTP Traffic that the report will include. The **Count** values represent the minimum number of events of each traffic type that must occur for the report to list the associated host with a higher confidence score (higher likelihood of botnet infection). If the number of events is less than the **Count**, the report will display a lower confidence score or (for certain traffic types) won't display an entry for the host. For example, if you set the **Count** to three for **Malware URL visit**, then hosts that visit three or more known malware URLs will have higher scores than hosts that visit less than three. For details, see [Interpret Botnet Report Output](#).
3. Define the thresholds that determine whether the report will include hosts associated with traffic involving Unknown TCP or Unknown UDP applications.
4. Select the **IRC** check box to include traffic involving IRC servers.
5. Click **OK** to save the report configuration.

### Configure a Botnet Report (Continued)

Step 2 Schedule the report or run it on demand.

1. Click **Report Setting** on the right side of the page.
2. Select a time interval for the report in the **Test Run Time Frame** drop-down.
3. Select the **No. of Rows** to include in the report.
4. (Optional) **Add** queries to the Query Builder to filter the report output by attributes such as source/destination IP addresses, users, or zones.  
For example, if you know in advance that traffic initiated from the IP address 10.3.3.15 contains no potential botnet activity, you can add `not (addr.src in 10.0.1.35)` as a query to exclude that host from the report output. For details, see [Interpret Botnet Report Output](#).
5. Select **Scheduled** to run the report daily or click **Run Now** to run the report immediately.
6. Click **OK** and **Commit**.

### Interpret Botnet Report Output

The botnet report displays a line for each host that is associated with traffic you defined as suspicious when configuring the report. For each host, the report displays a confidence score of 1 to 5 to indicate the likelihood of botnet infection, where 5 indicates the highest likelihood. The scores correspond to threat severity levels: 1 is informational, 2 is low, 3 is medium, 4 is high, and 5 is critical. The firewall bases the scores on:

- **Traffic type**—Certain HTTP traffic types are more likely to involve botnet activity. For example, the report assigns a higher confidence to hosts that visit known malware URLs than to hosts that browse to IP domains instead of URLs, assuming you defined both those activities as suspicious.
- **Number of events**—Hosts that are associated with a higher number of suspicious events will have higher confidence scores based on the thresholds (**Count** values) you define when you [Configure a Botnet Report](#).
- **Executable downloads**—The report assigns a higher confidence to hosts that download executable files. Executable files are a part of many infections and, when combined with the other types of suspicious traffic, can help you prioritize your investigations of compromised hosts.

When reviewing the report output, you might find that the sources the firewall uses to evaluate botnet activity (for example, the list of malware URLs in PAN-DB) have gaps. You might also find that these sources identify traffic that you consider safe. To compensate in both cases, you can add query filters when you [Configure a Botnet Report](#).

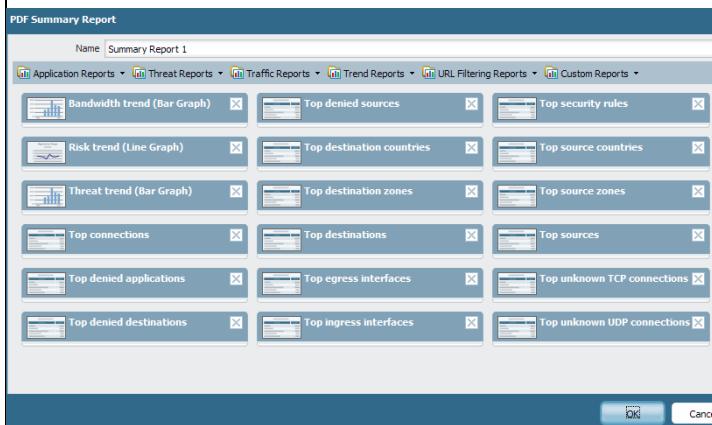
## Manage PDF Summary Reports

PDF summary reports contain information compiled from existing reports, based on data for the top 5 in each category (instead of top 50). They also contain trend charts that are not available in other reports.

### Generate PDF Summary Reports

#### Step 1 Set up a **PDF Summary Report**.

1. Select **Monitor > PDF Reports > Manage PDF Summary**.
2. Click **Add** and then enter a **Name** for the report.
3. Use the drop-down for each report group and select one or more of the elements to design the PDF Summary Report. You can include a maximum of 18 report elements.

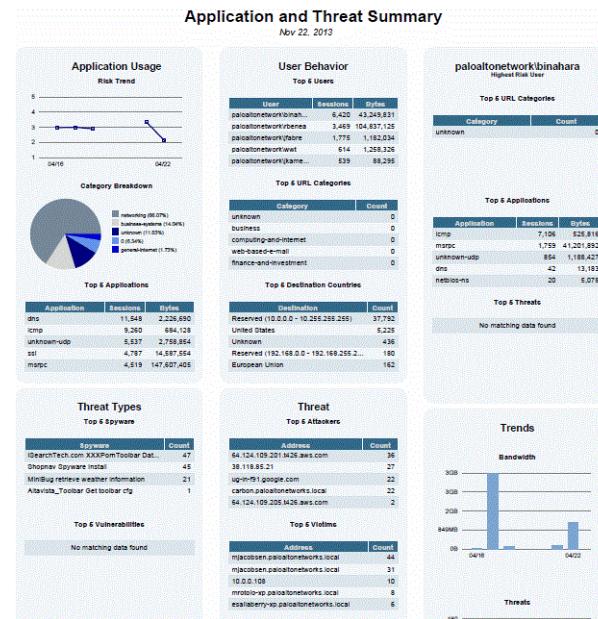


- To remove an element from the report, click the **X** icon or clear the selection from the drop-down for the appropriate report group.
  - To rearrange the reports, drag and drop the icons to another area of the report.
4. Click **OK** to save the report.
  5. **Commit** the changes.

## Generate PDF Summary Reports

**Step 2** View the report.

To download and view the PDF Summary Report, see [View Reports](#).



## Generate User/Group Activity Reports

User/Group Activity reports summarize the web activity of individual users or user groups. Both reports include the same information except for the **Browsing Summary by URL Category** and **Browse time calculations**, which only the User Activity report includes.

You must configure [User-ID](#) on the firewall to access the list of users and user groups.

Generate User/Group Activity Reports	
<p><b>Step 1</b> Configure the browse times and number of logs for User/Group Activity reports. Required only if you want to change the default values.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Management</b>, edit the Logging and Reporting Settings, and select the <b>Log Export and Reporting</b> tab.</li><li>2. For the <b>Max Rows in User Activity Report</b>, enter the maximum number of rows that the detailed user activity report supports (range is 1-1048576, default is 5000). This determines the number of logs that the report analyzes.</li><li>3. Enter the <b>Average Browse Time</b> in seconds that you estimate users should take to browse a web page (range is 0-300, default is 60). Any request made after the average browse time elapses is considered a new browsing activity. The calculation uses <a href="#">Container Pages</a> (logged in the URL Filtering logs) as the basis and ignores any new web pages that are loaded between the time of the first request (start time) and the average browse time. For example, if you set the <b>Average Browse Time</b> to two minutes and a user opens a web page and views that page for five minutes, the browse time for that page will still be two minutes. This is done because the firewall can't determine how long a user views a given page. The average browse time calculation ignores sites categorized as web advertisements and content delivery networks.</li><li>4. For the <b>Page Load Threshold</b>, enter the estimated time in seconds for page elements to load on the page (default is 20). Any requests that occur between the first page load and the page load threshold are assumed to be elements of the page. Any requests that occur outside of the page load threshold are assumed to be the user clicking a link within the page.</li><li>5. Click <b>OK</b> to save your changes.</li></ol>

**Generate User/Group Activity Reports (Continued)**

<b>Step 2</b> Generate the User/Group Activity report.	<ol style="list-style-type: none"><li>1. Select <b>Monitor &gt; PDF Reports &gt; User Activity Report</b>.</li><li>2. Click <b>Add</b> and then enter a <b>Name</b> for the report.</li><li>3. Create the report:<ul style="list-style-type: none"><li>• User Activity Report—Select <b>User</b> and enter the <b>Username</b> or <b>IP address</b> (IPv4 or IPv6) of the user.</li><li>• Group Activity Report—Select <b>Group</b> and select the <b>Group Name</b> of the user group.</li></ul></li><li>4. Select the <b>Time Period</b> for the report.</li><li>5. Optionally, select the <b>Include Detailed Browsing</b> check box (default is cleared) to include detailed URL logs in the report. The detailed browsing information can include a large volume of logs (thousands of logs) for the selected user or user group and can make the report very large.</li><li>6. To run the report on demand, click <b>Run Now</b>.</li><li>7. To save the report configuration, click <b>OK</b>. You can't save the output of User/Group Activity reports on the firewall. To schedule the report for email delivery, see <a href="#">Schedule Reports for Email Delivery</a>.</li></ol>
--	---

## Manage Report Groups

Report groups allow you to create sets of reports that the system can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

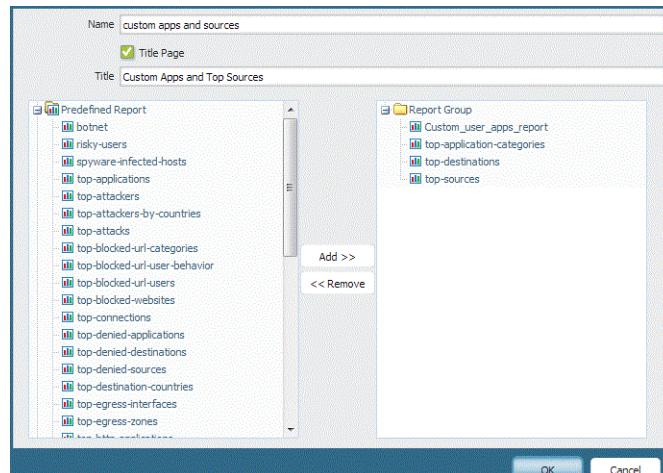
### Set up Report Groups

#### Step 1 Set up report groups.



You must set up a **Report Group** to email report(s).

1. [Create an Email server profile](#).
2. Define the **Report Group**. A report group can compile predefined reports, PDF Summary reports, custom reports, and Log View report into a single PDF.
  - a. Select **Monitor > Report Group**.
  - b. Click **Add** and then enter a **Name** for the report group.
  - c. (Optional) Select **Title Page** and add a **Title** for the PDF output.
  - d. Select reports from the left column and click **Add** to move each report to the report group on the right.



The **Log View** report is a report type that is automatically created each time you create a custom report and uses the same name as the custom report. This report will show the logs that were used to build the contents of the custom report.

To include the log view data, when creating a report group, add your custom report under the **Custom Reports** list and then add the log view report by selecting the matching report name from the **Log View** list. The report will include the custom report data and the log data that was used to create the custom report.

- e. Click **OK** to save the settings.
- f. To use the report group, see [Schedule Reports for Email Delivery](#).

## Schedule Reports for Email Delivery

Reports can be scheduled for daily delivery or delivered weekly on a specified day. Scheduled reports are executed starting at 2:00 AM, and email delivery starts after all scheduled reports have been generated.

### Schedule Reports for Email Delivery

- Step 1 Select **Monitor > PDF Reports > Email Scheduler** and click **Add**.
- Step 2 Enter a **Name** to identify the schedule.
- Step 3 Select the **Report Group** for email delivery. To set up a report group; see [Manage Report Groups](#).
- Step 4 For the **Email Profile**, select an Email Server profile to use for delivering the reports, or click the **Email Profile** link to [Create an Email server profile](#).
- Step 5 Select the frequency at which to generate and send the report in **Recurrence**.
- Step 6 The **Override Recipient email(s)** allows you to send this report exclusively to the recipients specified in this field. When you add recipients to the field, the report is not sent to the recipients configured in the email server profile. Use this option for those occasions when the report is for the attention of someone other than the administrators or recipients defined in the email server profile.



## Use External Services for Monitoring

Using an external service to monitor the firewall enables you to receive alerts for important events, archive monitored information on systems with dedicated long-term storage, and integrate with third-party security monitoring tools. The following are some common scenarios for using external services:

- For immediate notification about important system events or threats, you can [Monitor Device Statistics Using SNMP](#), [Forward Traps to an SNMP Manager](#), or [Configure Email Alerts](#).
- For long-term log storage and centralized firewall monitoring, you can [Configure Syslog Monitoring](#) to send log data to a syslog server. This enables integration with third-party security monitoring tools such as Splunk! or ArcSight.
- For monitoring statistics on the IP traffic that traverses firewall interfaces, you can [Configure NetFlow Exports](#) to view the statistics in a NetFlow collector.

You can [Configure Log Forwarding](#) from the firewalls directly to external services or from the firewalls to Panorama and then [configure Panorama to forward logs to the servers](#). Refer to [Log Forwarding Options](#) for the factors to consider when deciding where to forward logs.



You can't aggregate NetFlow records on Panorama; you must send them directly from the firewalls to a NetFlow collector.

# Configure Log Forwarding

To use Panorama or [Use External Services for Monitoring](#) the firewall, you must configure the firewall to forward its logs. Before forwarding to external services, the firewall automatically converts the logs to the necessary format: syslog messages, SNMP traps, or email notifications. Before starting this procedure, ensure that Panorama or the external server that will receive the log data is already set up.



The PA-7000 Series firewall can't forward logs to Panorama, only to external services. However, when you use Panorama to monitor logs or generate reports for a device group that includes a PA-7000 Series firewall, Panorama queries the PA-7000 Series firewall in real-time to display its log data.

You can forward logs from the firewalls directly to external services or from the firewalls to Panorama and then [configure Panorama to forward logs to the servers](#). Refer to [Log Forwarding Options](#) for the factors to consider when deciding where to forward logs.

You can [use Secure Copy \(SCP\) commands from the CLI](#) to export the entire log database to an SCP server and import it to another firewall. Because the log database is too large for an export or import to be practical on the PA-7000 Series firewall, it does not support these options. You can also use the web interface on all platforms to [Schedule Log Exports to an SCP or FTP Server](#), but only on a per log type basis, not the entire log database.

## Configure Log Forwarding

<p><b>Step 1</b> Configure a server profile for each external service that will receive log data.</p> <p> You can use separate profiles to send each log type to a different server. To increase availability, define multiple servers in a single profile.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Create an Email server profile</a>.</li> <li>• <a href="#">Configure an SNMP Trap server profile</a>. To enable the SNMP manager (trap server) to interpret firewall traps, you must load the Palo Alto Networks <a href="#">Supported MIBs</a> into the SNMP manager and, if necessary, compile them. For details, refer to your SNMP management software documentation.</li> <li>• <a href="#">Configure a Syslog server profile</a>. If the syslog server requires client authentication, you must also <a href="#">Create a certificate to secure syslog communication over SSL</a>.</li> </ul>
<p><b>Step 2</b> Create a log forwarding profile.</p> <p>The profile defines the destinations for Traffic, Threat, and WildFire Submission logs. (Threat logs include URL Filtering and Data Filtering logs.)</p>	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Log Forwarding</b> and click <b>Add</b>.</li> <li>2. Enter a <b>Name</b> to identify the profile. If you want the firewall to automatically assign the profile to new security rules and zones, enter <b>default</b>. If you don't want a default profile, or you want to override an existing default profile, enter a <b>Name</b> that will help you identify the profile when assigning it to security rules and zones.       <p> If no log forwarding profile named <b>default</b> exists, the profile selection is set to <b>None</b> by default in new security rules (<b>Log Forwarding</b> field) and new security zones (<b>Log Setting</b> field), although you can change the selection.</p> </li> <li>3. Perform the following steps for each log type and each severity level or WildFire verdict:       <ol style="list-style-type: none"> <li>a. Select the <b>Panorama</b> check box if you want to aggregate firewall logs on Panorama. (You can then <a href="#">configure Panorama to forward the logs</a> to external services.)</li> <li>b. Select the <b>SNMP Trap</b>, <b>Email</b>, or <b>Syslog</b> server profile you configured for this log type, and click <b>OK</b>.</li> </ol> </li> </ol>

<b>Configure Log Forwarding (Continued)</b>	
<b>Step 3</b> Assign the log forwarding profile to security rules.	<p>To trigger log generation and forwarding, the rules require certain <a href="#">Security Profiles</a> according to log type:</p> <ul style="list-style-type: none"> <li>Traffic logs—No security profile is necessary; the traffic only needs to match a specific security rule.</li> <li>Threat logs—The traffic must match any security profile assigned to a security rule.</li> <li>WildFire logs—The traffic must match a <a href="#">WildFire Analysis profile</a> assigned to a security rule.</li> </ul>
<b>Step 4</b> Configure the destinations of System, Config, HIP Match, and Correlation logs.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and click the rule.</li> <li>Select the <b>Actions</b> tab and select the <b>Log Forwarding</b> profile you just created.</li> <li>In the <b>Profile Type</b> drop-down, select <b>Profiles</b> or <b>Group</b>, and then select the security profiles or <b>Group Profile</b> required to trigger log generation and forwarding.</li> <li>For Traffic logs, select one or both of the <b>Log At Session Start</b> and <b>Log At Session End</b> check boxes, and click <b>OK</b>.</li> </ol>
<b>Step 5</b> (PA-7000 Series firewalls only) Configure a log card interface to perform log forwarding.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Log Settings</b>.</li> <li>Perform the following steps for each log type. For System and Correlation logs, start by clicking the Severity level. For Config and HIP Match logs, start by clicking the Edit icon. <ol style="list-style-type: none"> <li>Select the <b>Panorama</b> check box if you want to aggregate firewall logs on Panorama. You can then <a href="#">configure Panorama to forward the logs</a> to the external services.</li> <li>Select the <b>SNMP Trap</b>, <b>Email</b>, or <b>Syslog</b> server profile you configured for this log type and click <b>OK</b>.</li> </ol> </li> <li>Select <b>Network &gt; Interfaces &gt; Ethernet</b> and click <b>Add Interface</b>.</li> <li>Select the <b>Slot</b> and <b>Interface Name</b>.</li> <li>For the <b>Interface Type</b>, select <b>Log Card</b>.</li> <li>Enter the <b>IP Address</b>, <b>Default Gateway</b>, and (for IPv4 only) <b>Netmask</b>.</li> <li>Select <b>Advanced</b> and specify the <b>Link Speed</b>, <b>Link Duplex</b>, and <b>Link State</b>.  These fields default to <b>auto</b>, which specifies that the firewall automatically determines the values based on the connection. However, the minimum recommended <b>Link Speed</b> for any connection is <b>1000</b> (Mbps).</li> <li>Click <b>OK</b> to save your changes.</li> </ol>

**Configure Log Forwarding (Continued)**

Step 6 Commit and verify your changes.	<ol style="list-style-type: none"><li>1. Click <b>Commit</b> to complete the log forwarding configuration.</li><li>2. Verify the log destinations you configured are receiving firewall logs:<ul style="list-style-type: none"><li>• Panorama—if the firewall forwards logs to an M-Series appliance, you must <a href="#">configure a Collector Group</a> before Panorama will receive the logs. You can then <a href="#">verify log forwarding</a>.</li><li>• Email server—Verify that the specified recipients are receiving logs as email notifications.</li><li>• Syslog server—Refer to the documentation for your syslog server to verify it is receiving logs as syslog messages.</li><li>• SNMP manager—<a href="#">Use an SNMP Manager to Explore MIBs and Objects</a> to verify it is receiving logs as SNMP traps.</li></ul></li></ol>
--	--

# Configure Email Alerts

You can configure email alerts for System, Config, HIP Match, Correlation, Threat, WildFire Submission, and Traffic logs.

<b>Configure Email Alerts</b>	
<b>Step 1</b> Create an Email server profile.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Server Profiles &gt; Email</b>.</li> <li>Click <b>Add</b> and then enter a <b>Name</b> for the profile.</li> <li>If the firewall has more than one virtual system (vsys), select the <b>Location</b> (vsys or <b>Shared</b>) where this profile is available.</li> <li>For each Simple Mail Transport Protocol (SMTP) server (email server), click <b>Add</b> and define the following information:           <ul style="list-style-type: none"> <li><b>Name</b>—Name to identify the SMTP server (1-31 characters). This field is just a label and doesn't have to be the hostname of an existing email server.</li> <li><b>Email Display Name</b>—The name to show in the From field of the email.</li> <li><b>From</b>—The email address from which the Palo Alto Networks device sends emails.</li> <li><b>To</b>—The email address to which the Palo Alto Networks device sends emails.</li> <li><b>Additional Recipient</b>—If you want to send emails to a second account, enter the address here. You can add only one additional recipient. For multiple recipients, add the email address of a distribution list.</li> <li><b>Email Gateway</b>—The IP address or hostname of the SMTP gateway to use for sending emails.</li> </ul> </li> <li>(Optional) Select the <b>Custom Log Format</b> tab and customize the format of the email messages. For details on how to create custom formats for the various log types, refer to the <a href="#">Common Event Format Configuration Guide</a>.</li> <li>Click <b>OK</b> to save the Email server profile.</li> </ol>
<b>Step 2</b> Configure email alerts for Traffic, Threat, and WildFire Submission logs.	<ol style="list-style-type: none"> <li><a href="#">Create a log forwarding profile.</a> <ol style="list-style-type: none"> <li>Select <b>Objects &gt; Log Forwarding</b>, click <b>Add</b>, and enter a <b>Name</b> to identify the profile.</li> <li>For each log type and each severity level or WildFire verdict, select the Email server profile and click <b>OK</b>.</li> </ol> </li> <li><a href="#">Assign the log forwarding profile to security rules.</a></li> </ol>
<b>Step 3</b> Configure email alerts for System, Config, HIP Match, and Correlation logs.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Log Settings</b>.</li> <li>For System and Correlation logs, click each Severity level, select the <b>Email</b> server profile, and click <b>OK</b>.</li> <li>For Config and HIP Match logs, click the Edit icon, select the <b>Email</b> server profile, and click <b>OK</b>.</li> <li>Click <b>Commit</b>.</li> </ol>

## Use Syslog for Monitoring

Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices—such as routers, firewalls, printers—from different vendors into a central repository for archiving, analysis, and reporting. Palo Alto Networks devices can forward every type of log they generate to an external syslog server. You can use TCP or SSL for reliable and secure log forwarding, or UDP for non-secure forwarding.

- ▲ [Configure Syslog Monitoring](#)
- ▲ [Syslog Field Descriptions](#)

## Configure Syslog Monitoring

To [Use Syslog for Monitoring](#) a Palo Alto Networks device, create a Syslog server profile and assign it to the device log settings for each log type. Optionally, you can configure the header format used in syslog messages and enable client authentication for syslog over SSL.

<b>Configure Syslog Monitoring</b>	
<b>Step 1</b> Configure a Syslog server profile.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Server Profiles &gt; Syslog</b>.</li> <li>Click <b>Add</b> and enter a <b>Name</b> for the profile.</li> <li>If the firewall has more than one virtual system (vsys), select the <b>Location</b> (vsys or <b>Shared</b>) where this profile is available.</li> <li>For each syslog server, click <b>Add</b> and enter the information that the firewall requires to connect to it:           <ul style="list-style-type: none"> <li><b>Name</b>—Unique name for the server profile.</li> <li><b>Server</b>—IP address or fully qualified domain name (FQDN) of the syslog server.</li> <li><b>Transport</b>—Select TCP, UDP, or SSL as the method of communication with the syslog server.</li> <li><b>Port</b>—The port number on which to send syslog messages (default is UDP on port 514); you must use the same port number on the firewall and the syslog server.</li> <li><b>Format</b>—Select the syslog message format to use: <b>BSD</b> (the default) or <b>IETF</b>. Traditionally, <b>BSD</b> format is over UDP and <b>IETF</b> format is over TCP or SSL.</li> <li><b>Facility</b>—Select a syslog standard value (default is <b>LOG_USER</b>) to calculate the priority (PRI) field in your syslog server implementation. Select the value that maps to how you use the PRI field to manage your syslog messages.</li> </ul> </li> <li>(Optional) To customize the format of the syslog messages that the firewall sends, select the <b>Custom Log Format</b> tab. For details on how to create custom formats for the various log types, refer to the <a href="#">Common Event Format Configuration Guide</a>.</li> <li>Click <b>OK</b> to save the server profile.</li> </ol>
<b>Step 2</b> Configure syslog forwarding for Traffic, Threat, and WildFire Submission logs.	<ol style="list-style-type: none"> <li><a href="#">Create a log forwarding profile.</a> <ol style="list-style-type: none"> <li>Select <b>Objects &gt; Log Forwarding</b>, click <b>Add</b>, and enter a <b>Name</b> to identify the profile.</li> <li>For each log type and each severity level or WildFire verdict, select the <b>Syslog</b> server profile and click <b>OK</b>.</li> </ol> </li> <li><a href="#">Assign the log forwarding profile to security rules.</a></li> </ol>

<b>Configure Syslog Monitoring (Continued)</b>	
<b>Step 3</b> Configure syslog forwarding for System, Config, HIP Match, and Correlation logs.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Log Settings</b>.</li> <li>For System and Correlation logs, click each Severity level, select the <b>Syslog</b> server profile, and click <b>OK</b>.</li> <li>For Config, HIP Match, and Correlation logs, click the Edit icon, select the <b>Syslog</b> server profile, and click <b>OK</b>.</li> </ol>
<b>Step 4</b> (Optional) Configure the header format of syslog messages.  The log data includes the unique identifier of the device that generated the log. Choosing the header format provides more flexibility in filtering and reporting on the log data for some Security Information and Event Management (SIEM) servers.  This is a global setting and applies to all syslog server profiles configured on the device.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; Management</b> and edit the Logging and Reporting Settings.</li> <li>Select the <b>Log Export and Reporting</b> tab and select the <b>Syslog HOSTNAME Format</b>: <ul style="list-style-type: none"> <li>• <b>FQDN</b> (default)—Concatenates the hostname and domain name defined on the sending device.</li> <li>• <b>hostname</b>—Uses the hostname defined on the sending device.</li> <li>• <b>ipv4-address</b>—Uses the IPv4 address of the device interface used to send logs. By default, this is the MGT interface.</li> <li>• <b>ipv6-address</b>—Uses the IPv6 address of the device interface used to send logs. By default, this is the MGT interface.</li> <li>• <b>none</b>—Leaves the hostname field unconfigured on the device. There is no identifier for the device that sent the logs.</li> </ul> </li> <li>Click <b>OK</b> to save your changes.</li> </ol>
<b>Step 5</b> Create a certificate to secure syslog communication over SSL.  Required only if the syslog server uses client authentication. The syslog server uses the certificate to verify that the device is authorized to communicate with the syslog server.  Ensure the following conditions are met: <ul style="list-style-type: none"> <li>• The private key must be available on the sending device; the keys can't reside on a Hardware Security Module (HSM).</li> <li>• The subject and the issuer for the certificate must not be identical.</li> <li>• The syslog server and the sending device must have certificates that the same trusted certificate authority (CA) signed. Alternatively, you can generate a self-signed certificate on the device, export the certificate from the device, and import it in to the syslog server.</li> </ul>	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Generate</b>.</li> <li>Enter a <b>Name</b> for the certificate.</li> <li>In the <b>Common Name</b> field, enter the IP address of the device sending logs to the syslog server.</li> <li>In <b>Signed by</b>, select the trusted CA or the self-signed CA that the syslog server and the sending device both trust. The certificate can't be a <b>Certificate Authority</b> nor an <b>External Authority</b> (certificate signing request [CSR]).</li> <li>Click <b>Generate</b>. The device generates the certificate and key pair.</li> <li>Click the certificate Name to edit it, select the <b>Certificate for Secure Syslog</b> check box, and click <b>OK</b>.</li> </ol>

**Configure Syslog Monitoring (Continued)**

**Step 6** Commit your changes and review the logs on the syslog server.

1. Click **Commit**.
2. To review the logs, refer to the documentation of your syslog management software. You can also review the [Syslog Field Descriptions](#).

## Syslog Field Descriptions

The following topics list the standard fields of each log type that Palo Alto Networks devices can forward to an external server, as well as the severity levels, custom formats, and escape sequences. To facilitate parsing, the delimiter is a comma: each field is a comma-separated value (CSV) string. The FUTURE\_USE tag applies to fields that the devices do not currently implement.



WildFire Submission logs are a subtype of Threat log and use the same syslog format.

- ▲ [Traffic Logs](#)
- ▲ [Threat Logs](#)
- ▲ [HIP Match Logs](#)
- ▲ [Config Logs](#)
- ▲ [System Logs](#)
- ▲ [Correlated Events \(Logs\)](#)
- ▲ [Syslog Severity](#)
- ▲ [Custom Log/Event Format](#)
- ▲ [Escape Sequences](#)

### Traffic Logs

**Format:** FUTURE\_USE, Receive Time, Serial Number, Type, Subtype, FUTURE\_USE, Generated Time, Source IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Ingress Interface, Egress Interface, Log Forwarding Profile, FUTURE\_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Bytes, Bytes Sent, Bytes Received, Packets, Start Time, Elapsed Time, Category, FUTURE\_USE, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE\_USE, Packets Sent, Packets Received, Session End Reason, Device Group Hierarchy Level 1\*, Device Group Hierarchy Level 2\*, Device Group Hierarchy Level 3\*, Device Group Hierarchy Level 4\*, Virtual System Name\*, Device Name\*, Action Source\*

Field Name	Description
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; values are traffic, threat, config, system and hip-match

Field Name	Description
Subtype (subtype)	Subtype of traffic log; values are start, end, drop, and deny <ul style="list-style-type: none"> <li>Start—session started</li> <li>End—session ended</li> <li>Drop—session dropped before the application is identified and there is no rule that allows the session.</li> <li>Deny—session dropped after the application is identified and there is a rule to block or no rule that allows the session.</li> </ul>
Generated Time (time_generated)	Time the log was generated on the dataplane
Source IP (src)	Original session source IP address
Destination IP (dst)	Original session destination IP address
NAT Source IP (natsrc)	If Source NAT performed, the post-NAT Source IP address
NAT Destination IP (natdst)	If Destination NAT performed, the post-NAT Destination IP address
Rule Name (rule)	Name of the rule that the session matched
Source User (srcuser)	Username of the user who initiated the session
Destination User (dstuser)	Username of the user to which the session was destined
Application (app)	Application associated with the session
Virtual System (vsys)	Virtual System associated with the session
Source Zone (from)	Zone the session was sourced from
Destination Zone (to)	Zone the session was destined to
Ingress Interface (inbound_if)	Interface that the session was sourced from
Egress Interface (outbound_if)	Interface that the session was destined to
Log Forwarding Profile (logset)	Log Forwarding Profile that was applied to the session
Session ID (sessionid)	An internal numerical identifier applied to each session
Repeat Count (repeatcnt)	Number of sessions with same Source IP, Destination IP, Application, and Subtype seen within 5 seconds; used for ICMP only
Source Port (sport)	Source port utilized by the session
Destination Port (dport)	Destination port utilized by the session
NAT Source Port (natsport)	Post-NAT source port
NAT Destination Port (natdport)	Post-NAT destination port

Field Name	Description
Flags (flags)	<p>32-bit field that provides details on session; this field can be decoded by AND-ing the values with the logged value:</p> <ul style="list-style-type: none"> <li>• 0x80000000—session has a packet capture (PCAP)</li> <li>• 0x02000000—IPv6 session</li> <li>• 0x01000000—SSL session was decrypted (SSL Proxy)</li> <li>• 0x00800000—session was denied via URL filtering</li> <li>• 0x00400000—session has a NAT translation performed (NAT)</li> <li>• 0x00200000—user information for the session was captured via the captive portal (Captive Portal)</li> <li>• 0x00080000—X-Forwarded-For value from a proxy is in the source user field</li> <li>• 0x00040000—log corresponds to a transaction within a http proxy session (Proxy Transaction)</li> <li>• 0x00008000—session is a container page access (Container Page)</li> <li>• 0x00002000—session has a temporary match on a rule for implicit application dependency handling. Available in PAN-OS 5.0.0 and above.</li> <li>• 0x00000800—symmetric return was used to forward traffic for this session</li> </ul>
Protocol (proto)	IP protocol associated with the session
Action (action)	<p>Action taken for the session; possible values are:</p> <ul style="list-style-type: none"> <li>• Allow—session was allowed by policy</li> <li>• Deny—session was denied by policy</li> <li>• Drop—session was dropped silently</li> <li>• Drop ICMP—session was silently dropped with an ICMP unreachable message to the host or application</li> <li>• Reset both—session was terminated and a TCP reset is sent to both the sides of the connection</li> <li>• Reset client—session was terminated and a TCP reset is sent to the client</li> <li>• Reset server—session was terminated and a TCP reset is sent to the server</li> </ul>
Bytes (bytes)	Number of total bytes (transmit and receive) for the session
Bytes Sent (bytes_sent)	<p>Number of bytes in the client-to-server direction of the session Available on all models except the PA-4000 Series</p>
Bytes Received (bytes_received)	<p>Number of bytes in the server-to-client direction of the session Available on all models except the PA-4000 Series</p>
Packets (packets)	Number of total packets (transmit and receive) for the session
Start Time (start)	Time of session start
Elapsed Time (elapsed)	Elapsed time of the session
Category (category)	URL category associated with the session (if applicable)

Field Name	Description
Sequence Number (seqno)	A 64-bit log entry identifier incremented sequentially; each log type has a unique number space. This field is not supported on PA-7000 Series firewalls.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama
Source Location (srcloc)	Source country or Internal region for private addresses; maximum length is 32 bytes
Destination Location (dstloc)	Destination country or Internal region for private addresses. Maximum length is 32 bytes
Packets Sent (pkts_sent)	Number of client-to-server packets for the session Available on all models except the PA-4000 Series
Packets Received (pkts_received)	Number of server-to-client packets for the session Available on all models except the PA-4000 Series
Session End Reason (session_end_reason)	The reason a session terminated. If the termination had multiple causes, this field displays only the highest priority reason. The possible session end reason values are as follows, in order of priority (where the first is highest): <ul style="list-style-type: none"> <li>• threat—The firewall detected a threat associated with a reset, drop, or block (IP address) action.</li> <li>• policy-deny—The session matched a security rule with a deny or drop action.</li> <li>• tcp-rst-from-client—The client sent a TCP reset to the server.</li> <li>• tcp-rst-from-server—The server sent a TCP reset to the client.</li> <li>• resources-unavailable—The session dropped because of a system resource limitation. For example, the session could have exceeded the number of out-of-order packets allowed per flow or the global out-of-order packet queue.</li> <li>• tcp-fin—One host or both hosts in the connection sent a TCP FIN message to close the session.</li> <li>• tcp-reuse—A session is reused and the firewall closes the previous session.</li> <li>• decoder—The decoder detects a new connection within the protocol (such as HTTP-Proxy) and ends the previous connection.</li> <li>• aged-out—The session aged out.</li> <li>• unknown—This value applies in the following situations: <ul style="list-style-type: none"> <li>• Session terminations that the preceding reasons do not cover (for example, a <code>clear session all</code> command).</li> <li>• For logs generated in a PAN-OS release that does not support the session end reason field (releases older than PAN-OS 6.1), the value will be <code>unknown</code> after an upgrade to the current PAN-OS release or after the logs are loaded onto the firewall.</li> <li>• In Panorama, logs received from firewalls for which the PAN-OS version does not support session end reasons will have a value of <code>unknown</code>.</li> </ul> </li> <li>• n/a—This value applies when the traffic log type is not <code>end</code>.</li> </ul>

Field Name	Description
Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)  New in v7.0!	<p>A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure.</p> <p>If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods:</p>
	<p>CLI command in configure mode: <b>show readonly dg-meta-data</b></p> <p>API query:  <code>/api/?type=op&amp;cmd=&lt;show&gt;&lt;dg-hierarchy&gt;&lt;/dg-hierarchy&gt;&lt;/show&gt;</code></p>
Virtual System Name (vsys_name)  New in v7.0!	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.
Device Name (device_name)  New in v7.0!	The hostname of the firewall on which the session was logged.
Action Source (action_source)  New in v7.0!	Specifies whether the action taken to allow or block an application was defined in the application or in policy. The actions can be allow, deny, drop, reset-server, reset-client or reset-both for the session.

## Threat Logs

**Format:** FUTURE\_USE, Receive Time, Serial Number, Type, Subtype, FUTURE\_USE, Generated Time, Source IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Ingress Interface, Egress Interface, Log Forwarding Profile, FUTURE\_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Miscellaneous, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE\_USE, Content Type, PCAP\_id, Filedigest, Cloud, URL Index\*, User Agent, File Type, X-Forwarded-For, Referer, Sender, Subject, Recipient, Report ID, Device Group Hierarchy Level 1\*, Device Group Hierarchy Level 2\*, Device Group Hierarchy Level 3\*, Device Group Hierarchy Level 4\*, Virtual System Name\*, Device Name\*, FUTURE\_USE,

Field Name	Description
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Specifies type of log; values are traffic, threat, config, system and hip-match
Subtype (subtype)	<p>Subtype of threat log. Values include the following:</p> <ul style="list-style-type: none"> <li>• data—Data pattern matching a Data Filtering profile.</li> <li>• file—File type matching a File Blocking profile.</li> <li>• flood—Flood detected via a Zone Protection profile.</li> <li>• packet—Packet-based attack protection triggered by a Zone Protection profile.</li> <li>• scan—Scan detected via a Zone Protection profile.</li> <li>• spyware—Spyware detected via an Anti-Spyware profile.</li> <li>• url—URL filtering log.</li> <li>• virus—Virus detected via an Antivirus profile.</li> <li>• vulnerability—Vulnerability exploit detected via a Vulnerability Protection profile.</li> <li>• wildfire—A WildFire verdict generated when the firewall submits a file to WildFire per a WildFire Analysis profile and a verdict (malicious, grayware, or benign, depending on what you are logging) is logged in the WildFire Submissions log.</li> <li>• wildfire-virus—Virus detected via an Antivirus profile.</li> </ul>
Generated Time (time_generated)	Time the log was generated on the dataplane
Source IP (src)	Original session source IP address
Destination IP (dst)	Original session destination IP address
NAT Source IP (natsrc)	If source NAT performed, the post-NAT source IP address
NAT Destination IP (natdst)	If destination NAT performed, the post-NAT destination IP address
Rule Name (rule)	Name of the rule that the session matched
Source User (srcuser)	Username of the user who initiated the session

Field Name	Description
Destination User (dstuser)	Username of the user to which the session was destined
Application (app)	Application associated with the session
Virtual System (vsys)	Virtual System associated with the session
Source Zone (from)	Zone the session was sourced from
Destination Zone (to)	Zone the session was destined to
Ingress Interface (inbound_if)	Interface that the session was sourced from
Egress Interface (outbound_if)	Interface that the session was destined to
Log Forwarding Profile (logset)	Log Forwarding Profile that was applied to the session
Session ID (sessionid)	An internal numerical identifier applied to each session
Repeat Count (repeatcnt)	Number of sessions with same Source IP, Destination IP, Application, and Subtype seen within 5 seconds; used for ICMP only
Source Port (sport)	Source port utilized by the session
Destination Port (dport)	Destination port utilized by the session
NAT Source Port (natsport)	Post-NAT source port
NAT Destination Port (natdport)	Post-NAT destination port
Flags (flags)	<p>32-bit field that provides details on session; this field can be decoded by AND-ing the values with the logged value:</p> <ul style="list-style-type: none"> <li>• 0x80000000—session has a packet capture (PCAP)</li> <li>• 0x02000000—IPv6 session</li> <li>• 0x01000000—SSL session was decrypted (SSL Proxy)</li> <li>• 0x00800000—session was denied via URL filtering</li> <li>• 0x00400000—session has a NAT translation performed (NAT)</li> <li>• 0x00200000—user information for the session was captured via the captive portal (Captive Portal)</li> <li>• 0x00080000—X-Forwarded-For value from a proxy is in the source user field</li> <li>• 0x00040000—log corresponds to a transaction within a http proxy session (Proxy Transaction)</li> <li>• 0x00008000—session is a container page access (Container Page)</li> <li>• 0x00002000—session has a temporary match on a rule for implicit application dependency handling. Available in PAN-OS 5.0.0 and above</li> <li>• 0x00000800—symmetric return was used to forward traffic for this session</li> </ul>

Field Name	Description
Protocol (proto)	IP protocol associated with the session
Action (action)	<p>Action taken for the session; values are alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url.</p> <ul style="list-style-type: none"> <li>Alert—threat or URL detected but not blocked</li> <li>Allow—flood detection alert</li> <li>Deny—flood detection mechanism activated and deny traffic based on configuration</li> <li>Drop—threat detected and associated session was dropped</li> <li>Drop-all-packets—threat detected and session remains, but drops all packets</li> <li>Reset-client—threat detected and a TCP RST is sent to the client</li> <li>Reset-server—threat detected and a TCP RST is sent to the server</li> <li>Reset-both—threat detected and a TCP RST is sent to both the client and the server</li> <li>Block-url—URL request was blocked because it matched a URL category that was set to be blocked</li> </ul>
Miscellaneous (misc)	<p>Field with variable length with a maximum of 1023 characters</p> <p>The actual URI when the subtype is URL</p> <p>File name or file type when the subtype is file</p> <p>File name when the subtype is virus</p> <p>File name when the subtype is WildFire</p>
Threat ID (threatid)	<p>Palo Alto Networks identifier for the threat. It is a description string followed by a 64-bit numerical identifier in parentheses for some Subtypes:</p> <ul style="list-style-type: none"> <li>8000 – 8099—scan detection</li> <li>8500 – 8599—flood detection</li> <li>9999—URL filtering log</li> <li>10000 – 19999—spyware phone home detection</li> <li>20000 – 29999—spyware download detection</li> <li>30000 – 44999—vulnerability exploit detection</li> <li>52000 – 52999—filetype detection</li> <li>60000 – 69999—data filtering detection</li> <li>100000 – 2999999—virus detection</li> <li>3000000 – 3999999—WildFire signature feed</li> <li>4000000-4999999—DNS Botnet signatures</li> </ul>
Category (category)	For URL Subtype, it is the URL Category; For WildFire subtype, it is the verdict on the file and is either ‘malicious’, ‘grayware’, or ‘benign’; For other subtypes, the value is ‘any’.
Severity (severity)	Severity associated with the threat; values are informational, low, medium, high, critical

Field Name	Description
Direction (direction)	Indicates the direction of the attack, client-to-server or server-to-client: <ul style="list-style-type: none"><li>• 0—direction of the threat is client to server</li><li>• 1—direction of the threat is server to client</li></ul>
Sequence Number (seqno)	A 64-bit log entry identifier incremented sequentially. Each log type has a unique number space. This field is not supported on PA-7000 Series firewalls.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama.
Source Location (srcloc)	Source country or Internal region for private addresses. Maximum length is 32 bytes.
Destination Location (dstloc)	Destination country or Internal region for private addresses. Maximum length is 32 bytes.
Content Type (contenttype)	Applicable only when Subtype is URL. Content type of the HTTP response data. Maximum length 32 bytes.
PCAP ID (pcap_id)	The packet capture (pcap) ID is a 64 bit unsigned integral denoting an ID to correlate threat pcap files with extended pcaps taken as a part of that flow. All threat logs will contain either a pcap_id of 0 (no associated pcap), or an ID referencing the extended pcap file.
File Digest (filedigest)	Only for WildFire subtype; all other types do not use this field  The filedigest string shows the binary hash of the file sent to be analyzed by the WildFire service.
Cloud (cloud)	Only for WildFire subtype; all other types do not use this field.  The cloud string displays the FQDN of either the WildFire appliance (private) or the WildFire cloud (public) from where the file was uploaded for analysis.
URL Index (url_idx)  <b>New in v7.0!</b>	Used in URL Filtering and WildFire subtypes.  When an application uses TCP keepalives to keep a connection open for a length of time, all the log entries for that session have a single session ID. In such cases, when you have a single threat log (and session ID) that includes multiple URL entries, the url_idx is a counter that allows you to correlate the order of each log entry within the single session.  For example, to learn the URL of a file that the firewall forwarded to WildFire for analysis, locate the session ID and the url_idx from the WildFire Submissions log and search for the same session ID and url_idx in your URL filtering logs. The log entry that matches the session ID and url_idx will contain the URL of the file that was forwarded to WildFire.
User Agent (user_agent)	Only for the URL Filtering subtype; all other types do not use this field.  The User Agent field specifies the web browser that the user used to access the URL, for example Internet Explorer. This information is sent in the HTTP request to the server.
File Type (filetype)	Only for WildFire subtype; all other types do not use this field.  Specifies the type of file that the firewall forwarded for WildFire analysis.

Field Name	Description
X-Forwarded-For (xff)	<p>Only for the URL Filtering subtype; all other types do not use this field.</p> <p>The X-Forwarded-For field in the HTTP header contains the IP address of the user who requested the web page. It allows you to identify the IP address of the user, which is useful particularly if you have a proxy server on your network that replaces the user IP address with its own address in the source IP address field of the packet header.</p>
Referer (referer)	<p>Only for the URL Filtering subtype; all other types do not use this field.</p> <p>The Referer field in the HTTP header contains the URL of the web page that linked the user to another web page; it is the source that redirected (referred) the user to the web page that is being requested.</p>
Sender (sender)	<p>Only for WildFire subtype; all other types do not use this field.</p> <p>Specifies the name of the sender of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.</p>
Subject (subject)	<p>Only for WildFire subtype; all other types do not use this field.</p> <p>Specifies the subject of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.</p>
Recipient (recipient)	<p>Only for WildFire subtype; all other types do not use this field.</p> <p>Specifies the name of the receiver of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.</p>
Report ID (reportid)	<p>Only for WildFire subtype; all other types do not use this field.</p> <p>Identifies the analysis request on the WildFire cloud or the WildFire appliance.</p>
Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)  <span style="color: green;">New in v7.0!</span>	<p>A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure.</p> <p>If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods:</p> <p>CLI command in configure mode: <b>show readonly dg-meta-data</b></p> <p>API query: <code>/api/?type=op&amp;cmd=&lt;show&gt;&lt;dg-hierarchy&gt;&lt;/dg-hierarchy&gt;&lt;/show&gt;</code></p>
Virtual System Name (vsys_name)  <span style="color: green;">New in v7.0!</span>	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.
Device Name (device_name)  <span style="color: green;">New in v7.0!</span>	The hostname of the firewall on which the session was logged.

## HIP Match Logs

**Format:** FUTURE\_USE, Receive Time, Serial Number, Type, Subtype, FUTURE\_USE, Generated Time, Source User, Virtual System, Machine name, OS, Source Address, HIP, Repeat Count, HIP Type, FUTURE\_USE, FUTURE\_USE, Sequence Number, Action Flags, Device Group Hierarchy Level 1\*, Device Group Hierarchy Level 2\*, Device Group Hierarchy Level 3\*, Device Group Hierarchy Level 4\*, Virtual System Name\*, Device Name\*

Field Name	Description
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Type of log; values are traffic, threat, config, system and hip-match
Subtype (subtype)	Subtype of HIP match log; unused
Generated Time (time_generated)	Time the log was generated on the dataplane
Source User (srcuser)	Username of the user who initiated the session
Virtual System (vsys)	Virtual System associated with the HIP match log
Machine Name (machinename)	Name of the user's machine
OS	The operating system installed on the user's machine or device (or on the client system)
Source Address (src)	IP address of the source user
HIP (matchname)	Name of the HIP object or profile
Repeat Count (repeatcnt)	Number of times the HIP profile matched
HIP Type (matchtype)	Whether the hip field represents a HIP object or a HIP profile
Sequence Number (seqno)	A 64-bit log entry identifier incremented sequentially; each log type has a unique number space. This field is not supported on PA-7000 Series firewalls.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama
Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4) <b>New in v7.0!</b>	<p>A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure.</p> <p>If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods:</p> <ul style="list-style-type: none"> <li>CLI command in configure mode: <b>show readonly dg-meta-data</b></li> <li>API query: <code>/api/?type=op&amp;cmd=&lt;show&gt;&lt;dg-hierarchy&gt;&lt;/dg-hierarchy&gt;&lt;/show&gt;</code></li> </ul>

Field Name	Description
Virtual System Name (vsys_name) <b>New in v7.0!</b>	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.
Device Name (device_name) <b>New in v7.0!</b>	The hostname of the firewall on which the session was logged.

## Config Logs

**Format:** FUTURE\_USE, Receive Time, Serial Number, Type, Subtype, FUTURE\_USE, Generated Time, Host, Virtual System, Command, Admin, Client, Result, Configuration Path, Sequence Number, Action Flags, Before Change Detail, After Change Detail, Device Group Hierarchy Level 1\*, Device Group Hierarchy Level 2\*, Device Group Hierarchy Level 3\*, Device Group Hierarchy Level 4\*, Virtual System Name\*, Device Name\*

Field Name	Description
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Type of log; values are traffic, threat, config, system and hip-match
Subtype (subtype)	Subtype of configuration log; unused
Generated Time (time_generated)	Time the log was generated on the dataplane
Host (host)	Hostname or IP address of the client machine
Virtual System (vsys)	Virtual System associated with the configuration log
Command (cmd)	Command performed by the Admin; values are add, clone, commit, delete, edit, move, rename, set.
Admin (admin)	Username of the Administrator performing the configuration
Client (client)	Client used by the Administrator; values are Web and CLI
Result (result)	Result of the configuration action; values are Submitted, Succeeded, Failed, and Unauthorized
Configuration Path (path)	The path of the configuration command issued; up to 512 bytes in length
Sequence Number (seqno)	A 64bit log entry identifier incremented sequentially; each log type has a unique number space. This field is not supported on PA-7000 Series firewalls.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama.
Before Change Detail (before_change_detail)	This field is in custom logs only; it is not in the default format. It contains the full xpath before the configuration change.

Field Name	Description
After Change Detail (after_change_detail)  New in v7.0!	This field is in custom logs only; it is not in the default format. It contains the full xpath after the configuration change.
Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)  New in v7.0!	A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure.  If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods:  CLI command in configure mode: <b>show readonly dg-meta-data</b>  API query: <code>/api/?type=op&amp;cmd=&lt;show&gt;&lt;dg-hierarchy&gt;&lt;/dg-hierarchy&gt;&lt;/sho w&gt;</code>
Virtual System Name (vsys_name)  New in v7.0!	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.
Device Name (device_name)  New in v7.0!	The hostname of the firewall on which the session was logged.

## System Logs

**Format:** FUTURE\_USE, Receive Time, Serial Number, Type, Subtype, FUTURE\_USE, Generated Time, Virtual System, Event ID, Object, FUTURE\_USE, FUTURE\_USE, Module, Severity, Description, Sequence Number, Action Flags, Device Group Hierarchy Level 1\*, Device Group Hierarchy Level 2\*, Device Group Hierarchy Level 3\*, Device Group Hierarchy Level 4\*, Virtual System Name\*, Device Name\*

Field Name	Description
Receive Time (receive_time)	Time the log was received at the management plane
Serial Number (serial)	Serial number of the device that generated the log
Type (type)	Type of log; values are traffic, threat, config, system and hip-match
Subtype (subtype)	Subtype of the system log; refers to the system daemon generating the log; values are crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn
Generated Time (time_generated)	Time the log was generated on the dataplane
Virtual System (vsys)	Virtual System associated with the configuration log
Event ID (eventid)	String showing the name of the event
Object (object)	Name of the object associated with the system event
Module (module)	This field is valid only when the value of the Subtype field is general. It provides additional information about the sub-system generating the log; values are general, management, auth, ha, upgrade, chassis
Severity (severity)	Severity associated with the event; values are informational, low, medium, high, critical
Description (opaque)	Detailed description of the event, up to a maximum of 512 bytes
Sequence Number (seqno)	A 64-bit log entry identifier incremented sequentially; each log type has a unique number space. This field is not supported on PA-7000 Series firewalls.
Action Flags (actionflags)	A bit field indicating if the log was forwarded to Panorama
Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)  New in v7.0!	<p>A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure.</p> <p>If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods:</p> <p>CLI command in configure mode: <b>show readonly dg-meta-data</b></p> <p>API query:  <code>/api/?type=op&amp;cmd=&lt;show&gt;&lt;dg-hierarchy&gt;&lt;/dg-hierarchy&gt;&lt;/sh&lt;br&gt;ow&gt;</code></p>

Field Name	Description
Virtual System Name (vsys_name) <b>New in v7.0!</b>	The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.
Device Name (device_name) <b>New in v7.0!</b>	The hostname of the firewall on which the session was logged.

## Correlated Events (Logs)

**Format:** Receive Time\*, Serial Number\*, Device Name\*, Type\*, Virtual System Name\*, Virtual System ID\*, Device Group Hierarchy Level 1\*, Device Group Hierarchy Level 2\*, Device Group Hierarchy Level 3\*, Device Group Hierarchy Level 4\*, Source User\*, Source\*, Object Name\*, Object ID\*, Category\*, Severity\*, Evidence\*

\*All these fields are new in v7.0.5!

Field Name	Description
Receive Time (receive_time) *New in v7.0!	The time the firewall or Panorama recorded the event match.
Serial Number (serial) *New in v7.0!	Serial number of the firewall that generated the log.
Device Name (device_name) *New in v7.0!	The hostname of the firewall that generated the log.
Type (type) *New in v7.0!	Correlation log
Virtual System (vsys) *New in v7.0!	Name of the virtual system on the firewall that generated the correlation log (not pertinent to Panorama)
Virtual System ID(vsys_id) *New in v7.0!	ID of the virtual system on the firewall that generated the correlation log. (not pertinent to Panorama)
Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4) *New in v7.0!	A sequence of identification numbers that indicate the device group's location within a device group hierarchy. The firewall (or virtual system) generating the log includes the identification number of each ancestor in its device group hierarchy. The shared device group (level 0) is not included in this structure.  If the log values are 12, 34, 45, 0, it means that the log was generated by a firewall (or virtual system) that belongs to device group 45, and its ancestors are 34, and 12. To view the device group names that correspond to the value 12, 34 or 45, use one of the following methods:  CLI command in configure mode: <b>show readonly dg-meta-data</b>  API query: <code>/api/?type=op&amp;cmd=&lt;show&gt;&lt;dg-hierarchy&gt;&lt;/dg-hierarchy&gt;&lt;/sh ow&gt;</code>
Source User (srcuser) *New in v7.0!	Username of the user who triggered the event.
Source (src) *New in v7.0!	IP address of the user who triggered the event.
Object Name (object_name) *New in v7.0!	Name of the correlation object that was matched on. For example, Beacon Detection.

Field Name	Description
Object ID (object_id) <i>*New in v7.0!</i>	ID of the correlation object associated with the event.
Category (category) <i>*New in v7.0!</i>	Category of the correlation object that triggered the match. For example, Compromised Host.
Severity (severity) <i>*New in v7.0!</i>	Severity associated with the event; values are informational, low, medium, high, critical
Evidence (evidence) <i>*New in v7.0!</i>	A summary statement with evidence to indicate how many times the host has matched against the conditions defined in the correlation object. For example, Host visited known malware URL (19 times).

## Syslog Severity

The syslog severity is set based on the log type and contents.

Log Type/Severity	Syslog Severity
Traffic	Info
Config	Info
Threat/System—Informational	Info
Threat/System—Low	Notice
Threat/System—Medium	Warning
Threat/System—High	Error
Threat/System—Critical	Critical

## Custom Log/Event Format

To facilitate the integration with external log parsing systems, the firewall allows you to customize the log format; it also allows you to add custom *Key: Value* attribute pairs. Custom message formats can be configured under **Device > Server Profiles > Syslog > Syslog Server Profile > Custom Log Format**.

To achieve ArcSight Common Event Format (CEF) compliant log formatting, refer to the [CEF Configuration Guide](#).

## Escape Sequences

Any field that contains a comma or a double-quote is enclosed in double quotes. Furthermore, if a double-quote appears inside a field it is escaped by preceding it with another double-quote. To maintain backward compatibility, the Misc field in threat log is always enclosed in double-quotes.

## SNMP Monitoring and Traps

The following topics describe how Palo Alto Networks devices implement Simple Network Management Protocol (SNMP), and the procedures to configure SNMP monitoring and trap delivery.

- ▲ [SNMP for Palo Alto Networks Devices](#)
- ▲ [Use an SNMP Manager to Explore MIBs and Objects](#)
- ▲ [Enable SNMP Services for Firewall-Secured Network Elements](#)
- ▲ [Monitor Device Statistics Using SNMP](#)
- ▲ [Forward Traps to an SNMP Manager](#)
- ▲ [Supported MIBs](#)

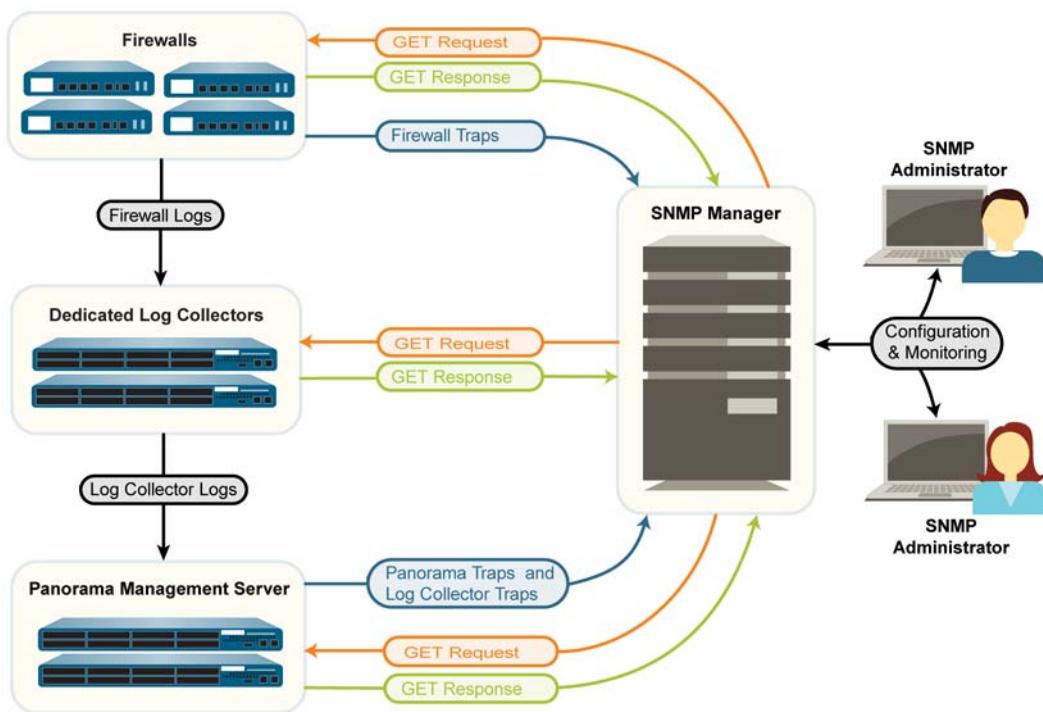
## SNMP for Palo Alto Networks Devices

You can use a Simple Network Management Protocol (SNMP) manager to monitor event-driven alerts and operational statistics for Palo Alto Networks devices and the traffic that those devices secure. The statistics and traps can help you identify resource limitations, system changes or failures, and malware attacks. You configure devices to send the alerts by forwarding log data as traps, and enable devices to send statistics in response to GET messages (requests) from your SNMP manager. Each trap and statistic has an object identifier (OID). Related OIDs are organized hierarchically within the Management Information Bases (MIBs) that you load into the SNMP manager to enable monitoring.

Palo Alto Networks devices support SNMP Version 2c and Version 3. Decide which to use based on the version that other devices in your network support and on your network security requirements. SNMPv3 is more secure and enables more granular access control for device statistics than SNMPv2c. The following table summarizes the security features of each version. You select the version and configure the security features when you [Monitor Device Statistics Using SNMP](#) and [Forward Traps to an SNMP Manager](#).

SNMP Version	Device/User Authentication	Message Privacy	Message Integrity	MIB Access Granularity
SNMPv2c	Community string	No (cleartext)	No	SNMP community access for all MIBs on a device
SNMPv3	EngineID, username, and authentication password (SHA hashing for the password)	Privacy password for AES 128 encryption of SNMP messages	Yes	User access based on views that include or exclude specific OIDs

**Figure: SNMP for Palo Alto Networks Devices** illustrates a deployment in which firewalls forward traps to an SNMP manager while also forwarding logs to Log Collectors. Alternatively, you could configure the Log Collectors to forward the firewall traps to the SNMP manager. For details on these deployments, refer to [Log Forwarding Options](#). In all deployments, the SNMP manager gets statistics directly from the devices. In this example, a single SNMP manager collects both traps and statistics, though you can use separate managers for these functions if that better suits your network.

**Figure: SNMP for Palo Alto Networks Devices**

## Use an SNMP Manager to Explore MIBs and Objects

To use SNMP for monitoring Palo Alto Networks devices, you must first load the [Supported MIBs](#) into your SNMP manager and determine which object identifiers (OIDs) correspond to the statistics and traps you want to monitor. The following topics provide an overview of how to find OIDs and MIBs in an SNMP manager. For the specific steps to perform these tasks, refer to your SNMP management software.

- ▲ [Identify a MIB Containing a Known OID](#)
- ▲ [Walk a MIB](#)
- ▲ [Identify the OID for a Palo Alto Networks Device Statistic or Trap](#)

### Identify a MIB Containing a Known OID

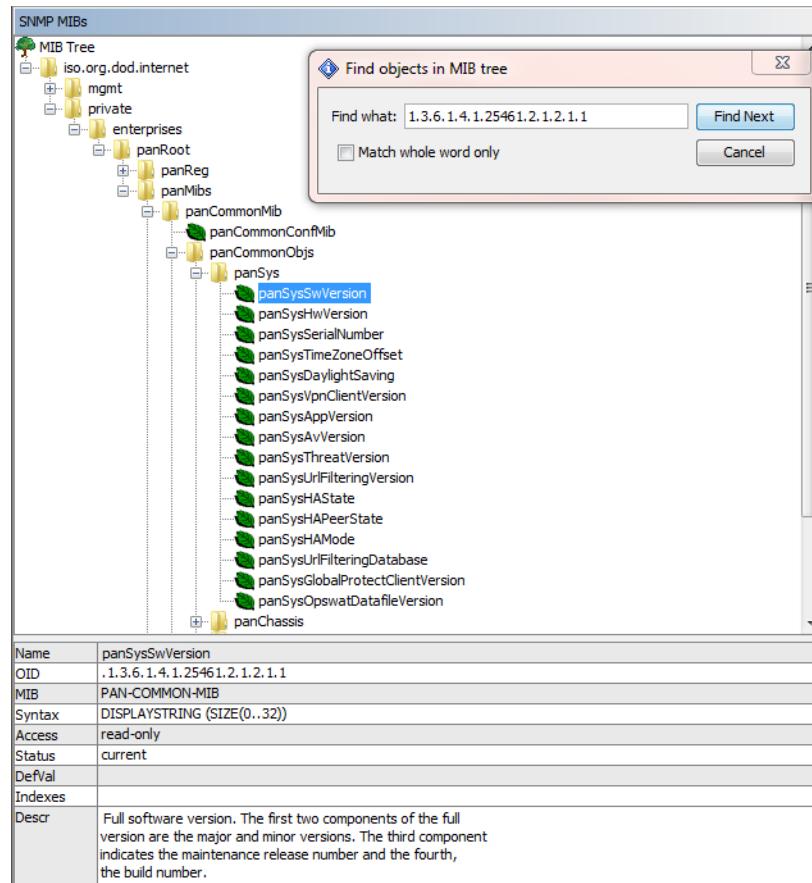
If you already know the OID for a particular SNMP object (device statistic or trap) and want to know the OIDs of similar objects so you can monitor them, you can explore the MIB that contains the known OID.

#### Identify a MIB Containing a Known OID

**Step 1** Load all the [Supported MIBs](#) into your SNMP manager.

### Identify a MIB Containing a Known OID (Continued)

**Step 2** Search the entire MIB tree for the known OID. The search result displays the MIB path for the OID, as well as information about the OID (for example, name, status, and description). You can then select other OIDs in the same MIB to see information about them.



**Step 3** Optionally, [Walk a MIB](#) to display all its objects.

### Walk a MIB

If you want to see which SNMP objects (device statistics and traps) are available for monitoring, displaying all the objects of a particular MIB can be useful. To do this, load the [Supported MIBs](#) into your SNMP manager and perform a *walk* on the desired MIB. To list the traps that Palo Alto Networks devices support, walk the panCommonEventEventsV2 MIB. In the following example, walking the [PAN-COMMON-MIB.my](#) displays the following list of OIDs and their values for certain device statistics:

The screenshot shows the 'SNMP MIBs' interface. On the left, the 'MIB Tree' pane displays a hierarchical tree structure of MIB objects under 'iso.org.dod.internet.private.enterprise.panRoot'. One specific object, 'panCommonMib', is highlighted with a blue selection box. On the right, the 'Result Table' pane shows a list of MIB objects with their corresponding values, types, and IP:Port details.

Name/OID	Value	Type	IP:Port
panSysHwVersion.0		OctetString	10.5.68.19:161
panSysTimeZoneOffset.0	-28800	Integer	10.5.68.19:161
panSysDaylightSaving.0	0	Integer	10.5.68.19:161
panSysThreatVersion.0	0	OctetString	10.5.68.19:161
panSysUrlFilteringVersion.0	0	OctetString	10.5.68.19:161
panSysOpswatDatafileVersion.0	0	OctetString	10.5.68.19:161
.1.3.6.1.4.1.25461.2.1.2.1.17.0	0	OctetString	10.5.68.19:161
.1.3.6.1.4.1.25461.2.1.2.1.18.0	0	OctetString	10.5.68.19:161
panSysIpClientVersion.0	0.0.0	OctetString	10.5.68.19:161
panSysGlobalProtectClientVersion.0	0.0.0	OctetString	10.5.68.19:161
panSysSerialNumber.0	0007PM00001	OctetString	10.5.68.19:161
panSysAvVersion.0	1751-2167	OctetString	10.5.68.19:161
panSysAppVersion.0	465-2420	OctetString	10.5.68.19:161
panSysSwVersion.0	7.0.0-c8	OctetString	10.5.68.19:161
panSysHAMode.0	disabled	OctetString	10.5.68.19:161
panSysUrlFilteringDatabase.0	paloaltonetworks	OctetString	10.5.68.19:161
panSysHAPeerState.0	unknown	OctetString	10.5.68.19:161

## Identify the OID for a Palo Alto Networks Device Statistic or Trap

To use an SNMP manager for monitoring Palo Alto Networks devices, you must know the OIDs of the device statistics and traps you want to monitor.

### Identify the OID for a Palo Alto Networks Device Statistic or Trap

- Step 1** Review the [Supported MIBs](#) to determine which one contains the type of statistic you want. For example, the [PAN-COMMON-MIB.my](#) contains device version information. The panCommonEventEventsV2 MIB contains all the traps that Palo Alto Networks devices support.
- Step 2** Open the MIB in a text editor and perform a keyword search. For example, using **Hardware version** as a search string in PAN-COMMON-MIB identifies the panSysHwVersion object:

```
panSysHwVersion OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Hardware version of the unit."
    ::= {panSys 2}
```

**Identify the OID for a Palo Alto Networks Device Statistic or Trap (Continued)**

**Step 3** In a MIB browser, search the MIB tree for the identified object name to display its OID. For example, the panSysHwVersion object has an OID of 1.3.6.1.4.1.25461.2.1.2.1.2.

The screenshot shows a MIB browser interface. On the left is a tree view of the MIB structure under 'SNMP MIBs'. The tree includes standard MIBs like iso.org.dod.internet and private enterprises, specifically the panRoot subtree which contains panReg and panMibs, and the panCommonMib subtree which contains panCommonConfMib and panCommonObjs. Under panCommonObjs is the panSys subtree, which contains objects like panSysSwVersion, panSysHwVersion (which is highlighted), panSysSerialNumber, panSysTimeZoneOffset, panSysDaylightSaving, panSysVpnClientVersion, panSysAppVersion, panSysAvVersion, panSysThreatVersion, panSysUrlFilteringVersion, panSysHASState, panSysHAPeerState, panSysHAMode, panSysUrlFilteringDatabase, panSysGlobalProtectClientVersion, and panSysOpswatDatafileVersion. At the bottom of the tree is panChassis. A search dialog box titled 'Find objects in MIB tree' is open in the center, with the text 'panSysHwVersion' entered in the 'Find what:' field and a checked 'Match whole word only' option. Below the tree is a detailed table for the selected object:

Name	panSysHwVersion
OID	.1.3.6.1.4.1.25461.2.1.2.1.2
MIB	PAN-COMMON-MIB
Syntax	DISPLAYSTRING (SIZE(0..128))
Access	read-only
Status	current
Def/val	
Indexes	
Descr	Hardware version of the unit.

## Enable SNMP Services for Firewall-Secured Network Elements

If you will use Simple Network Management Protocol (SNMP) to monitor or manage network elements (for example, switches and routers) that are within the security zones of Palo Alto Networks firewalls, you must create a security rule that allows SNMP services for those elements.



You don't need a security rule to enable SNMP monitoring of Palo Alto Networks devices. For details, see [Monitor Device Statistics Using SNMP](#).

### Enable SNMP Services for Firewall-Secured Network Elements

Step 1	Create an application group.	<ol style="list-style-type: none"><li>1. Select <b>Objects &gt; Application Group</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> to identify the application group.</li><li>3. Click <b>Add</b>, type <b>snmp</b>, and select <b>snmp</b> and <b>snmp-trap</b> from the drop-down.</li><li>4. Click <b>OK</b> to save the application group.</li></ol>
Step 2	Create a security rule to allow SNMP services.	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b> and click <b>Add</b>.</li><li>2. In the <b>General</b> tab, enter a <b>Name</b> for the rule.</li><li>3. In the <b>Source</b> and <b>Destination</b> tabs, click <b>Add</b> and enter a <b>Source Zone</b> and a <b>Destination Zone</b> for the traffic.</li><li>4. In the <b>Applications</b> tab, click <b>Add</b>, type the name of the applications group you just created, and select it from the drop-down.</li><li>5. In the <b>Actions</b> tab, verify that the <b>Action</b> is set to <b>Allow</b>, and then click <b>OK</b> and <b>Commit</b>.</li></ol>

## Monitor Device Statistics Using SNMP

The statistics that a Simple Network Management Protocol (SNMP) manager collects from Palo Alto Networks devices can help you gauge the health of your network (devices and connections), identify resource limitations, and monitor traffic or processing loads. The statistics include information such as interface states (up or down), active user sessions, concurrent sessions, session utilization, temperature, and system uptime.



You can't configure an SNMP manager to control Palo Alto Networks devices (using SET messages), only to collect statistics from them (using GET messages).

For details on how SNMP is implemented for Palo Alto Networks devices, see [SNMP for Palo Alto Networks Devices](#).

### Monitor Device Statistics Using SNMP

**Step 1** Configure the SNMP Manager to get statistics from devices.

The following steps provide an overview of the tasks you perform on the SNMP manager. For the specific steps, refer to the documentation of your SNMP manager.

1. To enable the SNMP manager to interpret device statistics, load the [Supported MIBs](#) for Palo Alto Networks devices and, if necessary, compile them.
2. For each device that the SNMP manager will monitor, define the connection settings (IP address and port) and authentication settings (SNMPv2c community string or SNMPv3 EngineID/username/password) for the device. Note that all Palo Alto Networks devices use port 161. The SNMP manager can use the same or different connection and authentication settings for multiple devices. The settings must match those you define when you configure SNMP on the device (see [Step 3](#)). For example, if you use SNMPv2c, the community string you define when configuring the device must match the community string you define in the SNMP manager for that device.
3. Determine the object identifiers (OIDs) of the statistics you want to monitor. For example, to monitor the session utilization percentage of a firewall, a MIB browser shows that this statistic corresponds to OID 1.3.6.1.4.1.25461.2.1.2.3.1.0 in [PAN-COMMON-MIB.my](#). For details, see [Use an SNMP Manager to Explore MIBs and Objects](#).
4. Configure the SNMP manager to monitor the desired OIDs.

**Monitor Device Statistics Using SNMP (Continued)**

<p><b>Step 2</b> Enable SNMP traffic on a device interface.</p> <p>This is the interface that will receive statistics requests from the SNMP manager.</p> <p><b>!</b> PAN-OS doesn't synchronize management (MGT) interface settings for devices in a high availability (HA) configuration. You must configure the interface for each HA peer.</p>	<p>Perform this step in the device web interface.</p> <p>To enable SNMP traffic on the MGT interface:</p> <ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Management</b> and edit the Management Interface Settings.</li><li>2. In the <b>Services</b> section, select the <b>SNMP</b> check box.</li><li>3. Click <b>OK</b> and <b>Commit</b>.</li></ol> <p>To enable SNMP traffic on any other interface:</p> <ol style="list-style-type: none"><li>1. Create an interface management profile for SNMP services:<ol style="list-style-type: none"><li>a. Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b> and click <b>Add</b>.</li><li>b. Enter a <b>Name</b> for the profile, then select the check boxes for <b>SNMP</b> and any other services the interface must support.</li><li>c. Click <b>OK</b> to save the profile.</li></ol></li><li>2. Assign the profile to the interface that will receive the SNMP requests:<ol style="list-style-type: none"><li>a. Select <b>Network &gt; Interfaces</b> and <b>Add</b> or edit the interface that will receive the SNMP requests. The interface type must be Layer 3 Ethernet.</li><li>b. Select <b>Advanced &gt; Other Info</b> and select the <b>Management Profile</b> you just created.</li><li>c. Click <b>OK</b> and <b>Commit</b>.</li></ol></li></ol>
--	---

**Monitor Device Statistics Using SNMP (Continued)**

<p><b>Step 3</b> Configure the device to respond to statistics requests from an SNMP manager.</p> <p> PAN-OS doesn't synchronize SNMP response settings for devices in a high availability (HA) configuration. You must configure these settings for each HA peer.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Operations</b> and, in the Miscellaneous section, click <b>SNMP Setup</b>.</li><li>2. Select the <b>SNMP Version</b> and configure the authentication values as follows. For version details, see <a href="#">SNMP for Palo Alto Networks Devices</a>.<ul style="list-style-type: none"><li>• <b>V2c</b>—Enter the <b>SNMP Community String</b>, which identifies a community of SNMP managers and monitored devices, and serves as a password to authenticate the community members to each other.<p> As a best practice, don't use the default community string <code>public</code>; it's well known and therefore not secure.</p></li><li>• <b>V3</b>—Create at least one SNMP view group and one user. User accounts and views provide authentication, privacy, and access control when devices forward traps and SNMP managers get device statistics.<ul style="list-style-type: none"><li>– <b>Views</b>—Each view is a paired OID and bitwise mask: the OID specifies a MIB and the mask (in hexadecimal format) specifies which objects are accessible within (include matching) or outside (exclude matching) that MIB. Click <b>Add</b> in the first list and enter a <b>Name</b> for the group of views. For each view in the group, click <b>Add</b> and configure the view <b>Name</b>, <b>OID</b>, matching <b>Option (include or exclude)</b>, and <b>Mask</b>.</li><li>– <b>Users</b>: Click <b>Add</b> in the second list, enter a username under <b>Users</b>, select the <b>View</b> group from the drop-down, enter the authentication password (<b>Auth Password</b>) used to authenticate to the SNMP manager, and enter the privacy password (<b>Priv Password</b>) used to encrypt SNMP messages to the SNMP manager.</li></ul></li></ul></li><li>3. Click <b>OK</b> and <b>Commit</b>.</li></ol>
<p><b>Step 4</b> Monitor the firewall statistics in an SNMP manager.</p>	<p>Refer to the documentation of your SNMP manager.</p> <p> When monitoring statistics related to firewall interfaces, you must match the interface indexes in the SNMP manager with interface names in the firewall web interface. For details, see <a href="#">Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors</a>.</p>

## Forward Traps to an SNMP Manager

Simple Network Management Protocol (SNMP) traps can alert you to system events (failures or changes in hardware or software of Palo Alto Networks devices) or to threats (traffic that matches a firewall security rule) that require immediate attention.



To see the list of traps that Palo Alto Networks devices support, use your SNMP Manager to access the panCommonEventEventsV2 MIB. For details, see [Use an SNMP Manager to Explore MIBs and Objects](#).

For details on how for Palo Alto Networks devices implement SNMP, see [SNMP for Palo Alto Networks Devices](#).

### Forward Firewall Traps to an SNMP Manager

<b>Step 1</b> Enable the SNMP manager to interpret the traps it receives.	Load the <a href="#">Supported MIBs</a> for Palo Alto Networks devices and, if necessary, compile them. For the specific steps, refer to the documentation of your SNMP manager.
<b>Step 2</b> Configure an SNMP Trap server profile.  The profile defines how the device accesses the SNMP managers (trap servers). You can define up to four SNMP managers for each profile.   Optionally, you can configure separate SNMP Trap server profiles for different log types, severity levels, and WildFire verdicts.	<ol style="list-style-type: none"> <li>1. Log in to the web interface of the Palo Alto Networks device.</li> <li>2. Select <b>Device &gt; Server Profiles &gt; SNMP Trap</b>.</li> <li>3. Click <b>Add</b> and enter a <b>Name</b> for the profile.</li> <li>4. If the firewall has more than one virtual system (vsys), select the <b>Location</b> (vsys or <b>Shared</b>) where this profile is available.</li> <li>5. Select the SNMP <b>Version</b> and configure the authentication values as follows. For version details, see <a href="#">SNMP for Palo Alto Networks Devices</a>.           <ul style="list-style-type: none"> <li>• <b>V2c</b>—For each server, click <b>Add</b> and enter the server <b>Name</b>, IP address (<b>SNMP Manager</b>), and <b>Community String</b>. The community string identifies a community of SNMP managers and monitored devices, and serves as a password to authenticate the community members to each other.                As a best practice, don't use the default community string <code>public</code>; it's well known and therefore not secure.             </li> <li>• <b>V3</b>—For each server, click <b>Add</b> and enter the server <b>Name</b>, IP address (<b>SNMP Manager</b>), SNMP <b>User</b> account (this must match a username defined in the SNMP manager), <b>EngineID</b> used to uniquely identify the device (you can leave the field blank to use the device serial number), authentication password (<b>Auth Password</b>) used to authenticate to the server, and privacy password (<b>Priv Password</b>) used to encrypt SNMP messages to the server.             </li> </ul> </li> <li>6. Click <b>OK</b> to save the server profile.</li> </ol>

**Forward Firewall Traps to an SNMP Manager (Continued)**

Step 3 Configure log forwarding.	<ol style="list-style-type: none"><li>1. Configure the destinations of Traffic, Threat, and WildFire traps:<ol style="list-style-type: none"><li>a. <a href="#">Create a log forwarding profile</a>. For each log type and each severity level or WildFire verdict, select the <b>SNMP Trap</b> server profile.</li><li>b. <a href="#">Assign the log forwarding profile to security rules</a>. The rules will trigger trap generation and forwarding.</li></ol></li><li>2. <a href="#">Configure the destinations of System, Config, HIP Match, and Correlation logs</a>. For each log (trap) type and severity level, select the <b>SNMP Trap</b> server profile.</li><li>3. Click <b>Commit</b>.</li></ol>
Step 4 Monitor the traps in an SNMP manager.	<p>Refer to the documentation of your SNMP manager.</p> <p> When monitoring traps related to firewall interfaces, you must match the interface indexes in the SNMP manager with interface names in the firewall web interface. For details, see <a href="#">Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors</a>.</p>

## Supported MIBs

The following table lists the Simple Network Management Protocol (SNMP) management information bases (MIBs) that Palo Alto Networks devices support. You must load these MIBs into your SNMP manager to monitor the objects (device statistics and traps) that are defined in the MIBs. For details, see [Use an SNMP Manager to Explore MIBs and Objects](#).

MIB Type	Supported MIBs
<b>Standard</b> —The Internet Engineering Task Force (IETF) maintains most standard MIBs. You can download the MIBs from the <a href="#">IETF website</a> .  Palo Alto Networks devices don't support every object (OID) in every one of these MIBs. See the <a href="#">Supported MIBs</a> links for an overview of the supported OIDs.	<a href="#">MIB-II</a> <a href="#">IF-MIB</a> <a href="#">HOST-RESOURCES-MIB</a> <a href="#">ENTITY-MIB</a> <a href="#">ENTITY-SENSOR-MIB</a> <a href="#">ENTITY-STATE-MIB</a> <a href="#">IEEE 802.3 LAG MIB</a> <a href="#">LLDP-V2-MIB.my</a>
<b>Enterprise</b> —You can download the enterprise MIBs from the Palo Alto Networks <a href="#">Technical Documentation</a> site.	<a href="#">PAN-COMMON-MIB.my</a> <a href="#">PAN-GLOBAL-REG-MIB.my</a> <a href="#">PAN-GLOBAL-TC-MIB.my</a> <a href="#">PAN-LC-MIB.my</a> <a href="#">PAN-PRODUCT-MIB.my</a> <a href="#">PAN-ENTITY-EXT-MIB.my</a> <a href="#">PAN-TRAPS.my</a>

### MIB-II

MIB-II provides object identifiers (OIDs) for network management protocols in TCP/IP-based networks. Use this MIB to monitor general information about devices and interfaces. For example, you can analyze trends in bandwidth usage by interface type (ifType object) to determine if the firewall needs more interfaces of that type to accommodate spikes in traffic volume.

Palo Alto Networks devices support only the following object groups:

Object Group	Description
system	Provides device information such as the hardware model, system uptime, FQDN, and physical location.
interfaces	Provides statistics for physical and logical interfaces such as type, current bandwidth (speed), operational status (for example, up or down), and discarded packets. Logical interface support includes VPN tunnels, aggregate groups, Layer 2 subinterfaces, Layer 3 subinterfaces, loopback interfaces, and VLAN interfaces.

[RFC 1213](#) defines this MIB.

## IF-MIB

IF-MIB supports interface types (physical and logical) and larger counters (64K) beyond those defined in [MIB-II](#). Use this MIB to monitor interface statistics in addition to those that MIB-II provides. For example, to monitor the current bandwidth of high-speed interfaces (greater than 2.2Gps) such as the 10G interfaces of the PA-5000 Series firewalls, you must check the ifHighSpeed object in IF-MIB instead of the ifSpeed object in MIB-II. IF-MIB statistics can be useful when evaluating the capacity of your network.

Palo Alto Networks devices support only the ifXTable in IF-MIB, which provides interface information such as the number of multicast and broadcast packets transmitted and received, whether an interface is in promiscuous mode, and whether an interface has a physical connector.

[RFC 2863](#) defines this MIB.

## HOST-RESOURCES-MIB

HOST-RESOURCES-MIB provides information for host computer resources. Use this MIB to monitor CPU and memory usage statistics for devices. For example, checking the current CPU load (`hrProcessorLoad` object) can help you troubleshoot performance issues on the firewall.

Palo Alto Networks devices support portions of the following object groups:

Object Group	Description
hrDevice	Provides information such as CPU load, storage capacity, and partition size. The <code>hrProcessorLoad</code> OIDs provide an average of the cores that process packets. For the PA-5060 firewall, which has multiple dataplanes (DPs), the average is of the cores across all the three DPs that process packets.
hrSystem	Provides information such as device uptime, number of current user sessions, and number of current processes.
hrStorage	Provides information such as the amount of used storage.

[RFC 2790](#) defines this MIB.

## ENTITY-MIB

ENTITY-MIB provides OIDs for multiple logical and physical components. Use this MIB to determine what physical components are loaded on a device (for example, fans and temperature sensors) and see related information such as models and serial numbers. You can also use the index numbers for these components to determine their operational status in the [ENTITY-SENSOR-MIB](#) and [ENTITY-STATE-MIB](#).

Palo Alto Networks devices support only portions of the `entPhysicalTable` group:

Object	Description
<code>entPhysicalIndex</code>	A single namespace that includes disk slots and disk drives.
<code>entPhysicalDescr</code>	The component description.

Object	Description
entPhysicalVendorType	The sysObjectID (see <a href="#">PAN-PRODUCT-MIB.my</a> ) when it is available (chassis and module objects).
entPhysicalContainedIn	The value of entPhysicalIndex for the component that contains this component.
entPhysicalClass	Chassis (3), container (5) for a slot, power supply (6), fan (7), sensor (8) for each temperature or other environmental, and module (9) for each line card.
entPhysicalParentRelPos	The relative position of this <i>child</i> component among its <i>sibling</i> components. Sibling components are defined as entPhysicalEntry components that share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects.
entPhysicalName	Supported only if the management (MGT) interface allows for naming the line card.
entPhysicalHardwareRev	The vendor-specific hardware revision of the component.
entPhysicalFirmwareRev	The vendor-specific firmware revision of the component.
entPhysicalSoftwareRev	The vendor-specific software revision of the component.
entPhysicalSerialNum	The vendor-specific serial number of the component.
entPhysicalMfgName	The name of the manufacturer of the component.
entPhysicalMfgDate	The date when the component was manufactured.
entPhysicalModelName	The disk model number.
entPhysicalAlias	An alias that the network manager specified for the component.
entPhysicalAssetID	A user-assigned asset tracking identifier that the network manager specified for the component.
entPhysicalIsFRU	Indicates whether the component is a field replaceable unit (FRU).
entPhysicalUris	The Common Language Equipment Identifier (CLEI) number of the component (for example, URN:CLEI:CNME120ARA).

[RFC 4133](#) defines this MIB.

## ENTITY-SENSOR-MIB

ENTITY-SENSOR-MIB adds support for physical sensors of networking equipment beyond what [ENTITY-MIB](#) defines. Use this MIB in tandem with the ENTITY-MIB to monitor the operational status of the physical components of a device (for example, fans and temperature sensors). For example, to troubleshoot issues that might result from environmental conditions, you can map the entity indexes from the ENTITY-MIB (entPhysicalDescr object) to operational status values (entPhysSensorOperStatus object) in the ENTITY-SENSOR-MIB. In the following example, all the fans and temperature sensors for a PA-3020 firewall are working:

Name/OID	Value
entPhysicalDescr.1	PA-3020
entPhysicalDescr.2	Fan #1 RPM
entPhysicalDescr.3	Fan #2 RPM
entPhysicalDescr.4	Fan #3 RPM
entPhysicalDescr.5	Fan #4 RPM
entPhysicalDescr.6	Temperature @ Ocelot
entPhysicalDescr.7	Temperature @ Switch
entPhysicalDescr.8	Temperature @ Cavium
entPhysicalDescr.9	Temperature @ Intel PHY
entPhysicalDescr.10	Temperature @ Switch Core
entPhysicalDescr.11	Temperature @ Cavium Core
entPhySensorOperStatus.2	ok (1)
entPhySensorOperStatus.3	ok (1)
entPhySensorOperStatus.4	ok (1)
entPhySensorOperStatus.5	ok (1)
entPhySensorOperStatus.6	ok (1)
entPhySensorOperStatus.7	ok (1)
entPhySensorOperStatus.8	ok (1)
entPhySensorOperStatus.9	ok (1)
entPhySensorOperStatus.10	ok (1)
entPhySensorOperStatus.11	ok (1)



The same OID might refer to different sensors on different device platforms. Use the ENTITY-MIB for the targeted platform to match the value to the description.

Palo Alto Networks devices support only portions of the entPhySensorTable group. The supported portions vary by platform. The devices support only thermal (temperature in Celsius) and fan (in RPM) sensors.

[RFC 3433](#) defines the ENTITY-SENSOR-MIB.

## ENTITY-STATE-MIB

ENTITY-STATE-MIB provides information about the state of physical components beyond what ENTITY-MIB defines, including the administrative and operational state of components in chassis-based platforms. Use this MIB in tandem with the ENTITY-MIB to monitor the operational state of the components of a PA-7000 Series firewall (for example, line cards, fan trays, and power supplies). For example, to troubleshoot log forwarding issues for Threat logs, you can map the log processing card (LPC) indexes from the ENTITY-MIB (entPhysicalDescr object) to operational state values (entStateOper object) in the ENTITY-STATE-MIB. The operational state values use numbers to indicate state: 1 for unknown, 2 for disabled, 3 for enabled, and 4 for testing. The PA-7000 Series firewall is the only Palo Alto Networks device that supports this MIB.

[RFC 4268](#) defines the ENTITY-STATE-MIB.

## IEEE 802.3 LAG MIB

Use the IEEE 802.3 LAG MIB to monitor the status of aggregate groups that have Link Aggregation Control Protocol ([LACP](#)) enabled. When the firewall logs LACP events, it also generates traps that are useful for troubleshooting. For example, the traps can tell you whether traffic interruptions between the firewall and an LACP peer resulted from lost connectivity or from mismatched interface speed and duplex values.

PAN-OS implements the following SNMP tables for LACP. Note that the dot3adTablesLastChanged object indicates the time of the most recent change to dot3adAggTable, dot3adAggPortListTable, and dot3adAggPortTable.

Table	Description
Aggregator Configuration Table (dot3adAggTable)	<p>This table contains information about every aggregate group that is associated with a firewall. Each aggregate group has one entry.</p> <p>Some table objects have restrictions, which the dot3adAggIndex object describes. This index is the unique identifier that the local system assigns to the aggregate group. It identifies an aggregate group instance among the subordinate managed objects of the containing object. The identifier is read-only.</p> <p> The ifTable MIB (a list of interface entries) does not support logical interfaces and therefore does not have an entry for the aggregate group.</p>
Aggregation Port List Table (dot3adAggPortListTable)	<p>This table lists the ports associated with each aggregate group in a firewall. Each aggregate group has one entry.</p> <p>The dot3adAggPortListPorts attribute lists the complete set of ports associated with an aggregate group. Each bit set in the list represents a port member. For non-chassis platforms, this is a 64-bit value. For chassis platforms, the value is an array of eight 64-bit entries.</p>
Aggregation Port Table (dot3adAggPortTable)	<p>This table contains LACP configuration information about every port associated with an aggregate group in a firewall. Each port has one entry. The table has no entries for ports that are not associated with an aggregate group.</p>
LACP Statistics Table (dot3adAggPortStatsTable)	<p>This table contains link aggregation information about every port associated with an aggregate group in a firewall. Each port has one row. The table has no entries for ports that are not associated with an aggregate group.</p>

The IEEE 802.3 LAG MIB includes the following LACP-related traps:

Trap Name	Description
panLACPLostConnectivityTrap	The peer lost connectivity to the firewall.
panLACPUnresponsiveTrap	The peer does not respond to the firewall.
panLACPNegotiationFailTrap	LACP negotiation with the peer failed.
panLACPSpeedDuplexTrap	The link speed and duplex settings on the firewall and peer do not match.
panLACPLinkDownTrap	An interface in the aggregate group is down.
panLACPLacpDownTrap	An interface was removed from the aggregate group.
panLACPLacpUpTrap	An interface was added to the aggregate group.

For the MIB definitions, refer to [IEEE 802.3 LAG MIB](#).

## LLDP-V2-MIB.my

Use the LLDP-V2-MIB to monitor Link Layer Discovery Protocol ([LLDP](#)) events. For example, you can check the lldpV2StatsRxPortFramesDiscardedTotal object to see the number of LLDP frames that were discarded for any reason. The Palo Alto Networks firewall uses LLDP to discover neighboring devices and their capabilities. LLDP makes troubleshooting easier, especially for virtual wire deployments where the ping or traceroute utilities won't detect the firewall.

Palo Alto Networks devices support all the LLDP-V2-MIB objects except:

- The following lldpV2Statistics objects:
  - lldpV2StatsRemTablesLastChangeTime
  - lldpV2StatsRemTablesInserts
  - lldpV2StatsRemTablesDeletes
  - lldpV2StatsRemTablesDrops
  - lldpV2StatsRemTablesAgeouts
- The following lldpV2RemoteSystemsData objects:
  - The lldpV2RemOrgDefInfoTable table
  - In the lldpV2RemTable table: lldpV2RemTimeMark

[RFC 4957](#) defines this MIB.

## PAN-COMMON-MIB.my

Use the PAN-COMMON-MIB to monitor the following information for Palo Alto Networks devices:

Object Group	Description
panSys	Contains such objects as device software/hardware versions, dynamic content versions, serial number, HA mode/state, and global counters. The global counters include those related to Denial of Service (DoS), IP fragmentation, TCP state, and dropped packets. Tracking these counters enables you to monitor traffic irregularities that result from DoS attacks, device or connection faults, or resource limitations. PAN-COMMON-MIB supports global counters for firewalls but not for Panorama.
panChassis	Chassis type and M-Series appliance mode (Panorama or Log Collector).
panSession	Session utilization information. For example, the total number of active sessions on the firewall or a specific virtual system.
panMgmt	Status of the connection from the firewall to the Panorama management server.
panGlobalProtect	GlobalProtect gateway utilization as a percentage, maximum tunnels allowed, and number of active tunnels.

Object Group	Description
panLogCollector	Log Collector information such as the logging rate, log database storage duration (in days), and RAID disk usage.

## PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my contains global, top-level OID definitions for various sub-trees of Palo Alto Networks enterprise MIB modules. This MIB doesn't contain objects for you to monitor; it is required only for referencing by other MIBs.

## PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my defines conventions (for example, character length and allowed characters) for the text values of objects in Palo Alto Networks enterprise MIB modules. All Palo Alto Networks products use these conventions. This MIB doesn't contain objects for you to monitor; it is required only for referencing by other MIBs.

## PAN-LC-MIB.my

PAN-LC-MIB.my contains definitions of managed objects that Log Collectors (M-Series appliances in Log Collector mode) implement. Use this MIB to monitor the logging rate, log database storage duration (in days), and disk usage (in MB) of each logical disk (up to four) on a Log Collector. For example, you can use this information to determine whether you should add more Log Collectors or forward logs to an external server (for example, a syslog server) for archiving.

## PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my defines sysObjectID OIDs for all Palo Alto Networks products. This MIB doesn't contain objects for you to monitor; it is required only for referencing by other MIBs.

## PAN-ENTITY-EXT-MIB.my

Use PAN-ENTITY-EXT-MIB.my in tandem with the [ENTITY-MIB](#) to monitor power usage for the physical components of a PA-7000 Series firewall (for example, fan trays, and power supplies), which is the only Palo Alto Networks device that supports this MIB. For example, when troubleshooting log forwarding issues, you might want to check the power usage of the log processing cards (LPCs): you can map the LPC indexes from the ENTITY-MIB (entPhysicalDescr object) to values in the PAN-ENTITY-EXT-MIB (panEntryFRUModelPowerUsed object).

## PAN-TRAPS.my

Use PAN-TRAPS.my to see a complete listing of all the generated traps and information about them (for example, a description). For a list of traps that Palo Alto Networks devices support, refer to the [PAN-COMMON-MIB.my](#) > **panCommonEvents** > **panCommonEventsEvents** > **panCommonEventEventsV2** object.

# NetFlow Monitoring

NetFlow is an industry-standard protocol that the firewall can use to export statistics about the IP traffic that traverses its interfaces. The firewall exports the statistics as NetFlow fields to a NetFlow collector. The NetFlow collector is a server you use to analyze network traffic for security, administration, accounting and troubleshooting. All Palo Alto Networks firewalls support NetFlow (Version 9) except the PA-4000 Series and PA-7000 Series firewalls. The firewalls support only unidirectional NetFlow, not bidirectional. You can enable NetFlow exports on all interface types except HA, log card, or decrypt mirror. To identify firewall interfaces in a NetFlow collector, see [Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors](#). The firewall supports standard and enterprise (PAN-OS specific) NetFlow templates.

## ▲ Configure NetFlow Exports

## ▲ NetFlow Templates

## Configure NetFlow Exports

Configure NetFlow Exports	
Step 1 Create a NetFlow server profile.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Server Profiles &gt; NetFlow</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> for the profile.</li><li>3. Specify the frequency at which the firewall refreshes <a href="#">NetFlow Templates</a> in <b>Minutes</b> (default is 30) or <b>Packets</b> (default is 20), according to the requirements of your NetFlow collector.</li><li>4. For the <b>Active Timeout</b>, specify the frequency in minutes at which the firewall exports records (default is 5).</li><li>5. Select the <b>PAN-OS Field Types</b> check box if you want the firewall to export App-ID and User-ID fields.</li><li>6. For each NetFlow collector (up to two per profile) that will receive fields, click <b>Add</b> and enter an identifying server <b>Name</b>, hostname or IP address (<b>NetFlow Server</b>), and access <b>Port</b> (default is 2055).</li><li>7. Click <b>OK</b> to save the profile.</li></ol>
Step 2 Assign the NetFlow server profile to the interfaces that carry the traffic you want to analyze.  In this example, you assign the profile to an existing Ethernet interface.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and click an interface name to edit it.</li><li>2. In the <b>NetFlow Profile</b> drop-down, select the NetFlow server profile and click <b>OK</b>.</li><li>3. Click <b>Commit</b>.</li></ol>
Step 3 Monitor the firewall traffic in a NetFlow collector.	Refer to the documentation for your NetFlow collector.   When monitoring statistics, you must match the interface indexes in the NetFlow collector with interface names in the firewall web interface. For details, see <a href="#">Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors</a> .

## NetFlow Templates

NetFlow collectors use templates to decipher the fields that the firewall exports. The firewall selects a template based on the type of exported data: IPv4 or IPv6 traffic, with or without NAT, and with standard or enterprise-specific (PAN-OS specific) fields. The firewall periodically refreshes templates to re-evaluate which one to use (in case the type of exported data changes) and to apply any changes to the fields in the selected template. When you [Configure NetFlow Exports](#), you set the refresh frequency according to the requirements of your NetFlow collector.

The Palo Alto Networks firewall supports the following NetFlow templates:

Template	ID
IPv4 Standard	256
IPv4 Enterprise	257
IPv6 Standard	258
IPv6 Enterprise	259
IPv4 with NAT Standard	260
IPv4 with NAT Enterprise	261
IPv6 with NAT Standard	262
IPv6 with NAT Enterprise	263

The following table lists the NetFlow fields that the firewall can send, along with the templates that define them:

Value	Field	Description	Templates
1	IN_BYTES	Incoming counter with length N * 8 bits for the number of bytes associated with an IP flow. By default, N is 4.	All templates
2	IN_PKTS	Incoming counter with length N * 8 bits for the number of packets associated with an IP flow. By default, N is 4.	All templates
4	PROTOCOL	IP protocol byte.	All templates
5	TOS	Type of Service byte setting when entering the ingress interface.	All templates
6	TCP_FLAGS	Total of all the TCP flags in this flow.	All templates
7	L4_SRC_PORT	TCP/UDP source port number (for example, FTP, Telnet, or equivalent).	All templates
8	IPV4_SRC_ADDR	IPv4 source address.	IPv4 standard IPv4 enterprise IPv4 with NAT standard IPv4 with NAT enterprise

Value	Field	Description	Templates
10	INPUT_SNMP	Input interface index. The value length is 2 bytes by default, but higher values are possible. For details on how Palo Alto Networks firewalls generate interface indexes, see <a href="#">Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors</a> .	All templates
11	L4_DST_PORT	TCP/UDP destination port number (for example, FTP, Telnet, or equivalent).	All templates
12	IPV4_DST_ADDR	IPv4 destination address.	IPv4 standard IPv4 enterprise IPv4 with NAT standard IPv4 with NAT enterprise
14	OUTPUT_SNMP	Output interface index. The value length is 2 bytes by default, but higher values are possible. For details on how Palo Alto Networks firewalls generate interface indexes, see <a href="#">Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors</a> .	All templates
21	LAST_SWITCHED	System uptime in milliseconds when the last packet of this flow was switched.	All templates
22	FIRST_SWITCHED	System uptime in milliseconds when the first packet of this flow was switched.	All templates
27	IPV6_SRC_ADDR	IPv6 source address.	IPv6 standard IPv6 enterprise IPv6 with NAT standard IPv6 with NAT enterprise
28	IPV6_DST_ADDR	IPv6 destination address.	IPv6 standard IPv6 enterprise IPv6 with NAT standard IPv6 with NAT enterprise
32	ICMP_TYPE	Internet Control Message Protocol (ICMP) packet type. This is reported as: ICMP Type * 256 + ICMP code	All templates
61	DIRECTION	Flow direction: • 0 = ingress • 1 = egress	All templates

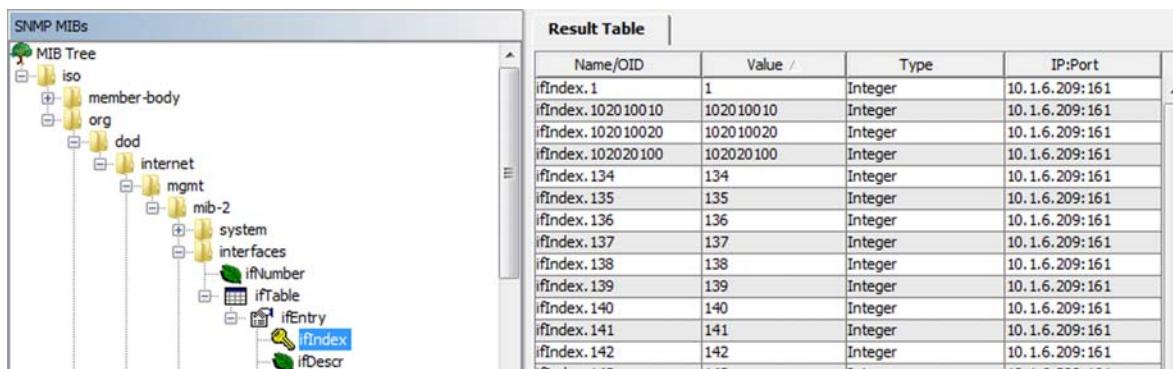
Value	Field	Description	Templates
148	flowId	An identifier of a flow that is unique within an observation domain. You can use this information element to distinguish between different flows if flow keys such as IP addresses and port numbers are not reported or are reported in separate records. The flowID corresponds to the session ID field in Traffic and Threat logs.	All templates
233	firewallEvent	Indicates a firewall event: <ul style="list-style-type: none"><li>• 0 = Ignore (invalid)</li><li>• 1 = Flow created</li><li>• 2 = Flow deleted</li><li>• 3 = Flow denied</li><li>• 4 = Flow alert</li><li>• 5 = Flow update (the session state changed from active to deny)</li></ul>	All templates
225	postNATSourceIPv4Address	The definition of this information element is identical to that of sourceIPv4Address, except that it reports a modified value that the firewall produced during network address translation after the packet traversed the interface.	IPv4 with NAT standard IPv4 with NAT enterprise
226	postNATDestinationIPv4Address	The definition of this information element is identical to that of destinationIPv4Address, except that it reports a modified value that the firewall produced during network address translation after the packet traversed the interface.	IPv4 with NAT standard IPv4 with NAT enterprise
227	postNAPTSourceTransportPort	The definition of this information element is identical to that of sourceTransportPort, except that it reports a modified value that the firewall produced during network address port translation after the packet traversed the interface.	IPv4 with NAT standard IPv4 with NAT enterprise
228	postNAPTDestinationTransportPort	The definition of this information element is identical to that of destinationTransportPort, except that it reports a modified value that the firewall produced during network address port translation after the packet traversed the interface.	IPv4 with NAT standard IPv4 with NAT enterprise

Value	Field	Description	Templates
281	postNATSourceIPv6Address	The definition of this information element is identical to the definition of information element sourceIPv6Address, except that it reports a modified value that the firewall produced during NAT64 network address translation after the packet traversed the interface. See <a href="#">RFC 2460</a> for the definition of the source address field in the IPv6 header. See <a href="#">RFC 6146</a> for NAT64 specification.	IPv6 with NAT standard IPv6 with NAT enterprise
282	postNATDestinationIPv6Address	The definition of this information element is identical to the definition of information element destinationIPv6Address, except that it reports a modified value that the firewall produced during NAT64 network address translation after the packet traversed the interface. See <a href="#">RFC 2460</a> for the definition of the destination address field in the IPv6 header. See <a href="#">RFC 6146</a> for NAT64 specification.	IPv6 with NAT standard IPv6 with NAT enterprise
346	privateEnterpriseNumber	This is a unique private enterprise number that identifies Palo Alto Networks: 25461.	IPv4 enterprise IPv4 with NAT enterprise IPv6 enterprise IPv6 with NAT enterprise
56701	App-ID	The name of an application that App-ID identified. The name can be up to 32 bytes.	IPv4 enterprise IPv4 with NAT enterprise IPv6 enterprise IPv6 with NAT enterprise
56702	User-ID	A username that User-ID identified. The name can be up to 64 bytes.	IPv4 enterprise IPv4 with NAT enterprise IPv6 enterprise IPv6 with NAT enterprise

## Firewall Interface Identifiers in SNMP Managers and NetFlow Collectors

When you use a NetFlow collector (see [NetFlow Monitoring](#)) or SNMP manager (see [SNMP Monitoring and Traps](#)) to monitor the Palo Alto Networks firewall, an interface index (SNMP ifindex object) identifies the interface that carried a particular flow (see [Figure: Interface Indexes in an SNMP Manager](#)). In contrast, the firewall web interface uses interface names as identifiers (for example, ethernet1/1), not indexes. To understand which statistics that you see in a NetFlow collector or SNMP manager apply to which firewall interface, you must be able to match the interface indexes with interface names.

**Figure: Interface Indexes in an SNMP Manager**



The screenshot shows the SNMP MIB browser interface. On the left, the MIB tree is displayed under the 'SNMP MIBs' tab, specifically the 'MIB Tree' section. The tree structure includes 'iso', 'member-body', 'org', 'dod', 'internet', 'mgmt', 'mib-2', 'system', 'interfaces', 'ifNumber', 'ifTable', 'ifEntry', 'ifIndex', and 'ifDescr'. On the right, a 'Result Table' is shown with the following data:

Name/OID	Value /	Type	IP:Port
ifIndex.1	1	Integer	10.1.6.209:161
ifIndex.102010010	102010010	Integer	10.1.6.209:161
ifIndex.102010020	102010020	Integer	10.1.6.209:161
ifIndex.102020100	102020100	Integer	10.1.6.209:161
ifIndex.134	134	Integer	10.1.6.209:161
ifIndex.135	135	Integer	10.1.6.209:161
ifIndex.136	136	Integer	10.1.6.209:161
ifIndex.137	137	Integer	10.1.6.209:161
ifIndex.138	138	Integer	10.1.6.209:161
ifIndex.139	139	Integer	10.1.6.209:161
ifIndex.140	140	Integer	10.1.6.209:161
ifIndex.141	141	Integer	10.1.6.209:161
ifIndex.142	142	Integer	10.1.6.209:161

You can match the indexes with names by understanding the formulas that the firewall uses to calculate indexes. The formulas vary by platform and interface type: physical or logical.

Physical interface indexes have a range of 1-9999, which the firewall calculates as follows:

Firewall Platform	Calculation	Example Interface Index
Non-chassis based: VM-Series, PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series   The PA-4000 Series platform supports SNMP but not NetFlow.	MGT port + physical port offset <ul style="list-style-type: none"> <li>• MGT port—This is a constant that depends on the platform:           <ul style="list-style-type: none"> <li>• 2 for hardware-based firewalls (for example, the PA-5000 Series firewall)</li> <li>• 1 for the VM-Series firewall</li> </ul> </li> <li>• Physical port offset—This is the physical port number.</li> </ul>	PA-5000 Series firewall, Eth1/4 = 2 (MGT port) + 4 (physical port) = 6

Firewall Platform	Calculation	Example Interface Index
Chassis based: PA-7000 Series firewalls  This platform supports SNMP but not NetFlow.	(Max. ports * slot) + physical port offset + MGT port <ul style="list-style-type: none"> <li>Maximum ports—This is a constant of 64.</li> <li>Slot—This is the chassis slot number of the network interface card.</li> <li>Physical port offset—This is the physical port number.</li> <li>MGT port—This is a constant of 5 for PA-7000 Series firewalls.</li> </ul>	PA-7000 Series firewall, Eth3/9 = [64 (max. ports) * 3 (slot)] + 9 (physical port) + 5 (MGT port) = <b>206</b>

Logical interface indexes for all platforms are nine-digit numbers that the firewall calculates as follows:

Interface Type	Range	Digit 9	Digits 7-8	Digits 5-6	Digits 1-4	Example Interface Index
Layer 3 subinterface	101010001-199999999	Type: 1	Interface slot: 1-9 (01-09)	Interface port: 1-9 (01-09)	Subinterface: suffix 1-9999 (0001-9999)	Eth1/5.22 = 100000000 (type) + 100000 (slot) + 50000 (port) + 22 (suffix) = <b>101050022</b>
Layer 2 subinterface	101010001-199999999	Type: 1	Interface slot: 1-9 (01-09)	Interface port: 1-9 (01-09)	Subinterface: suffix 1-9999 (0001-9999)	Eth2/3.6 = 100000000 (type) + 200000 (slot) + 30000 (port) + 6 (suffix) = <b>102030006</b>
Vwire subinterface	101010001-199999999	Type: 1	Interface slot: 1-9 (01-09)	Interface port: 1-9 (01-09)	Subinterface: suffix 1-9999 (0001-9999)	Eth4/2.312 = 100000000 (type) + 400000 (slot) + 20000 (port) + 312 (suffix) = <b>104020312</b>
VLAN	200000001-200009999	Type: 2	00	00	VLAN suffix: 1-9999 (0001-9999)	VLAN.55 = 200000000 (type) + 55 (suffix) = <b>200000055</b>
Loopback	300000001-300009999	Type: 3	00	00	Loopback suffix: 1-9999 (0001-9999)	Loopback.55 = 300000000 (type) + 55 (suffix) = <b>300000055</b>
Tunnel	400000001-400009999	Type: 4	00	00	Tunnel suffix: 1-9999 (0001-9999)	Tunnel.55 = 400000000 (type) + 55 (suffix) = <b>400000055</b>
Aggregate group	500010001-500089999	Type: 5	00	AE suffix: 1-8 (01-08)	Subinterface: suffix 1-9999 (0001-9999)	AE5.99 = 500000000 (type) + 50000 (AE Suffix) + 99 (suffix) = <b>500050099</b>



# User-ID

---

---

The User Identification (User-ID™) feature of the Palo Alto Networks next-generation firewall enables you to create policies and perform reporting based on users and groups rather than individual IP addresses.

- ▲ [User-ID Overview](#)
- ▲ [User-ID Concepts](#)
- ▲ [Enable User-ID](#)
- ▲ [Map Users to Groups](#)
- ▲ [Map IP Addresses to Users](#)
- ▲ [Configure a Firewall to Share User Mapping Data with Other Firewalls](#)
- ▲ [Enable User- and Group-Based Policy](#)
- ▲ [Enable Policy for Users with Multiple Accounts](#)
- ▲ [Verify the User-ID Configuration](#)
- ▲ [Deploy User-ID in a Large-Scale Network](#)

## User-ID Overview

User-ID seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory and terminal services offerings, enabling you to tie application activity and policy rules to users and groups—not just IP addresses. Furthermore, with User-ID enabled, the Application Command Center (ACC), App-Scope, reports, and logs all include usernames in addition to user IP addresses.

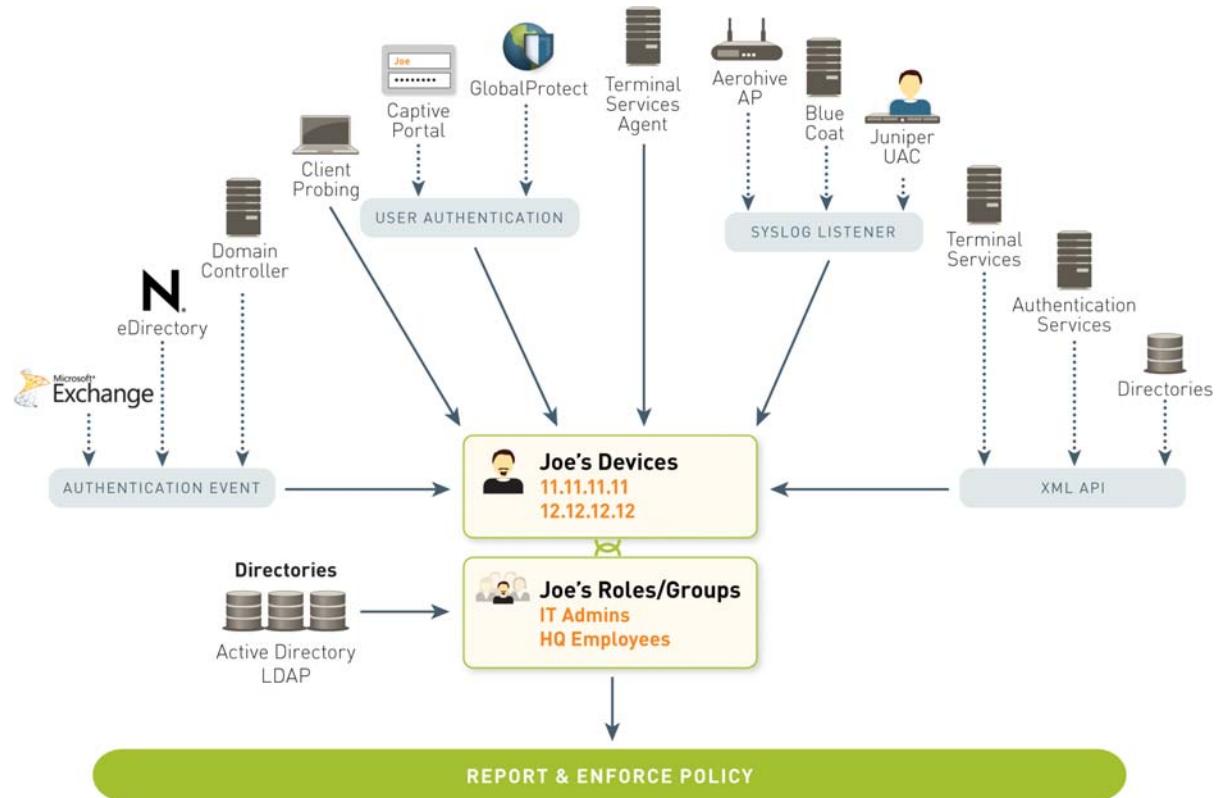
Palo Alto Networks firewalls support monitoring of the following enterprise services:

- Microsoft Active Directory
- Lightweight Directory Access Protocol (LDAP)
- Novell eDirectory
- Citrix Metaframe Presentation Server or XenApp
- Microsoft Terminal Services

For user- and group-based policies, the firewall requires a list of all available users and their corresponding group mappings that you can select when defining your policies. The firewall collects [Group Mapping](#) information by connecting directly to your LDAP directory server.

To enforce user- and group-based policies, the firewall must be able to map the IP addresses in the packets it receives to usernames. User-ID provides many mechanisms to collect this [User Mapping](#) information. For example, the User-ID agent monitors server logs for login events, probes clients, and listens for syslog messages from authenticating services. To identify mappings for IP addresses that the agent didn't map, you can configure the firewall to redirect HTTP requests to a Captive Portal login. You can tailor the user mapping mechanisms to suit your environment, and even use different mechanisms at different sites.

 User-ID does not work in environments where the source IP addresses of users are subject to NAT translation before the firewall maps the IP addresses to usernames.

**Figure: User-ID**

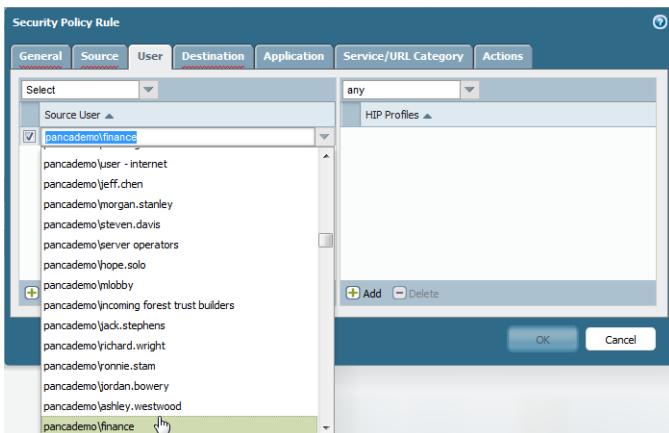
See [User-ID Concepts](#) for information on how User-ID works and [Enable User-ID](#) for instructions on setting up User-ID.

# User-ID Concepts

- ▲ Group Mapping
- ▲ User Mapping

## Group Mapping

To define policy rules based on user or group, first you create an LDAP server profile that defines how the firewall connects and authenticates to your directory server. The firewall supports a variety of directory servers, including Microsoft Active Directory (AD), Novell eDirectory, and Sun ONE Directory Server. The server profile also defines how the firewall searches the directory to retrieve the list of groups and the corresponding list of members. Next you create a group mapping configuration to [Map Users to Groups](#). Then you can select the users or groups when defining policy rules.



Defining policy rules based on group membership rather than on individual users simplifies administration because you don't have to update the rules whenever new users are added to a group. For example, the following security rules allow access to specific internal applications based on group membership:

Name	Tags	Type	Zone	Address	User	HIP Profile	Application
CRM Access	none	universal	trust	any	Finance	Patches	sap
Eng access	none	universal	trust	any	Engineering	any	bugzilla perforce

When configuring group mapping, you can limit which groups will be available in policy rules. You can specify groups that already exist in your directory service or define custom groups based on LDAP filters. Defining custom groups can be quicker than creating new groups or changing existing ones on an LDAP server, and doesn't require an LDAP administrator to intervene. User-ID maps all the LDAP directory users who match the filter to the custom group. For example, you might want a security policy that allows contractors in the Marketing Department to access social networking sites. If no Active Directory group exists for that department, you can configure an LDAP filter that matches users for whom the LDAP attribute Department is set to Marketing. Log queries and reports that are based on user groups will include custom groups.

## User Mapping

Having the names of the users and groups is only one piece of the puzzle. The firewall also needs to know which IP addresses map to which users so that security rules can be enforced appropriately. [Figure: User-ID](#) illustrates the different methods that are used to identify users and groups on your network and shows how user mapping and group mapping work together to enable user- and group-based security enforcement and visibility.

The following topics describe the different methods of user mapping:

- ▲ [Server Monitoring](#)
- ▲ [Client Probing](#)
- ▲ [Port Mapping](#)
- ▲ [Syslog](#)
- ▲ [Captive Portal](#)
- ▲ [GlobalProtect](#)
- ▲ [User-ID XML API](#)

### [Server Monitoring](#)

With server monitoring a User-ID agent—either a Windows-based agent running on a domain server in your network, or the integrated PAN-OS User-ID agent running on the firewall—monitors the security event logs for specified Microsoft Exchange Servers, domain controllers, or Novell eDirectory servers for login events. For example, in an AD environment, you can configure the User-ID agent to monitor the security logs for Kerberos ticket grants or renewals, Exchange server access (if configured), and file and print service connections. Note that for these events to be recorded in the security log, the AD domain must be configured to log successful account login events. In addition, because users can log in to any of the servers in the domain, you must set up server monitoring for all servers to capture all user login events.

Because server monitoring requires very little overhead and because the majority of users can generally be mapped using this method, it is recommended as the base user mapping method for most User-ID deployments. See [Configure User Mapping Using the Windows User-ID Agent](#) or [Configure User Mapping Using the PAN-OS Integrated User-ID Agent](#) for details.

### [Client Probing](#)

In a Microsoft Windows environment, you can configure the User-ID agent to probe client systems using Windows Management Instrumentation (WMI). The Windows-based User-ID agent can also perform NetBIOS probing (not supported on the PAN-OS integrated User-ID agent). Probing is particularly useful in environments with a high IP address turnover because changes will be reflected on the firewall more quickly, enabling more accurate enforcement of user-based policies. However, if the correlation between IP addresses and users is fairly static, you probably do not need to enable client probing. Because probing can generate a large amount of network traffic (based on the total number of mapped IP addresses), the agent that will be initiating the probes should be located as close as possible to the end clients.

If probing is enabled, the agent will probe each learned IP address periodically (every 20 minutes by default, but this is configurable) to verify that the same user is still logged in. In addition, when the firewall encounters an IP address for which it has no user mapping, it will send the address to the agent for an immediate probe.

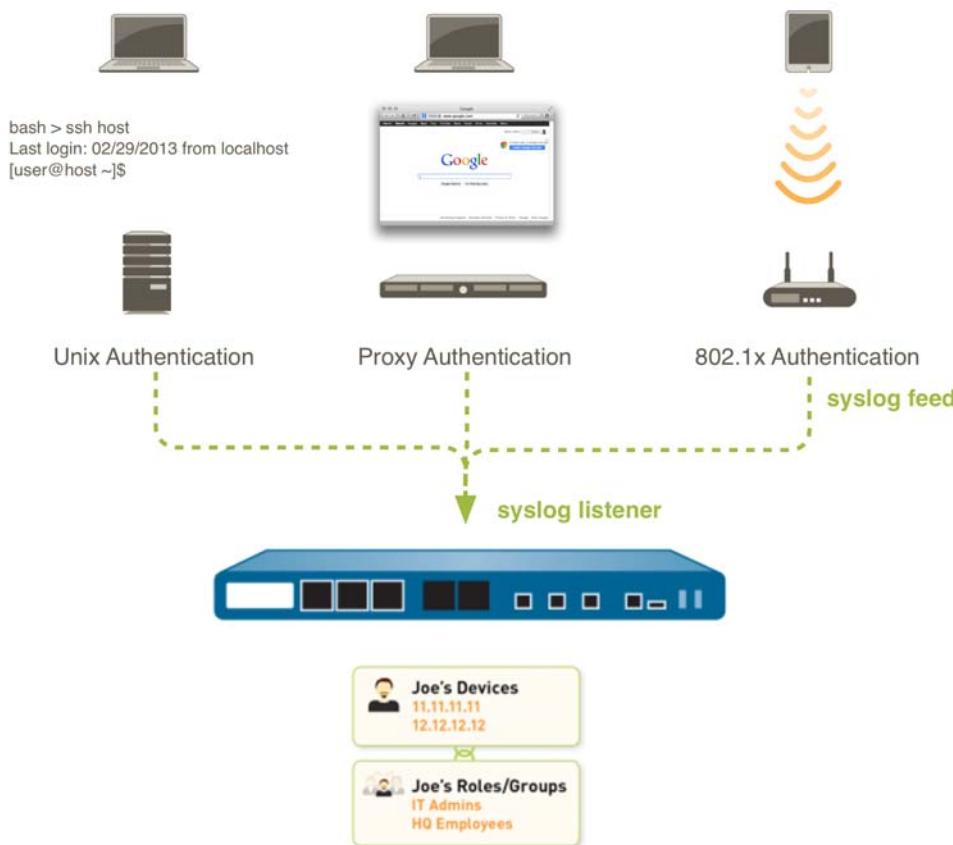
See [Configure User Mapping Using the Windows User-ID Agent](#) or [Configure User Mapping Using the PAN-OS Integrated User-ID Agent](#) for details.

## Port Mapping

In environments with multi-user systems—such as Microsoft Terminal Server or Citrix environments—many users share the same IP address. In this case, the user-to-IP address mapping process requires knowledge of the source port of each client. To perform this type of mapping, you must install the Palo Alto Networks Terminal Services Agent on the Windows/Citrix terminal server itself to intermediate the assignment of source ports to the various user processes. For terminal servers that do not support the Terminal Services Agent, such as Linux terminal servers, you can use the XML API to send user mapping information from login and logout events to User-ID. See [Configure User Mapping for Terminal Server Users](#) for configuration details.

## Syslog

In environments with existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—the firewall User-ID agent (either the Windows agent or the PAN-OS integrated agent on the firewall) can listen for authentication syslog messages from those services. Syslog filters, which are provided by a content update (integrated User-ID agent only) or configured manually, allow the User-ID agent to parse and extract usernames and IP addresses from authentication syslog events generated by the external service, and add the information to the User-ID IP address-to-username mappings maintained by the firewall. See [Configure User-ID to Receive User Mappings from a Syslog Sender](#) for configuration details.

**Figure: User-ID Integration with Syslog**

## Captive Portal

If the firewall or the User-ID agent can't map an IP address to a username—for example, if the user isn't logged in or uses an operating system such as Linux that your domain servers don't support—you can configure Captive Portal. Any web traffic (HTTP or HTTPS) that matches a Captive Portal policy rule requires user authentication. You can base the authentication on a transparent browser-challenge ([Kerberos Single Sign-On \(SSO\)](#) or [NT LAN Manager \(NTLM\)](#) authentication), web form (for RADIUS, TACACS+, LDAP, Kerberos, or local database authentication), or client certificates. For details, see [Map IP Addresses to Usernames Using Captive Portal](#).

## GlobalProtect

For mobile or roaming users, the GlobalProtect client provides the user mapping information to the firewall directly. In this case, every GlobalProtect user has an agent or app running on the client that requires the user to enter login credentials for VPN access to the firewall. This login information is then added to the User-ID user mapping table on the firewall for visibility and user-based security policy enforcement. Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is

explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service. For more information on setting up GlobalProtect, refer to the [GlobalProtect Administrator's Guide](#).

## User-ID XML API

For other types of user access that cannot be mapped using any of the standard user mapping methods or Captive Portal—for example, to add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x enabled wireless network—you can use the User-ID XML API to capture login events and send them to the User-ID agent or directly to the firewall. See [Send User Mappings to User-ID Using the XML API](#) for details.

## Enable User-ID

You must complete the following tasks to set up the firewall to user users and groups in policy enforcement, logging, and reporting:

- [Map Users to Groups](#)
- [Map IP Addresses to Users](#)
- [Enable User- and Group-Based Policy](#)
- [Verify the User-ID Configuration](#)

# Map Users to Groups

Use the following procedure to enable the firewall to connect to your LDAP directory and retrieve [Group Mapping](#) information:



The following are best practices for group mapping in an Active Directory (AD) environment:

- If you have a single domain, you need only one LDAP server profile that connects the firewall to the domain controller with the best connectivity. You can add additional domain controllers for fault tolerance.
- If you have multiple domains and/or multiple forests, you must create a server profile to connect to a domain server in each domain/forest. Take steps to ensure unique usernames in separate forests.
- If you have Universal Groups, create a server profile to connect to the Global Catalog server.

## Map Users to Groups

<p><b>Step 1</b> Add an LDAP server profile.</p> <p>The profile defines how the firewall connects to the directory servers from which it collects group mapping information. You can add up to four servers to the profile but they must be the same <b>Type</b>.</p>	<p><b>Configure an LDAP Server Profile:</b></p> <ol style="list-style-type: none"><li>1. Select <b>Device &gt; Server Profiles &gt; LDAP</b>, click <b>Add</b>, and enter a <b>Profile Name</b>.</li><li>2. For each LDAP server, click <b>Add</b> and enter the server <b>Name</b>, IP address (<b>LDAP Server</b>), and <b>Port</b> (default is 389).</li><li>3. Based on your <b>Type</b> selection (for example, <b>active-directory</b>), the firewall automatically populates the correct LDAP attributes in the group mapping settings. However, if you customized your LDAP schema, you might need to modify the default settings.</li><li>4. In the <b>Base DN</b> field, enter the Distinguished Name (DN) of the LDAP tree location where you want the firewall to begin its search for user and group information.</li><li>5. Enter the authentication credentials for binding to the LDAP tree in the <b>Bind DN</b>, <b>Password</b>, and <b>Confirm Password</b> fields. The <b>Bind DN</b> can be a fully qualified LDAP name (for example, <code>cn=administrator,cn=users,dc=acme,dc=local</code>) or a user principal name (for example, <code>administrator@acme.local</code>).</li><li>6. Click <b>OK</b> to save the profile.</li></ol>
---	---

**Map Users to Groups (Continued)**

**Step 2** Configure the server settings in a group mapping configuration.

1. Select **Device > User Identification > Group Mapping Settings**.
2. If the firewall has more than one virtual system (vsys), select a **Location** (vsys or Shared) for this configuration.
3. Click **Add** and enter a unique **Name** to identify the group mapping configuration.
4. Select the **LDAP Server Profile** you just created.
5. (Optional) By default, the **User Domain** field is blank: the firewall automatically detects the domain names for Active Directory (AD) servers. If you enter a value, it overrides any domain names that the firewall retrieves from the LDAP source. Your entry must be the NetBIOS domain name.
6. (Optional) To filter the groups that the firewall tracks for group mapping, in the Group Objects section, enter a **Search Filter** (LDAP query), **Object Class** (group definition), **Group Name**, and **Group Member**.
7. (Optional) To filter the users that the firewall tracks for group mapping, in the User Objects section, enter a **Search Filter** (LDAP query), **Object Class** (user definition), and **User Name**.
8. (Optional) To match User-ID information with email header information identified in the links and attachments of emails forwarded to WildFire™, enter the list of email domains in your organization in the Mail Domains section, **Domain List** field. Use commas to separate multiple domains (up to 256 characters). After you click **OK**, PAN-OS automatically populates the **Mail Attributes** field based on your LDAP server type (Sun/RFC, Active Directory, or Novell). When a match occurs, the username in the WildFire log email header section will contain a link that opens the **ACC** tab, filtered by user or user group.
9. Make sure the **Enabled** check box is selected.

**Map Users to Groups (Continued)**

<p><b>Step 3</b> Limit which groups will be available in policy rules.</p> <p>Required only if you want to limit policy rules to specific groups. By default, if you don't specify groups, all groups are available in policy rules.</p> <p> Any custom groups you create will also be available in the Allow List of authentication profiles.</p>	<ol style="list-style-type: none"><li>1. Add existing groups from the directory service:<ol style="list-style-type: none"><li>a. Select the <b>Group Include List</b> tab.</li><li>b. In the Available Groups list, select the groups you want to appear in policy rules and click the Add icon.</li></ol></li><li>2. If you want to base policy rules on user attributes that don't match existing user groups, create custom groups based on LDAP filters:<ol style="list-style-type: none"><li>a. Select the <b>Custom Group</b> tab and click <b>Add</b>.</li><li>b. Enter a group <b>Name</b> that is unique in the group mapping configuration for the current firewall or virtual system. If the <b>Name</b> has the same value as the Distinguished Name (DN) of an existing AD group domain, the firewall uses the custom group in all references to that name (for example, in policies and logs).</li><li>c. Specify an <b>LDAP Filter</b> of up to 2,048 UTF-8 characters and click <b>OK</b>. The firewall doesn't validate LDAP filters, so it's up to you to ensure they are accurate.<p> To minimize the performance impact on the LDAP directory server, use only indexed attributes in the filter.</p></li></ol></li><li>3. Click <b>OK</b> and <b>Commit</b>. A commit is necessary before custom groups will be available in policies and objects.</li></ol>
---	---

## Map IP Addresses to Users

The tasks you perform to map IP addresses to usernames depends on the type and location of the client systems on your network. Complete as many of the following tasks as necessary to enable mapping of your client systems:

- To map users as they log in to your Exchange servers, domain controllers, or eDirectory servers, or Windows clients that can be directly probed, you must configure a User-ID agent to monitor the server logs and probe client systems. You can either [Configure User Mapping Using the Windows User-ID Agent](#) (a standalone agent that you install on one or more member servers in the domain that contains the servers and clients that the agent will monitor) or [Configure User Mapping Using the PAN-OS Integrated User-ID Agent](#). For guidance on which agent is appropriate for your network and the required number and placements of agents, refer to [Architecting User Identification Deployments](#).
- If you have clients running multi-user systems in a Windows environment, such as Microsoft Terminal Server or Citrix Metaframe Presentation Server or XenApp, [Configure the Palo Alto Networks Terminal Server Agent for User Mapping](#). For a multi-user system that doesn't run on Windows, you can [Retrieve User Mappings from a Terminal Server Using the User-ID XML API](#).
- To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—[Configure User-ID to Receive User Mappings from a Syslog Sender](#). You can use either the Windows agent or the agentless user mapping feature on the firewall to listen for authentication syslog messages from the network services.
- If you have users with client systems that aren't logged into your domain servers—for example, users running Linux clients that don't log in to the domain—you can [Map IP Addresses to Usernames Using Captive Portal](#).
- For other clients that you can't map using the preceding methods, you can [Send User Mappings to User-ID Using the XML API](#).
- Because policy is local to each firewall, each firewall needs current user mapping and group mapping information to accurately enforce policy by user and group. However, if you want one firewall to function as the sole, central collection and distribution point for user mappings, you can [Configure a Firewall to Share User Mapping Data with Other Firewalls](#).

## Configure User Mapping Using the Windows User-ID Agent

In most cases, the majority of your network users will have logins to your monitored domain services. For these users, the Palo Alto Networks User-ID agent monitors the servers for login events and performs the IP address to username mapping. The way you configure the User-ID agent depends on the size of your environment and the location of your domain servers. As a best practice, you should locate your User-ID agents near your monitored servers (that is, the monitored servers and the Windows User-ID agent should not be across a WAN link from each other). This is because most of the traffic for user mapping occurs between the agent and the monitored server, with only a small amount of traffic—the delta of IP address mappings since the last update—from the agent to the firewall.

The following topics describe how to install and configure the User-ID Agent and how to configure the firewall to retrieve user mapping information from the agent:

- ▲ [Install the User-ID Agent](#)
- ▲ [Configure the User-ID Agent for User Mapping](#)

### Install the User-ID Agent

The following procedure shows how to install the User-ID agent on a member server in the domain and set up the service account with the required permissions. If you are upgrading, the installer will automatically remove the older version, however, it is a good idea to back up the config.xml file before running the installer.



For information about the system requirements for installing the Windows-based User-ID agent and for information on the supported server OS versions are supported, refer to “Operating System (OS) Compatibility User-ID Agent” in the User-ID Agent Release Notes, which are available on the Palo Alto Networks [Software Updates](#) page.

#### Install the Windows User-ID Agent

<p><b>Step 1</b> Decide where to install the User-ID agent.</p> <p>The User-ID agent queries the Domain Controller and Exchange server logs using Microsoft Remote Procedure Calls (MSRPCs), which require a complete transfer of the entire log at each query. Therefore, always install one or more User-ID agents at each site that has servers to be monitored.</p> <p> For more detailed information on where to install User-ID agents, refer to <a href="#">Architecting User Identification (User-ID) Deployments</a>.</p>	<ul style="list-style-type: none"><li>• You must install the User-ID agent on a system running one of the supported OS versions: see “Operating System (OS) Compatibility User-ID Agent” in the User-ID Agent Release Notes.</li><li>• Make sure the system that will host the User-ID agent is a member of the same domain as the servers it will monitor.</li><li>• As a best practice, install the User-ID agent close to the servers it will be monitoring (there is more traffic between the User-ID agent and the monitored servers than there is between the User-ID agent and the firewall, so locating the agent close to the monitored servers optimizes bandwidth usage).</li><li>• To ensure the most comprehensive mapping of users, you must monitor all servers that contain user login information. You might need to install multiple User-ID agents to efficiently monitor all of your resources.</li></ul>
---	---

## Install the Windows User-ID Agent (Continued)

### Step 2 Download the User-ID agent installer.

As a best practice, install the User-ID agent version that is the same as the PAN-OS version running on the firewalls.

1. Log in to [Palo Alto Networks Support](#) site.
2. Select **Software Updates** from the Manage Devices section.
3. Scroll to the User Identification Agent section of the screen and **Download** the version of the User-ID agent you want to install.
4. Save the `UaInstall-x.x.x-xx.msi` file on the system(s) where you plan to install the agent.

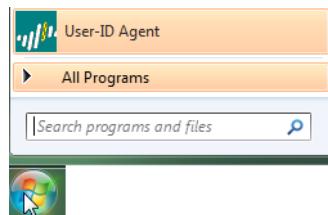
### Step 3 Run the installer as an administrator.



1. To launch a command prompt as an administrator, click Start and right-click **Command Prompt** and then select **Run as administrator**.
2. From the command line, run the .msi file you downloaded. For example, if you saved the .msi file to the Desktop you would enter the following:  

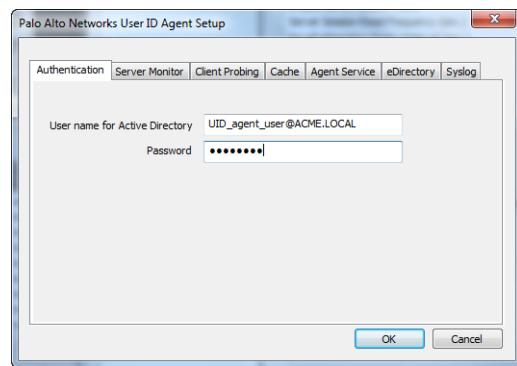
```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```
3. Follow the setup prompts to install the agent using the default settings. By default, the agent gets installed to the `C:\Program Files (x86)\Palo Alto Networks\User-ID Agent` folder, but you can **Browse** to a different location.
4. When the installation completes, **Close** the setup window.

### Step 4 Launch the User-ID Agent application.



1. Click Start and select **User-ID Agent**.

### Step 5 (Optional) Change the service account that the User-ID agent uses to log in.



By default, the agent uses the administrator account used to install the .msi file. However, you may want to switch this to a restricted account as follows:

1. Select **User Identification > Setup** and click **Edit**.
2. Select the **Authentication** tab and enter the service account name that you want the User-ID agent to use in the **User name for Active Directory** field.
3. Enter the **Password** for the specified account.

## Install the Windows User-ID Agent (Continued)

<p><b>Step 6</b> (Optional) Assign account permissions to the installation folder.</p> <p>You only need to perform this step if the service account you configured for the User-ID agent is not a member of the administrators group for the domain or a member of both the Server Operators and the Event Log Readers groups.</p>	<ol style="list-style-type: none"><li>1. Give the service account permissions to the installation folder:<ol style="list-style-type: none"><li>a. From the Windows Explorer, navigate to C:\Program Files\Palo Alto Networks and right-click the folder and select <b>Properties</b>.</li><li>b. On the <b>Security</b> tab, <b>Add</b> the User-ID agent service account and assign it permissions to <b>Modify</b>, <b>Read &amp; execute</b>, <b>List folder contents</b>, and <b>Read</b> and then click <b>OK</b> to save the account settings.</li></ol></li><li>2. Give the service account permissions to the User-ID Agent registry sub-tree:<ol style="list-style-type: none"><li>a. Run regedit32 and navigate to the Palo Alto Networks sub-tree in one of the following locations:<ul style="list-style-type: none"><li>– <b>32-bit systems</b>—HKEY_LOCAL_MACHINE\Software\Palo Alto Networks</li><li>– <b>64-bit systems</b>—HKEY_LOCAL_MACHINE\Software\WOW6432Node\Palo Alto Networks</li></ul></li><li>b. Right-click the Palo Alto Networks node and select <b>Permissions</b>.</li><li>c. Assign the User-ID service account <b>Full Control</b> and then click <b>OK</b> to save the setting.</li></ol></li><li>3. On the domain controller, add the service account to the builtin groups to enable privileges to read the security log events (Event Log Reader group) and open sessions (Server Operator group):<ol style="list-style-type: none"><li>a. Run the MMC and Launch the Active Directory Users and Computers snap-in.</li><li>b. Navigate to the Builtin folder for the domain and then right-click each group you need to edit (Event Log Reader and Server Operator) and select <b>Add to Group</b> to open the properties dialog.</li><li>c. Click <b>Add</b> and enter the name of the service account that you configured the User-ID service to use and then click <b>Check Names</b> to validate that you have the proper object name.</li><li>d. Click <b>OK</b> twice to save the settings.</li></ol></li></ol>
--	--

## Configure the User-ID Agent for User Mapping

The Palo Alto Networks User-ID agent is a Windows service that connects to servers on your network—for example, Active Directory servers, Microsoft Exchange servers, and Novell eDirectory servers—and monitors the logs for login events. The agent uses this information to map IP addresses to usernames. Palo Alto Networks firewalls connect to the User-ID agent to retrieve this user mapping information, enabling visibility into user activity by username rather than IP address and enables user- and group-based security enforcement.

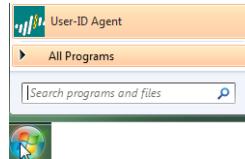


For information about the server OS versions supported by the User-ID agent, refer to “Operating System (OS) Compatibility User-ID Agent” in the *User-ID Agent Release Notes*, which are available on the Palo Alto Networks [Software Updates](#) page.

## Map IP Addresses to Users Using the User-ID Agent

**Step 1** Launch the User-ID Agent application.

1. Select **User-ID Agent** from the Windows Start menu.



**Step 2** Define the servers the User-ID agent should monitor to collect IP address to user mapping information.

The User-ID agent can monitor up to 100 servers, of which up to 50 can be syslog senders.

Keep in mind that to collect all of the required mappings, you must connect to all servers that your users log in to in order to monitor the security log files on all servers that contain login events.

1. Select **User Identification > Discovery**.
2. In the **Servers** section of the screen, click **Add**.
3. Enter a **Name** and **Server Address** for the server to be monitored. The network address can be a FQDN or an IP address.
4. Select the **Server Type (Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, or Syslog Sender)** and then click **OK** to save the server entry. Repeat this step for each server to be monitored.
5. (Optional) To enable the firewall to automatically discover domain controllers on your network using DNS lookups, click **Auto Discover**.  
 The auto-discovery locates domain controllers in the local domain only; you must manually add Exchange servers, eDirectory servers, and syslog senders.
6. (Optional) To tune the frequency at which the firewall polls configured servers for mapping information, select **User Identification > Setup** and **Edit** the Setup section. On the **Server Monitor** tab, modify the value in the **Server Log Monitor Frequency (seconds)** field. As a best practice, you should increase the value in this field to 5 seconds in environments with older Domain Controllers or high-latency links. Click **OK** to save the changes.

### Map IP Addresses to Users Using the User-ID Agent (Continued)

<p><b>Step 3</b> (Optional) If you configured the agent to connect to a Novell eDirectory server, you must specify how the agent should search the directory.</p>	<ol style="list-style-type: none"> <li>1. Select <b>User Identification &gt; Setup</b> and click <b>Edit</b> in the Setup section of the window.</li> <li>2. Select the <b>eDirectory</b> tab and then complete the following fields: <ul style="list-style-type: none"> <li>• <b>Search Base</b>—The starting point or root context for agent queries, for example: dc=domain1, dc=example, dc=com.</li> <li>• <b>Bind Distinguished Name</b>—The account to use to bind to the directory, for example: cn=admin, ou=IT, dc=domain1, dc=example, dc=com.</li> <li>• <b>Bind Password</b>—The bind account password. The agent saves the encrypted password in the configuration file.</li> <li>• <b>Search Filter</b>—The search query for user entries (default is objectClass=Person).</li> <li>• <b>Server Domain Prefix</b>—A prefix to uniquely identify the user. This is only required if there are overlapping name spaces, such as different users with the same name from two different directories.</li> <li>• <b>Use SSL</b>—Select the check box to use SSL for eDirectory binding.</li> <li>• <b>Verify Server Certificate</b>—Select the check box to verify the eDirectory server certificate when using SSL.</li> </ul> </li> </ol>
<p><b>Step 4</b> (Optional) Enable client probing.</p> <p>Client probing is useful in environments where IP addresses are not tightly bound to users because it ensures that previously mapped addresses are still valid. However, as the total number of learned IP addresses grows, so does the amount of traffic generated. As a best practice, only enable probing on network segments where IP address turnover is high.</p> <p>For more details on the placement of User-ID agents using client probing, refer to <a href="#">Architecting User Identification (User-ID) Deployments</a>.</p>	<ol style="list-style-type: none"> <li>1. On the <b>Client Probing</b> tab, select the <b>Enable WMI Probing</b> check box and/or the <b>Enable NetBIOS Probing</b> check box.</li> <li>2. Make sure the Windows firewall will allow client probing by adding a remote administration exception to the Windows firewall for each probed client.</li> </ol> <p> For NetBIOS probing to work effectively, each probed client PC must allow port 139 in the Windows firewall and must also have file and printer sharing services enabled. WMI probing is always preferred over NetBIOS whenever possible.</p>
<p><b>Step 5</b> Save the configuration.</p>	<p>Click <b>OK</b> to save the User-ID agent setup settings and then click <b>Commit</b> to restart the User-ID agent and load the new settings.</p>

### Map IP Addresses to Users Using the User-ID Agent (Continued)

<p><b>Step 6</b> (Optional) Define the set of users for which you do not need to provide IP address-to-user name mappings, such as kiosk accounts.</p> <p> You can also use the <code>ignore-user</code> list to identify users whom you want to force to authenticate using Captive Portal.</p>	<p>Create an <code>ignore_user_list.txt</code> file and save it to the User-ID Agent folder on the domain server where the agent is installed. List the user accounts to ignore; there is no limit to the number of accounts you can add to the list. Each user account name must be on a separate line. For example:</p> <pre>SPAdmin SPInstall TFSReport</pre> <p>You can use an asterisk as a wildcard character to match multiple usernames, but only as the last character in the entry. For example, <code>corpdomain\it-admin*</code> would match all administrators in the <code>corpdomain</code> domain whose usernames start with the string <code>it-admin</code>.</p>
<p><b>Step 7</b> Configure the firewalls to connect to the User-ID agent.</p>	<p>Complete the following steps on each firewall you want to connect to the User-ID agent to receive user mappings:</p> <ol style="list-style-type: none"> <li>1. Select <b>Device &gt; User Identification &gt; User-ID Agents</b> and click <b>Add</b>.</li> <li>2. Enter a <b>Name</b> for the User-ID agent.</li> <li>3. Enter the IP address of the Windows <b>Host</b> on which the User-ID Agent is installed.</li> <li>4. Enter the <b>Port</b> number (1-65535) on which the agent will listen for user mapping requests. This value must match the value configured on the User-ID agent. By default, the port is set to 5007 on the firewall and on newer versions of the User-ID agent. However, some older User-ID agent versions use port 2010 as the default.</li> <li>5. Make sure that the configuration is <b>Enabled</b>, then click <b>OK</b>.</li> <li>6. <b>Commit</b> the changes.</li> <li>7. Verify that the <b>Connected status</b> displays as connected (a green light).</li> </ol>
<p><b>Step 8</b> Verify that the User-ID agent is successfully mapping IP addresses to usernames and that the firewalls can connect to the agent.</p>	<ol style="list-style-type: none"> <li>1. Launch the User-ID agent and select <b>User Identification</b>.</li> <li>2. Verify that the agent status shows <b>Agent is running</b>. If the Agent is not running, click <b>Start</b>.</li> <li>3. To verify that the User-ID agent can connect to monitored servers, make sure the Status for each Server is <b>Connected</b>.</li> <li>4. To verify that the firewalls can connect to the User-ID agent, make sure the Status for each of the Connected Devices is <b>Connected</b>.</li> <li>5. To verify that the User-ID agent is mapping IP addresses to usernames, select <b>Monitoring</b> and make sure that the mapping table is populated. You can also <b>Search</b> for specific users, or <b>Delete</b> user mappings from the list.</li> </ol>

## Configure User Mapping Using the PAN-OS Integrated User-ID Agent

The following procedure shows how to configure the PAN-OS integrated agent on the firewall for user mapping. The integrated User-ID agent performs the same tasks as the Windows-based agent with the exception of NetBIOS client probing (WMI probing is supported).

### Map IP Addresses to Users Using the Integrated User-ID Agent

<b>Step 1</b>	<p>Create an Active Directory (AD) account for the User-ID agent.</p> <p>The account must have the privilege levels required to log in to each service or host that the User-ID agent will monitor to collect user mapping data.</p>	<ul style="list-style-type: none"><li><b>Windows 2008 or later domain servers</b>—Add the account to the Event Log Readers group. If you are using the on-device User-ID agent, the account must also be a member of the Distributed COM Users Group.</li><li><b>Windows 2003 domain servers</b>—Assign Manage Auditing and Security Logs permissions through group policy.</li><li><b>WMI probing</b>—Make sure the account has rights to read the CIMV2 namespace; by default, Domain Administrator and Server Operator accounts have this permission.</li><li><b>NTLM authentication</b>—Because the firewall must join the domain if you are using Captive Portal NTLM authentication with an on-device User-ID agent, the Windows account you create for NTLM access must have administrative privileges. Note that due to AD restrictions on virtual systems running on the same host, if the firewall has multiple virtual systems, only vsys1 will be able to join the domain.</li></ul>
---------------	--	--

### Map IP Addresses to Users Using the Integrated User-ID Agent (Continued)

- Step 2** Define the servers that the firewall will monitor to collect IP address-to-user mapping information.

Within the total maximum of 100 monitored servers per firewall, you can define no more than 50 syslog senders for any single virtual system.

Note that to collect all the required mappings, the firewall must connect to all servers that your users log in to so it can monitor the security log files on all servers that contain login events.

- Select **Device > User Identification > User Mapping**.
- In the Server Monitoring section of the screen, click **Add**.
- Enter a **Name** and **Network Address** for the server. The network address can be a FQDN or an IP address.
- Select the **Type** of server.
- Make sure the **Enabled** check box is selected and then click **OK**.
- (Optional) To enable the firewall to automatically discover domain controllers on your network using DNS lookups, click **Discover**.



The auto-discovery feature is for domain controllers only; you must manually add any Exchange servers or eDirectory servers you want to monitor.

- (Optional) Specify the frequency at which the firewall polls Windows servers for mapping information. This is the interval between the end of the last query and the start of the next query.

If the query load is high, the observed delay between queries might significantly exceed the specified frequency.

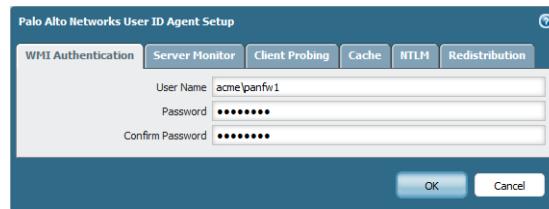
- In the **Palo Alto Networks User ID Agent Setup** section, click the Edit icon.
- Select the **Server Monitor** tab and specify the **Server Log Monitor Frequency** in seconds (default is 2, range is 1-3600).

As a best practice, increase the value in this field to 5 seconds in environments with older domain controllers or high-latency links.

- Click **OK** to save the changes.

- Step 3** Set the domain credentials for the account the firewall will use to access Windows resources. This is required for monitoring Exchange servers and domain controllers as well as for WMI probing.

- Edit the Palo Alto Networks User ID Agent Setup section of the screen.
- On the **WMI Authentication** tab, enter the **User Name** and **Password** for the account that will be used to probe the clients and monitor servers. Enter the user name using the domain\username syntax.



<b>Map IP Addresses to Users Using the Integrated User-ID Agent (Continued)</b>	
<b>Step 4</b> (Optional) Enable WMI probing.	<p>1. On the <b>Client Probing</b> tab, select the <b>Enable Probing</b> check box.</p> <p>2. (Optional) If necessary, modify the <b>Probe Interval</b> (in minutes) to ensure it is long enough for the User-ID agent to probe all the learned IP addresses (default is 20, range is 1-1440). This is the interval between the end of the last probe request and the start of the next request.</p> <p>If the request load is high, the observed delay between requests might significantly exceed the specified interval.</p> <p>3. Make sure the Windows firewall will allow client probing by adding a remote administration exception to the Windows firewall for each probed client.</p>
<b>Step 5</b> Save the configuration.	<p>1. Click <b>OK</b> to save the User-ID agent setup settings.</p> <p>2. Click <b>Commit</b> to save the configuration.</p>
<b>Step 6</b> (Optional) Define the set of users for which you do not need to provide IP address-to-user name mappings, such as kiosk accounts.	<p>1. Open a CLI session to the firewall.</p> <p>2. To add the list of user accounts for which you do not want the firewall to perform mapping, run the following command:</p> <pre>set user-id-collector ignore-user &lt;value&gt;</pre> <p>where &lt;value&gt; is a list of the user accounts to ignore; there is no limit to the number of accounts you can add to the list. Separate entries with a space and do not include the domain name with the username. For example:</p> <pre>set user-id-collector ignore-user SPAdmin SPIInstall TFSReport</pre> <p>3. <b>Commit</b> your changes.</p>
<b>Step 7</b> Verify the configuration.	<p>1. From the CLI, enter the following command:</p> <pre>show user server-monitor state all</pre> <p>2. On the <b>Device &gt; User Identification &gt; User Mapping</b> tab in the web interface, verify that the <b>Status</b> of each server you configured for server monitoring is <b>Connected</b>.</p>

## Configure User-ID to Receive User Mappings from a Syslog Sender

The following topics describe how to configure the User-ID agent (either the Windows agent or the integrated agent on the firewall) as a [Syslog](#) listener:

- ▲ [Configure the Integrated User-ID Agent as a Syslog Listener](#)
- ▲ [Configure the Windows User-ID Agent as a Syslog Listener](#)

### Configure the Integrated User-ID Agent as a Syslog Listener

The following workflow describes how to configure the PAN-OS integrated User-ID agent to receive syslog messages from authenticating services.



The PAN-OS integrated User-ID agent accepts syslogs over SSL and UDP only. However, you must use caution when using UDP to receive syslog messages because it is an unreliable protocol and as such there is no way to verify that a message was sent from a trusted syslog server. Although you can restrict syslog messages to specific source IP addresses, an attacker can still spoof the IP address, potentially allowing the injection of unauthorized syslog messages into the firewall. As a best practice, always use SSL to listen for syslog messages. However, if you must use UDP, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending UDP traffic to the firewall.

#### Collect User Mappings from Syslog Senders

**Step 1** Determine whether there is a pre-defined syslog filter for your particular syslog sender(s).

Palo Alto Networks provides several pre-defined syslog filters, which are delivered as Application content updates and are therefore updated dynamically as new filters are developed. The pre-defined filters are global to the firewall, whereas manually-defined filters apply to a single virtual system only.



Any new syslog filters in a given content release will be documented in the corresponding release note along with the specific regex used to define the filter.

1. Verify that your Application or Application and Threat database is up to date:
  - a. Select **Device > Dynamic Updates**.
  - b. Click **Check Now** (located in the lower left-hand corner of the window) to check for the latest updates.
  - c. If a new update is available, **Download** and **Install** it.
2. Check to see what pre-defined filters are available:
  - a. Select **Device > User Identification > User Mapping**.
  - b. In the Server Monitoring section of the screen, click **Add**.
  - c. Select **Syslog Sender** as the server **Type**.
  - d. Select the **Filter** drop-down and check to see if there is a filter for the manufacturer and product you plan to forward syslogs from. If the filter you need is available, skip to [Step 5](#) for instructions on defining the servers. If the filter you need is not available, continue to [Step 2](#).

**Collect User Mappings from Syslog Senders (Continued)**

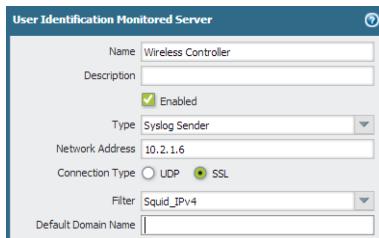
<p><b>Step 2</b> Manually define syslog filter(s) for extracting the User-ID IP address to username mapping information from syslog messages.</p> <p>In order to be parsed by the User-ID agent, syslog messages must meet the following criteria:</p> <ul style="list-style-type: none"><li>• Each syslog message must be a single-line text string. Line breaks are delimited by a carriage return and a new line (\r\n) or a new line (\n).</li><li>• The maximum allowed size of an individual syslog message is 2048 bytes.</li><li>• Syslog messages sent over UDP must be contained in a single packet; messages sent over SSL can span multiple packets.</li><li>• A single packet may contain multiple syslog messages.</li></ul>	<ol style="list-style-type: none"><li>1. Review the syslogs generated by the authenticating service to identify the syntax of the login events. This enables you to create the matching patterns that will allow the firewall to identify and extract the authentication events from the syslogs.</li><li>2. Select <b>Device &gt; User Identification &gt; User Mapping</b> and edit the Palo Alto Networks User-ID Agent Setup section.</li><li>3. On the <b>Syslog Filters</b> tab, <b>Add</b> a new syslog parse profile.</li><li>4. Enter a name for the <b>Syslog Parse Profile</b>.</li><li>5. Specify the <b>Type</b> of parsing to use to filter out the user mapping information by selecting one of the following options:<ul style="list-style-type: none"><li>• <b>Regex Identifier</b>—With this type of parsing, you specify regular expressions to describe search patterns for identifying and extracting user mapping information from syslog messages. Continue to <a href="#">Step 3</a> for instructions on creating the regex identifiers.</li><li>• <b>Field Identifier</b>—With this type of parsing, you specify a string to match the authentication event, and prefix and suffix strings to identify the user mapping information in the syslogs. Continue to <a href="#">Step 4</a> for instructions on creating the field identifiers.</li></ul></li></ol>
--	---

### Collect User Mappings from Syslog Senders (Continued)

**Step 3** If you selected **Regex Identifier** as the parsing **Type**, create the regex matching patterns for identifying the authentication events and extracting the user mapping information.

The example below shows a regex configuration for matching syslog messages with the following format:

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator
authentication success User:johndoe1
Source:192.168.3.212
```



If the syslog contains a standalone space and/or tab as a delimiter, you must use an \s (for a space) and/or \t (for a tab) in order for the agent to parse the syslog.

**1.** Specify how to match successful authentication events in the syslogs by entering a matching pattern in the **Event Regex** field. For example, when matched against the example syslog message, the following regex instructs the firewall to extract the first {1} instance of the string authentication success. The backslash before the space is a standard regex escape character that instructs the regex engine not to treat the space as a special character: (authentication\ success){1}.

**2.** Enter the regex for identifying the beginning of the username in the authentication success messages in the **Username Regex** field. For example, the regex User:( [a-zA-Z0-9\\\\.\\\_]+) would match the string User: johndoe1 in the example message and extract acme\\johndoe1 as the User-ID.



If the syslogs do not contain domain information and you require domain names in your user mappings, be sure to enter the **Default Domain Name** when defining the monitored server entry in **Step 5**.

**3.** Enter the regex for identifying the IP address portion of the authentication success messages in the **Address Regex** field. For example, the following regular expression Source:( [0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}) would match an IPv4 address (Source:192.168.0.212 in the example syslog).

**4.** Click **OK**.

### Collect User Mappings from Syslog Senders (Continued)

<p><b>Step 4</b> If you selected <b>Field Identifier</b> as the parsing <b>Type</b>, define the string matching patterns for identifying the authentication events and extracting the user mapping information.</p> <p>The example below shows a field identifier configuration for matching syslog messages with the following format:</p>	<ol style="list-style-type: none"> <li>1. Specify how to match successful authentication events in the syslogs by entering a matching pattern in the <b>Event String</b> field. For example, when matched against the sample syslog message, you would enter the string <code>authentication success</code> to identify authentication events in the syslog.</li> <li>2. Enter the matching string for identifying the beginning of the username field within the authentication syslog message in the <b>Username Prefix</b> field. For example, the string <code>User:</code> identifies the beginning of the username field in the sample syslog.</li> <li>3. Enter the <b>Username Delimiter</b> to mark the end of the username field within an authentication syslog message. For example, if the username is followed by a space, you would enter <code>\s</code> to indicate that the username field is delimited by a standalone space in the sample log.</li> <li>4. Enter the matching string for identifying the beginning of the IP address field within the authentication event log in the <b>Address Prefix</b> field. For example, the string <code>Source:</code> identifies the beginning of the address field in the example log.</li> <li>5. Enter the <b>Address Delimiter</b> to mark the end of the IP address field within the authentication success message within the field. For example, if the address is followed by a line break, you would enter <code>\n</code> to indicate that the address field is delimited by a new line.</li> <li>6. Click <b>OK</b>.</li> </ol>
<p><b>Step 5</b> Define the servers that will send syslog messages to the firewall for user mapping purposes.</p> <p>Within the total maximum of 100 monitored servers per firewall, you can define no more than 50 syslog senders for any single virtual system.</p> <p>The firewall will discard any syslog messages received from servers that are not on this list.</p> <p> A Syslog sender using SSL to connect will only show a <b>Status</b> of <b>Connected</b> when there is an active SSL connection. Syslog senders using UDP will not show a <b>Status</b> value.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; User Identification &gt; User Mapping</b>.</li> <li>2. In the Server Monitoring section of the screen, click <b>Add</b>.</li> <li>3. Enter a <b>Name</b> and <b>Network Address</b> for the server.</li> <li>4. Select <b>Syslog Sender</b> as the server <b>Type</b>.</li> <li>5. Make sure the <b>Enabled</b> check box is selected.</li> <li>6. (Optional) If the syslogs that the authenticating device sends do not include domain information in the login event logs, enter the <b>Default Domain Name</b> to append to the user mappings.</li> <li>7. Click <b>OK</b> to save the settings.</li> </ol>

**Collect User Mappings from Syslog Senders (Continued)**

<p><b>Step 6</b> Enable syslog listener services in the management profile associated with the interface used for user mapping.</p> <p> Use caution when using UDP to receive syslog messages because it is an unreliable protocol and as such there is no way to verify that a message was sent from a trusted syslog server. Although you can restrict syslog messages to specific source IP addresses, an attacker can still spoof the IP address, potentially allowing the injection of unauthorized syslog messages into the firewall. As a best practice, always use SSL to listen for syslog messages when using agentless User Mapping on a firewall. However, if you must use UDP, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending UDP traffic to the firewall.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b> and then select an Interface Management profile to edit or click <b>Add</b> to create a new profile.</li><li>2. Select <b>User-ID Syslog Listener-SSL</b> and/or <b>User-ID Syslog Listener-UDP</b>, depending on the protocols you defined when you set up your syslog senders in the Server Monitor list.  On the Windows User-ID agent, the default listening port for syslog over UDP or TCP is 514, but the port value is configurable. For the agentless User Mapping feature on the firewall, only syslog over UDP and SSL are supported and the listening ports (514 for UDP and 6514 for SSL) are not configurable; they are enabled through the management service only.</li><li>3. Click <b>OK</b> to save the interface management profile.  Even after enabling the User-ID Syslog Listener service on the interface, the interface will only accept syslog connections from servers that have a corresponding entry in the User-ID monitored servers configuration. Connections or messages from servers that are not on the list will be discarded.</li></ol>
<p><b>Step 7</b> Save the configuration.</p>	<p>Click <b>Commit</b> to save the configuration.</p>

### Collect User Mappings from Syslog Senders (Continued)

**Step 8** Verify the configuration by opening an SSH connection to the firewall and then running the following CLI commands:

To see the status of a particular syslog sender:

```
admin@PA-5050> show user server-monitor state Syslog2
  UDP Syslog Listener Service is enabled
  SSL Syslog Listener Service is enabled

Proxy: Syslog2(vsys: vsys1)      Host: Syslog2(10.5.204.41)
  number of log messages          : 1000
  number of auth. success messages: 1000
  number of active connections    : 0
  total connections made         : 4
```

To see how many log messages came in from syslog senders and how many entries were successfully mapped:

```
admin@PA-5050> show user server-monitor statistics
```

Directory Servers:				
Name	Type	Host	Vsys	Status
AD	AD	10.2.204.43	vsys1	Connected

Syslog Servers:				
Name	Connection	Host	Vsys	Status
Syslog1	UDP	10.5.204.40	vsys1	N/A
Syslog2	SSL	10.5.204.41	vsys1	Not connected

To see how many user mappings were discovered through syslog senders:

```
admin@PA-5050> show user ip-user-mapping all type SYSLOG
IP           Vsys   From       User           IdleTimeout(s) M
axTimeout(s)
----- -----
192.168.3.8  vsys1  SYSLOG   acme\jreddick     2476        2
476
192.168.5.39 vsys1  SYSLOG   acme\jdonaldson   2480        2
480
192.168.2.147 vsys1  SYSLOG   acme\ccrisp      2476        2
476
192.168.2.175 vsys1  SYSLOG   acme\jjaso       2476        2
476
192.168.4.196 vsys1  SYSLOG   acme\jblevins    2480        2
480
192.168.4.103 vsys1  SYSLOG   acme\bmoss       2480        2
480
192.168.2.193 vsys1  SYSLOG   acme\esogard     2476        2
476
192.168.2.119 vsys1  SYSLOG   acme\acallaspo   2476        2
476
192.168.3.176 vsys1  SYSLOG   acme\jlowrie     2478        2
478

Total: 9 users
```

## Configure the Windows User-ID Agent as a Syslog Listener

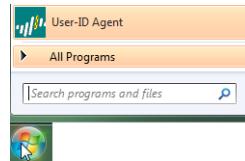
The following workflow describes how to configure a Windows-based User-ID agent to listen for syslogs from authenticating services.

**!** The Windows User-ID agent accepts syslogs over TCP and UDP only. However, you must use caution when using UDP to receive syslog messages because it is an unreliable protocol and as such there is no way to verify that a message was sent from a trusted syslog server. Although you can restrict syslog messages to specific source IP addresses, an attacker can still spoof the IP address, potentially allowing the injection of unauthorized syslog messages into the firewall. As a best practice, use TCP instead of UDP. In either case, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending syslogs to the User-ID agent.

## Configure the Windows User-ID Agent to Collect User Mappings from Syslog Senders

**Step 1** Launch the User-ID Agent application.

**1.** Click Start and select **User-ID Agent**.



**Step 2** Manually define syslog filter(s) for extracting the User-ID IP address to username mapping information from syslog messages.

In order to be parsed by the User-ID agent, syslog messages must meet the following criteria:

- Each syslog message must be a single-line text string. Line breaks are delimited by a carriage return and a new line (\r\n) or a new line (\n).
- The maximum allowed size of an individual syslog message is 2048 bytes.
- Syslog messages sent over UDP must be contained in a single packet; messages sent over SSL can span multiple packets.
- A single packet may contain multiple syslog messages.

**1.** Review the syslogs generated by the authenticating service to identify the syntax of the login events. This enables you to create the matching patterns that will allow the firewall to identify and extract the authentication events from the syslogs.

While reviewing the syslogs, also determine whether the domain name is included in the log entries. If the authentication logs do not contain domain information, consider defining a default domain name when adding the syslog sender to the monitored servers list in [Step 5](#).

**2.** Select **User Identification > Setup** and click **Edit** in the Setup section of the dialog.

**3.** On the **Syslog** tab, **Add** a new syslog parse profile.

**4.** Enter a **Profile Name** and **Description**.

**5.** Specify the **Type** of parsing to use to filter out the user mapping information by selecting one of the following options:

- **Regex**—With this type of parsing, you specify regular expressions to describe search patterns for identifying and extracting user mapping information from syslog messages. Continue to [Step 3](#) for instructions on creating the regex identifiers.

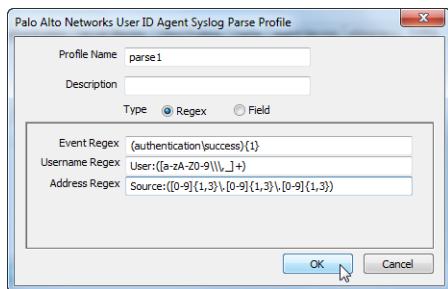
- **Field**—With this type of parsing, you specify a sting to match the authentication event, and prefix and suffix strings to identify the user mapping information in the syslogs. Continue to [Step 4](#) for instructions on creating the field identifiers.

### Configure the Windows User-ID Agent to Collect User Mappings from Syslog Senders (Continued)

**Step 3** If you selected **Regex** as the parsing **Type**, create the regex matching patterns for identifying the authentication events and extracting the user mapping information.

The example below shows a regex configuration for matching syslog messages with the following format:

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:john Doe1
Source:192.168.3.212
```



If the syslog contains a standalone space and/or tab as a delimiter, you must use an \s (for a space) and/or \t (for a tab) in order for the agent to parse the syslog.

- Specify how to match successful authentication events in the syslogs by entering a matching pattern in the **Event Regex** field. For example, when matched against the example syslog message, the following regex instructs the firewall to extract the first {1} instance of the string authentication success. The backslash before the space is a standard regex escape character that instructs the regex engine not to treat the space as a special character: (authentication\ success){1}.

- Enter the regex for identifying the beginning of the username in the authentication success messages in the **Username Regex** field. For example, the regex User:([a-zA-Z0-9\\\\.]+) would match the string User: john Doe1 in the example message and extract acme\\john Doe1 as the User-ID.



If the syslogs do not contain domain information and you require domain names in your user mappings, be sure to enter the **Default Domain Name** when defining the monitored server entry in **Step 5**.

- Enter the regex for identifying the IP address portion of the authentication success messages in the **Address Regex** field. For example, the following regular expression Source:([0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}) would match an IPv4 address (Source:192.168.0.212 in the example syslog).

- Click **OK** to save the profile.

### Configure the Windows User-ID Agent to Collect User Mappings from Syslog Senders (Continued)

<p><b>Step 4</b> If you selected <b>Field Identifier</b> as the parsing <b>Type</b>, define the string matching patterns for identifying the authentication events and extracting the user mapping information.</p> <p>The example below shows a field identifier configuration for matching syslog messages with the following format:</p>	<ol style="list-style-type: none"> <li>Specify how to match successful authentication events in the syslogs by entering a matching pattern in the <b>Event String</b> field. For example, when matched against the sample syslog message, you would enter the string <code>authentication success</code> to identify authentication events in the syslog.</li> <li>Enter the matching string for identifying the beginning of the username field within the authentication syslog message in the <b>Username Prefix</b> field. For example, the string <code>User:</code> identifies the beginning of the username field in the sample syslog.</li> <li>Enter the <b>Username Delimiter</b> to mark the end of the username field within an authentication syslog message. For example, if the username is followed by a space, you would enter <code>\s</code> to indicate that the username field is delimited by a standalone space in the sample log.</li> <li>Enter the matching string for identifying the beginning of the IP address field within the authentication event log in the <b>Address Prefix</b> field. For example, the string <code>Source:</code> identifies the beginning of the address field in the example log.</li> <li>Enter the <b>Address Delimiter</b> to mark the end of the IP address field within the authentication success message within the field. For example, if the address is followed by a line break, you would enter <code>\n</code> to indicate that the address field is delimited by a new line.</li> <li>Click <b>OK</b> to save the profile.</li> </ol>
<p><b>Step 5</b> Enable the syslog listening service on the agent.</p> <p> As a best practice, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending syslogs to the User-ID agent.</p>	<ol style="list-style-type: none"> <li>Select the <b>Enable Syslog Service</b> check box.</li> <li>(Optional) Modify the <b>Syslog Service Port</b> number to match the port number used by the syslog sender (default=514).</li> <li>To save the agent syslog configuration, click <b>OK</b>.</li> </ol>
<p><b>Step 6</b> Define the servers that will send syslog messages to the User-ID agent.</p> <p>Within the total maximum of 100 servers of all types that the User-ID agent can monitor, up to 50 can be syslog senders. The User-ID agent will discard any syslog messages received from servers that are not on this list.</p>	<ol style="list-style-type: none"> <li>Select <b>User Identification &gt; Discovery</b>.</li> <li>In the <b>Servers</b> section of the screen, click <b>Add</b>.</li> <li>Enter a <b>Name</b> and <b>Server Address</b> for the server that will send syslogs to the agent.</li> <li>Select <b>Syslog Sender</b> as the <b>Server Type</b>.</li> <li>Select a <b>Filter</b> you defined in <b>Step 2</b>.</li> <li>(Optional) If the syslogs that the authenticating device sends do not include domain information in the login event logs, enter the <b>Default Domain Name</b> to append to the user mappings.</li> <li>Click <b>OK</b> to save the settings.</li> </ol>
<p><b>Step 7</b> Save the configuration.</p>	<p>Click <b>Commit</b> to save the configuration.</p>

### Configure the Windows User-ID Agent to Collect User Mappings from Syslog Senders (Continued)

**Step 8** Verify the configuration by opening an SSH connection to the firewall and then running the following CLI commands:

To see the status of a particular syslog sender:

```
admin@PA-5050> show user server-monitor state Syslog2
  UDP Syslog Listener Service is enabled
  SSL Syslog Listener Service is enabled

Proxy: Syslog2(vsys: vsys1)      Host: Syslog2(10.5.204.41)
  number of log messages          : 1000
  number of auth. success messages: 1000
  number of active connections    : 0
  total connections made         : 4
```

To see how many log messages came in from syslog senders and how many entries were successfully mapped:

```
admin@PA-5050> show user server-monitor statistics
```

Directory Servers:		TYPE	Host	Vsys	Status
AD	AD	10.2.204.43	vsys1	Connected	

Syslog Servers:		Connection	Host	Vsys	Status
Syslog1	UDP	10.5.204.40	vsys1	N/A	
Syslog2	SSL	10.5.204.41	vsys1	Not connected	

To see how many user mappings were discovered through syslog senders:

```
admin@PA-5050> show user ip-user-mapping all type SYSLOG
IP           Vsys   From       User           IdleTimeout(s)  M
axTimeout(s)
----- -----
192.168.3.8  vsys1  SYSLOG   acme\jreddick    2476          2
476
192.168.5.39 vsys1  SYSLOG   acme\jdonaldson  2480          2
480
192.168.2.147 vsys1  SYSLOG   acme\ccrisp     2476          2
476
192.168.2.175 vsys1  SYSLOG   acme\jjaso      2476          2
476
192.168.4.196 vsys1  SYSLOG   acme\jblevins   2480          2
480
192.168.4.103 vsys1  SYSLOG   acme\bmoss      2480          2
480
192.168.2.193 vsys1  SYSLOG   acme\esogard     2476          2
476
192.168.2.119 vsys1  SYSLOG   acme\acallaspo   2476          2
476
192.168.3.176 vsys1  SYSLOG   acme\jlowrie    2478          2
478
Total: 9 users
```

## Map IP Addresses to Usernames Using Captive Portal

If the firewall receives a request from a security zone that has User-ID enabled and the source IP address does not have any user data associated with it yet, the firewall checks its Captive Portal policy rules for a match to determine whether to perform authentication. This is useful in environments where you have clients that are not logged in to your domain servers, such as Linux clients. The firewall triggers this user mapping method only for web traffic (HTTP or HTTPS) that matches a Captive Portal rule but has not been mapped using a different method.

- ▲ [Captive Portal Authentication Methods](#)
- ▲ [Captive Portal Modes](#)
- ▲ [Configure Captive Portal](#)

### Captive Portal Authentication Methods

Captive Portal uses the following methods to obtain user information from the client when a web request matches a Captive Portal rule:

Authentication Method	Description
Kerberos SSO	<p>The firewall uses <a href="#">Kerberos Single Sign-On (SSO)</a> to transparently obtain user credentials. To use this method, your network requires a Kerberos infrastructure, including a key distribution center (KDC) with an authentication server and ticket granting service. The firewall must have a Kerberos account, including a principal name and password.</p> <p>If Kerberos SSO authentication fails, the firewall falls back to <a href="#">NT LAN Manager (NTLM)</a> authentication. If you don't configure NTLM, or NTLM authentication fails, the firewall falls back to web form or client certificate authentication, depending on your Captive Portal configuration.</p>
NT LAN Manager (NTLM)	<p>The firewall uses an encrypted challenge-response mechanism to obtain the user credentials from the browser. When configured properly, the browser will transparently provide the credentials to the firewall without prompting the user, but will prompt for credentials if necessary.</p> <p>If you use the Windows-based User-ID agent, NTLM responses go directly to the domain controller where you installed the agent.</p> <p>If you configure Kerberos SSO authentication, the firewall tries that method first before falling back to NTLM authentication. If the browser can't perform NTLM or if NTLM authentication fails, the firewall falls back to web form or client certificate authentication, depending on your Captive Portal configuration.</p> <p>Microsoft Internet Explorer supports NTLM by default. You can configure Mozilla Firefox and Google Chrome to also use NTLM but you can't use NTLM to authenticate non-Windows clients.</p>

Authentication Method	Description
Web Form	The firewall redirects web requests to a web form for authentication. You can configure Captive Portal to use a local user database, RADIUS server, TACACS+ server, LDAP server, or Kerberos server to authenticate users. Although the firewall always prompts users for credentials, this method works with all browsers and operating systems.
Client Certificate Authentication	The firewall prompts the browser to present a valid client certificate to authenticate the user. To use this method, you must provision client certificates on each user system and install the trusted certificate authority (CA) certificate used to issue those certificates on the firewall.

## Captive Portal Modes

The Captive Portal mode defines how the firewall captures web requests for authentication:

Mode	Description
Transparent	The firewall intercepts the browser traffic per the Captive Portal rule and impersonates the original destination URL, issuing an HTTP 401 to invoke authentication. However, because the firewall does not have the real certificate for the destination URL, the browser displays a certificate error to users attempting to access a secure site. Therefore, you should only use this mode when absolutely necessary, such as in Layer 2 or virtual wire deployments.
Redirect	The firewall intercepts unknown HTTP or HTTPS sessions and redirects them to a Layer 3 interface on the firewall using an HTTP 302 redirect to perform authentication. This is the preferred mode because it provides a better end-user experience (no certificate errors). However, it does require additional Layer 3 configuration. Another benefit of the Redirect mode is that it provides for the use of session cookies, which enable the user to continue browsing to authenticated sites without requiring re-mapping each time the time outs expire. This is especially useful for users who roam from one IP address to another (for example, from the corporate LAN to the wireless network) because they won't need to re-authenticate when the IP address changes as long as the session stays open.  If you use Kerberos SSO or NTLM authentication, you must use Redirect mode because the browser will provide credentials only to trusted sites.

## Configure Captive Portal

The following procedure shows how to configure Captive Portal using the PAN-OS integrated User-ID agent to redirect web requests that match a Captive Portal rule to a redirect host. A redirect host is the intranet hostname (a hostname with no period in its name) that resolves to the IP address of the Layer 3 interface on the firewall to which the firewall will redirect requests.



If you use Captive Portal without the other User-ID functions (user mapping and group mapping), you don't need to configure a User-ID agent.

## Configure Captive Portal Using the PAN-OS Integrated User-ID Agent

<p><b>Step 1</b> Configure the interfaces that the firewall will use for redirecting web requests, authenticating users, and communicating with directory servers to map usernames to IP addresses.</p> <p>The firewall uses the management (MGT) interface for all these functions by default, but you can configure other interfaces. In redirect mode, you must use a Layer 3 interface for redirecting requests.</p>	<ol style="list-style-type: none"> <li>1. (MGT interface only) Select <b>Device &gt; Setup &gt; Management</b>, edit the Management Interface Settings, select the <b>User ID</b> check box, and click <b>OK</b>.</li> <li>2. (Non-MGT interface only) Assign an Interface Management profile to the Layer 3 interface that the firewall will use to redirect web requests and/or communicate with directory servers.             <ol style="list-style-type: none"> <li>a. Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b> and <b>Add</b> an Interface Management profile with a unique <b>Name</b>.</li> <li>b. Select the <b>Response Pages</b> and <b>User ID</b> check boxes, and click <b>OK</b>.</li> <li>c. Select <b>Network &gt; Interfaces</b>, click the interface, select the <b>Advanced</b> tab, select the Interface <b>Management Profile</b> you just created, and click <b>OK</b>.</li> </ol> </li> <li>3. (Non-MGT interface only) <a href="#">Configure a service route</a> for the interface that the firewall will use to authenticate users. If the firewall has more than one virtual system (vsys), the service route can be global or vsys-specific. The services must include <b>LDAP</b> and potentially the following:             <ul style="list-style-type: none"> <li>– <b>Kerberos, RADIUS, or TACACS+</b>—Configure a service route for one of these services only if you will use it for external authentication.</li> <li>– <b>UID Agent</b>—Configure this service only if you will enable <a href="#">NT LAN Manager (NTLM)</a> authentication or if you will <a href="#">Configure a Firewall to Share User Mapping Data with Other Firewalls</a>.</li> </ul> </li> <li>4. (Redirect mode only) Create a DNS address (A) record that maps the IP address on the Layer 3 interface to the redirect host. If you will use Kerberos SSO, you must also add a DNS pointer (PTR) record that performs the same mapping.</li> </ol> <p>If your network doesn't support access to the directory servers from any firewall interface, you must <a href="#">Configure User Mapping Using the Windows User-ID Agent</a>.</p>
<p><b>Step 2</b> Make sure Domain Name System (DNS) is configured to resolve your domain controller addresses.</p>	<p>To verify proper resolution, ping the server FQDN. For example:  <code>admin@PA-200&gt; ping host dc1.acme.com</code></p>
<p><b>Step 3</b> Create a Kerberos keytab for the redirect host.  Required for <a href="#">Kerberos SSO</a> authentication.</p>	<p><a href="#">Create a Kerberos keytab</a>. A keytab is a file that contains Kerberos account information (principal name and hashed password) for the redirect host (the firewall).  To support Kerberos SSO, your network must have a Kerberos infrastructure, including a key distribution center (KDC) with an authentication server and ticket granting service.</p>

**Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)**

<b>Step 4</b> Configure clients to trust Captive Portal certificates.  Required for redirect mode—to transparently redirect users without displaying certificate errors. You can generate a self-signed certificate or import a certificate that an external certificate authority (CA) signed.	To use a self-signed certificate, create a root CA certificate and use it to sign the certificate you will use for Captive Portal: <ol style="list-style-type: none"><li>1. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b>.</li><li>2. <a href="#">Create a Self-Signed Root CA Certificate</a> or import a CA certificate (see <a href="#">Import a Certificate and Private Key</a>).</li><li>3. <a href="#">Generate a Certificate on the Device</a> to use for Captive Portal. Be sure to configure the following fields:<ul style="list-style-type: none"><li>• <b>Common Name</b>—Enter the DNS name of the intranet host for the Layer 3 interface.</li><li>• <b>Signed By</b>—Select the CA certificate you just created or imported.</li><li>• Certificate Attributes—Click <b>Add</b>, for the <b>Type</b> select <b>IP</b> and, for the <b>Value</b>, enter the IP address of the Layer 3 interface to which the firewall will redirect requests.</li></ul></li><li>4. <a href="#">Configure an SSL/TLS Service Profile</a>. Assign the Captive Portal certificate you just created to the profile.</li><li>5. Configure clients to trust the certificate:<ol style="list-style-type: none"><li>a. <a href="#">Export the CA certificate</a> you created or imported.</li><li>b. Import the certificate as a trusted root CA into all client browsers, either by manually configuring the browser or by adding the certificate to the trusted roots in an Active Directory (AD) Group Policy Object (GPO).</li></ol></li></ol>
---	---

**Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)**

<p><b>Step 5</b> Configure an authentication server profile.</p> <p>Required for external authentication. If you enable Kerberos SSO or NTLM authentication, the firewall uses the external service only if those methods fail.</p>	<ul style="list-style-type: none"><li>• <a href="#">Configure a RADIUS Server Profile</a>.</li><li>• <a href="#">Configure a TACACS+ Server Profile</a></li><li>• <a href="#">Configure an LDAP Server Profile</a></li><li>• <a href="#">Configure a Kerberos Server Profile</a></li></ul> <p><b>!</b> The PAN-OS web server timeout (default is 3 seconds) must be the same as or greater than the server profile timeout multiplied by the number of servers in the profile. For RADIUS and TACACS+, the default server profile <b>Timeout</b> is 3 seconds. For LDAP, the timeout is the total of the <b>Bind Timeout</b> (default is 30 seconds) and <b>Search Timeout</b> (default is 30 seconds) for each server. For Kerberos, the non-configurable timeout can take up to 17 seconds for each server. Also, the Captive Portal session timeout (default is 30 seconds) must be greater than the web server timeout.</p> <p>To change the web server timeout, enter the following firewall CLI command, where &lt;value&gt; is 3-30 seconds: <code>set deviceconfig setting 13-service timeout &lt;value&gt;</code>. To change the Captive Portal session timeout, select <b>Device &gt; Setup &gt; Session</b>, edit the Session Timeouts, and enter a new <b>Captive Portal</b> value in seconds (range is 1-1,599,999). Keep in mind that the more you raise the web server and Captive Portal session timeouts, the slower Captive Portal will respond to users.</p>
<p><b>Step 6</b> Add the users and user groups to the local database on the firewall.</p> <p>Required for local database authentication. If you enable Kerberos SSO and/or NTLM authentication, the firewall uses the local database only if those methods fail.</p>	<p><a href="#">Create the local database</a>. Add the users who will authenticate using Captive Portal.</p>

## Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)

<p><b>Step 7</b> Add an authentication profile</p> <p>The profile defines the authentication methods to use (Kerberos SSO, external service, or local database) when a Captive Portal rule invokes <a href="#">Web Form</a> authentication. Even if you enable NTLM, you must define a secondary authentication method in case NTLM authentication fails or the User-ID agent doesn't support NTLM.</p> <p> If you set the authentication <b>Type</b> to <b>RADIUS</b>, specify a RADIUS <b>User Domain</b> in case users don't enter the domain at login.</p>	<p><b>Configure an authentication profile:</b></p> <ol style="list-style-type: none"> <li>If the authentication <b>Type</b> is an external service (<b>RADIUS</b>, <b>TACACS+</b>, <b>LDAP</b>, or <b>Kerberos</b>), select the authentication <b>Server Profile</b> you created.</li> <li>If you use Kerberos SSO, enter the <b>Kerberos Realm</b> (usually the DNS domain of the users, except that the realm is uppercase), and import the <b>Kerberos Keytab</b> you created.</li> <li>In the Allow List on the <b>Advanced</b> tab, <b>Add</b> the users and user groups that can authenticate using this profile. If the authentication <b>Type</b> is <b>Local Database</b>, add the Captive Portal users or user groups you created. You can select <b>all</b> to allow every user to authenticate. After you complete the Allow List, click <b>OK</b>.</li> </ol> <p> If your users are in multiple domains or Kerberos realms, you can create an authentication profile for each domain or realm, assign all the profiles to the authentication sequence (Step 8), and assign the sequence to the Captive Portal configuration.</p>
<p><b>Step 8</b> (Optional) Add an authentication sequence</p> <p> If the firewall might try multiple authentication profiles in the sequence for any one user (for example, if some directory server connections are unreliable), then the PAN-OS web server timeout must be the same as or greater than the timeout for the sequence, which is the total of the timeouts for all its authentication profiles. Also, the session timeout for Captive Portal must be greater than the web server timeout. To change these timeouts, see the note in Step 5.</p>	<p><b>Configure an authentication sequence:</b></p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Authentication Sequence</b>, click <b>Add</b>, and enter a <b>Name</b> to identify the authentication sequence.</li> <li>Select the <b>Use domain to determine authentication profile</b> check box: the device will match the domain name that a user enters during login with the <b>User Domain</b> or <b>Kerberos Realm</b> of an authentication profile in the sequence, and then use that profile to authenticate the user.</li> <li>For each authentication profile to include, click <b>Add</b> and select the profile from the drop-down.</li> <li>Click <b>OK</b> to save the authentication sequence.</li> </ol>

**Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)**

<p><b>Step 9</b> Configure Client Certificate Authentication.</p> <p>Required if Captive Portal will use this authentication method.</p> <p> You don't need an authentication profile or sequence for client certificate authentication. If you configure both an authentication profile/sequence and certificate authentication, users must authenticate using both.</p>	<ol style="list-style-type: none"><li>1. Use a root CA certificate to generate a client certificate for each user who will authenticate to Captive Portal. The CA in this case is usually your enterprise CA, not the firewall.</li><li>2. Export the CA certificate in PEM format to a system that the firewall can access.</li><li>3. Import the CA certificate onto the firewall: see <a href="#">Import a Certificate and Private Key</a>. After the import, click the imported certificate, select <b>Trusted Root CA</b>, and click <b>OK</b>.</li><li>4. Configure a Certificate Profile.<ul style="list-style-type: none"><li>In the <b>Username Field</b> drop-down, select the certificate field that contains the user identity information.</li><li>In the <b>CA Certificates</b> list, click <b>Add</b> and select the CA certificate you just imported.</li></ul></li></ol>
<p><b>Step 10</b> Enable <a href="#">NT LAN Manager (NTLM)</a> authentication.</p> <p>Required for NTLM authentication.</p> <p> When using the PAN-OS integrated User-ID agent, the firewall must successfully resolve the DNS name of your domain controller to join the domain (using the credentials you enter in this step).</p>	<ol style="list-style-type: none"><li>1. If you haven't already done so, <a href="#">Create an Active Directory (AD) account for the User-ID agent</a>.</li><li>2. Select <b>Device &gt; User Identification &gt; User Mapping</b> and edit the Palo Alto Networks User ID Agent Setup section.</li><li>3. On the <b>NTLM</b> tab, select the <b>Enable NTLM authentication processing</b> check box.</li><li>4. Enter the <b>NTLM Domain</b> against which the User-ID agent on the firewall will check NTLM credentials.</li><li>5. In the <b>Admin User Name</b>, <b>Password</b>, and <b>Confirm Password</b> fields, enter the username and password of the Active Directory account you created for the User-ID agent.<p> Do not include the domain in the <b>Admin User Name</b> field. Otherwise, the firewall will fail to join the domain. Palo Alto Networks recommends that you use a User-ID agent account that is separate from your firewall administrator account.</p></li><li>6. You don't need to configure any other settings for the User-ID agent: click <b>OK</b>.</li></ol>

**Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)**

Step 11 Configure the Captive Portal settings.

1. Select **Device > User Identification > Captive Portal Settings** and edit the settings.
2. Make sure the **Enable Captive Portal** check box is selected.
3. Select the **SSL/TLS Service Profile** you created for redirect requests over TLS.
4. Select the **Mode** (in this example, **Redirect**).
5. (Redirect mode only) Specify the **Redirect Host** name that resolves to the IP address of the Layer 3 interface for redirected requests.
6. Select the authentication method to use if NTLM fails (or if you don't use NTLM):
  - To use Kerberos SSO, an external server, or the local database, select the **Authentication Profile** or authentication sequence you created.
  - To use client certificate authentication, select the **Certificate Profile** you created.
7. Click **OK** and **Commit** to save the Captive Portal configuration.

## Configure User Mapping for Terminal Server Users

Individual terminal server users appear to have the same IP address and therefore an IP address-to-username mapping is not sufficient to identify a specific user. To enable identification of specific users on Windows-based terminal servers, the Palo Alto Networks Terminal Services agent (TS agent) allocates a port range to each user. It then notifies every connected firewall about the allocated port range, which allows the firewall to create an IP address-port-user mapping table and enable user- and group-based security policy enforcement. For non-Windows terminal servers, you can configure the User-ID XML API to extract user mapping information.

The following sections describe how to configure user mapping for terminal server users:

- ▲ [Configure the Palo Alto Networks Terminal Server Agent for User Mapping](#)
- ▲ [Retrieve User Mappings from a Terminal Server Using the User-ID XML API](#)

### Configure the Palo Alto Networks Terminal Server Agent for User Mapping

Use the following procedure to install the TS agent on the terminal server. You must install the TS agent on all terminal servers that your users log in to in order to successfully map all your users.



For information about the supported terminal servers supported by the TS Agent, refer to “Operating System (OS) Compatibility TS Agent” in the Terminal Services Agent Release Notes, which are available on the Palo Alto Networks [Software Updates](#) page.

#### Install the Windows Terminal Server Agent

**Step 1** Download the TS Agent installer.

1. Log in to the [Palo Alto Networks Support](#) site.
2. Select **Software Updates** from the Manage Devices section.
3. Scroll to the **Terminal Services Agent** section and **Download** the version of the agent you want to install.
4. Save the `TaInstall164.x64-x.x.x-xx.msi` or `TaInstall-x.x.x-xx.msi` file (be sure to select the appropriate version based on whether the Windows system is running a 32-bit OS or a 64-bit OS) on the system(s) where you plan to install the agent.

## Install the Windows Terminal Server Agent (Continued)

- Step 2** Run the installer as an administrator.



1. To launch a command prompt as an administrator, click Start and right-click **Command Prompt** and then select **Run as administrator**.

2. From the command line, run the .msi file you downloaded. For example, if you saved the .msi file to the Desktop you would enter the following:

```
C:\Users\administrator.acme>cd Desktop  
C:\Users\administrator.acme\Desktop>TaInstall-6.0.0-1.msi
```

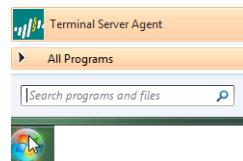
3. Follow the setup prompts to install the agent using the default settings. By default, the agent gets installed to the C:\Program Files (x86)\Palo Alto Networks\Terminal Server Agent folder, but you can **Browse** to a different location.

4. When the installation completes, **Close** the setup window.

 If you are upgrading to a TS Agent version that has a newer driver than the existing installation, the installation wizard prompts you to reboot the system after upgrading in order to use the new driver.

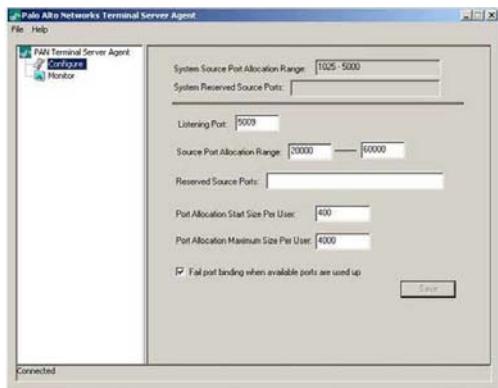
- Step 3** Launch the Terminal Server Agent application.

Click Start and select **Terminal Server Agent**.



## Install the Windows Terminal Server Agent (Continued)

- Step 4** Define the range of ports for the TS Agent to allocate to end users.



The **System Source Port Allocation Range** and **System Reserved Source Ports** fields specify the range of ports that will be allocated to non-user sessions. Make sure the values specified in these fields do not overlap with the ports you designate for user traffic. These values can only be changed by editing the corresponding Windows registry settings.

1. Select **Configure**.
2. Set the **Source Port Allocation Range** (default 20000-39999). This is the full range of port numbers that the TS Agent will allocate for user mapping. The port range you specify cannot overlap with the **System Source Port Allocation Range**.
3. (Optional) If there are ports/port ranges within the source port allocation that you do not want the TS Agent to allocate to user sessions, specify them as **Reserved Source Ports**. To include multiple ranges, use commas with no spaces, for example: 2000-3000,3500,4000-5000.
4. Specify the number of ports to allocate to each individual user upon login to the terminal server in the **Port Allocation Start Size Per User** field (default 200).
5. Specify the **Port Allocation Maximum Size Per User**, which is the maximum number of ports the Terminal Server agent can allocate to an individual user.
6. Specify whether to continue processing traffic from the user if the user runs out of allocated ports. By default, the **Fail port binding when available ports are used up** is selected, which indicates that the application will fail to send traffic when all ports are used. To enable users to continue using applications when they run out of ports, clear this check box. Keep in mind that this traffic may not be identified with User-ID.

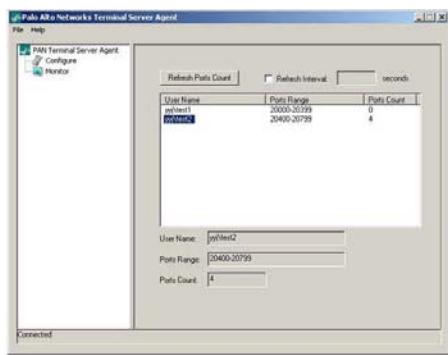
- Step 5** Configure the firewalls to connect to the Terminal Server agent.

Complete the following steps on each firewall you want to connect to the Terminal Server agent to receive user mappings:

1. Select **Device > User Identification > Terminal Server Agents** and click **Add**.
2. Enter a **Name** for the Terminal Server agent.
3. Enter the IP address of the Windows **Host** on which the Terminal Server agent is installed.
4. Enter the **Port** number on which the agent will listen for user mapping requests. This value must match the value configured on the Terminal Server agent. By default, the port is set to 5009 on the firewall and on the agent. If you change it here, you must also change the **Listening Port** field on the Terminal Server agent **Configure** screen.
5. Make sure that the configuration is **Enabled** and then click **OK**.
6. **Commit** the changes.
7. Verify that the **Connected** status displays as connected (a green light).

### Install the Windows Terminal Server Agent (Continued)

- Step 6** Verify that the Terminal Server agent is successfully mapping IP addresses to usernames and that the firewalls can connect to the agent.



1. Launch the Terminal Server agent and verify that the firewalls can connect by making sure the **Connection Status** for each of Device in the Connection List is **Connected**.
2. To verify that the Terminal Server agent is successfully mapping port ranges to usernames, select **Monitoring** and make sure that the mapping table is populated.

### Retrieve User Mappings from a Terminal Server Using the User-ID XML API

The User-ID XML API is a RESTful API that uses standard HTTP requests to send and receive data. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports RESTful services.

To enable a non-Windows terminal server to send user mapping information directly to the firewall, create scripts that extract the user login and logout events and use them for input to the User-ID XML API request format. Then define the mechanisms for submitting the XML API request(s) to the firewall using cURL or wget and providing the firewall's API key for secure communication. Creating user mappings from multi-user systems such as terminal servers requires use of the following API messages:

- **<multiusersystem>**—Sets up the configuration for an XML API Multi-user System on the firewall. This message allows for definition of the terminal server IP address (this will be the source address for all users on that terminal server). In addition, the **<multiusersystem>** setup message specifies the range of source port numbers to allocate for user mapping and the number of ports to allocate to each individual user upon login (called the *block size*). If you want to use the default source port allocation range (1025-65534) and block size (200), you do not need to send a **<multiusersystem>** setup event to the firewall. Instead, the firewall will automatically generate the XML API Multi-user System configuration with the default settings upon receipt of the first user login event message.
- **<blockstart>**—Used with the **<login>** and **<logout>** messages to indicate the starting source port number allocated to the user. The firewall then uses the block size to determine the actual range of port numbers to map to the IP address and username in the login message. For example, if the **<blockstart>** value is 13200 and the block size configured for the multi-user system is 300, the actual source port range allocated to the user is 13200 through 13499. Each connection initiated by the user should use a unique source port number within the allocated range, enabling the firewall to identify the user based on its IP address-port-user mappings for enforcement of user- and group-based security rules. When a user exhausts all the ports allocated, the terminal server must send a new **<login>** message allocating a new port range for the user so that the firewall can update the IP address-port-user mapping. In addition, a single username can

have multiple blocks of ports mapped simultaneously. When the firewall receives a <logout> message that includes a <blockstart> parameter, it removes the corresponding IP address-port-user mapping from its mapping table. When the firewall receives a <logout> message with a username and IP address, but no <blockstart>, it removes the user from its table. And, if the firewall receives a <logout> message with an IP address only, it removes the multi-user system and all mappings associated with it.



The XML files that the terminal server sends to the firewall can contain multiple message types and the messages do not need to be in any particular order within the file. However, upon receiving an XML file that contains multiple message types, the firewall will process them in the following order: multisystem requests first, followed by logins, then logouts.

The following workflow provides an example of how to use the User-ID XML API to send user mappings from a non-Windows terminal server to the firewall.

### Use the User-ID XML API to Map Non-Windows Terminal Services Users

<p><b>Step 1</b> Generate the API key that will be used to authenticate the API communication between the firewall and the Terminal server. To generate the key you must provide login credentials for an administrative account; the API is available to all administrators (including role-based administrators with XML API privileges enabled).</p> <p> Any special characters in the password must be URL/percent-encoded.</p>	<p>From a browser, log in to the firewall. Then, to generate the API key for the firewall, open a new browser window and enter the following URL:</p> <p><code>https://&lt;Firewall-IPaddress&gt;/api/?type=keygen&amp;user=&lt;username&gt;&amp;password=&lt;password&gt;</code></p> <p>Where &lt;Firewall-IPaddress&gt; is the IP address or FQDN of the firewall and &lt;username&gt; and &lt;password&gt; are the credentials for the administrative user account on the firewall. For example:</p> <p><code>https://10.1.2.5/api/?type=keygen&amp;user=admin&amp;password=admin</code></p> <p>The firewall responds with a message containing the key, for example:</p> <pre>&lt;response status="success"&gt;   &lt;result&gt;     &lt;key&gt;k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=&lt;/key&gt;   &lt;/result&gt; &lt;/response&gt;</pre>
---	--

### Use the User-ID XML API to Map Non-Windows Terminal Services Users (Continued)

<p><b>Step 2</b> (Optional) Generate a setup message that the terminal server will send to specify the port range and block size of ports per user that your terminal services agent uses.</p> <p>If the terminal services agent does not send a setup message, the firewall will automatically create a terminal server agent configuration using the following default settings upon receipt of the first login message:</p> <ul style="list-style-type: none"> <li>• Default port range: 1025 to 65534</li> <li>• Per user block size: 200</li> <li>• Maximum number of multi-user systems: 1,000</li> </ul>	<p>The following shows a sample setup message:</p> <pre>&lt;uid-message&gt;   &lt;payload&gt;     &lt;multiusersystem&gt;       &lt;entry ip="10.1.1.23" startport="20000"              endport="39999" blocksize="100"&gt;         &lt;/multiusersystem&gt;     &lt;/payload&gt;     &lt;type&gt;update&lt;/type&gt;     &lt;version&gt;1.0&lt;/version&gt; &lt;/uid-message&gt;</pre> <p>where <code>entry ip</code> specifies the IP address assigned to terminal server users, <code>startport</code> and <code>endport</code> specify the port range to use when assigning ports to individual users, and <code>blocksize</code> specifies the number of ports to assign to each user. The maximum blocksize is 4000 and each multi-user system can allocate a maximum of 1,000 blocks.</p> <p>If you define a custom blocksize and or port range, keep in mind that you must configure the values such that every port in the range gets allocated and that there are no gaps or unused ports. For example, if you set the port range to 1000–1499, you could set the block size to 100, but not to 200. This is because if you set it to 200, there would be unused ports at the end of the range.</p>
<p><b>Step 3</b> Create a script that will extract the login events and create the XML input file to send to the firewall.</p> <p>Make sure the script enforces assignment of port number ranges at fixed boundaries with no port overlaps. For example, if the port range is 1000–1999 and the block size is 200, acceptable blockstart values would be 1000, 1200, 1400, 1600, or 1800. Blockstart values of 1001, 1300, or 1850 would be unacceptable because some of the port numbers in the range would be left unused.</p> <p> The login event payload that the terminal server sends to the firewall can contain multiple login events.</p>	<p>The following shows the input file format for a user-ID XML login event:</p> <pre>&lt;uid-message&gt;   &lt;payload&gt;     &lt;login&gt;       &lt;entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000"&gt;       &lt;entry name="acme\jparker" ip="10.1.1.23" blockstart="20100"&gt;       &lt;entry name="acme\ccrisp" ip="10.1.1.23" blockstart="21000"&gt;     &lt;/login&gt;   &lt;/payload&gt;   &lt;type&gt;update&lt;/type&gt;   &lt;version&gt;1.0&lt;/version&gt; &lt;/uid-message&gt;</pre> <p>The firewall uses this information to populate its user mapping table. Based on the mappings extracted from the example above, if the firewall received a packet with a source address and port of 10.1.1.23:20101, it would map the request to user jparker for policy enforcement.</p> <p> Each multi-user system can allocate a maximum of 1,000 port blocks.</p>

### Use the User-ID XML API to Map Non-Windows Terminal Services Users (Continued)

<p><b>Step 4</b> Create a script that will extract the logout events and create the XML input file to send to the firewall.</p> <p>Upon receipt of a logout event message with a <code>blockstart</code> parameter, the firewall removes the corresponding IP address-port-user mapping. If the logout message contains a username and IP address, but no <code>blockstart</code> parameter, the firewall removes all mappings for the user. If the logout message contains an IP address only, the firewall removes the multi-user system and all associated mappings.</p>	<p>The following shows the input file format for a User-ID XML logout event:</p> <pre>&lt;uid-message&gt;   &lt;payload&gt;     &lt;logout&gt;       &lt;entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000"&gt;         &lt;entry name="acme\ccrisp" ip="10.1.1.23"&gt;           &lt;entry ip="10.2.5.4"&gt;         &lt;/logout&gt;     &lt;/payload&gt;     &lt;type&gt;update&lt;/type&gt;     &lt;version&gt;1.0&lt;/version&gt; &lt;/uid-message&gt;</pre> <p> You can also clear the multiuser system entry from the firewall using the following CLI command: <code>clear xml-api multiusersystem</code></p>
<p><b>Step 5</b> Make sure that the scripts you create include a way to dynamically enforce that the port block range allocated using the XML API matches the actual source port assigned to the user on the terminal server and that the mapping is removed when the user logs out or the port allocation changes.</p>	<p>One way to do this would be to use netfilter NAT rules to hide user sessions behind the specific port ranges allocated via the XML API based on the uid. For example, to ensure that a user with the user ID <code>jjaso</code> is mapped to a source network address translation (SNAT) value of <code>10.1.1.23:20000-20099</code>, the script you create should include the following:</p> <pre>[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner jjaso -p tcp -j SNAT --to-source 10.1.1.23:20000-20099</pre> <p>Similarly, the scripts you create should also ensure that the IP table routing configuration dynamically removes the SNAT mapping when the user logs out or the port allocation changes:</p> <pre>[root@ts1 ~]# iptables -t nat -D POSTROUTING 1</pre>
<p><b>Step 6</b> Define how to package the XML input files containing the setup, login, and logout events into wget or cURL messages for transmission to the firewall.</p>	<p><b>To apply the files to the firewall using wget:</b></p> <pre>&gt; wget --post file &lt;filename&gt; "https://&lt;Firewall-IPaddress&gt;/api/?type=user-id&amp;key=&lt;key&gt;&amp;file-name=&lt;input_filename.xml&gt;&amp;client=wget&amp;vsys=&lt;VSYS_name&gt;"</pre> <p>For example, the syntax for sending an input file named <code>login.xml</code> to the firewall at <code>10.2.5.11</code> using key <code>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg</code> using wget would look as follows:</p> <pre>&gt; wget --post file login.xml "https://10.2.5.11/api/?type=user-id&amp;key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&amp;file-name=login.xml&amp;client=wget&amp;vsys=vsys1"</pre> <p><b>To apply the file to the firewall using cURL:</b></p> <pre>&gt; curl --form file=@&lt;filename&gt; https://&lt;Firewall-IPaddress&gt;/api/?type=user-id&amp;key=&lt;key&gt;&amp;vsys=&lt;VSYS_name&gt; &gt;</pre> <p>For example, the syntax for sending an input file named <code>login.xml</code> to the firewall at <code>10.2.5.11</code> using key <code>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg</code> using cURL would look as follows:</p> <pre>&gt; curl --form file@login.xml "https://10.2.5.11/api/?type=user-id&amp;key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&amp;vsys=vsys1"</pre>

**Use the User-ID XML API to Map Non-Windows Terminal Services Users (Continued)**

<b>Step 7</b> Verify that the firewall is successfully receiving login events from the terminal servers.	Verify the configuration by opening an SSH connection to the firewall and then running the following CLI commands:  <b>To verify if the terminal server is connecting to the firewall over XML:</b> admin@PA-5050> <b>show user xml-api multiusersystem</b> Host Vsys Users Blocks ----- 10.5.204.43 vsys1 5 2  <b>To verify that the firewall is receiving mappings from a terminal server over XML:</b> admin@PA-5050> <b>show user ip-port-user-mapping all</b>  Global max host index 1, host hash count 1  XML API Multi-user System 10.5.204.43 Vsys 1, Flag 3 Port range: 20000 - 39999 Port size: start 200; max 2000 Block count 100, port count 20000 20000-20199: acme\administrator  Total host: 1
--	--

## Send User Mappings to User-ID Using the XML API

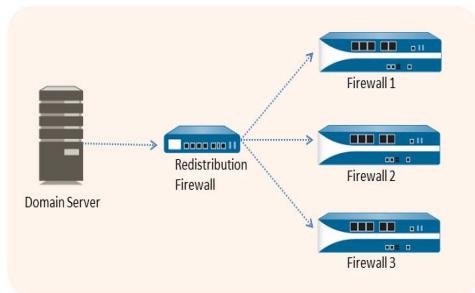
Although the User-ID functionality provides many out-of-the box methods for obtaining user mapping information, you may have some applications or devices that capture user information that cannot be natively integrated with User-ID. In this case you can use the User-ID XML API to create custom scripts that allow you to leverage existing user data and send it to the User-ID agent or directly to the firewall.

The User-ID XML API is a RESTful API that uses standard HTTP requests to send and receive data. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports RESTful services. To leverage user data from an existing system—such as a custom application developed internally or another device that is not supported by one of the existing user mapping mechanisms—you can create custom scripts to extract the data and send it to the firewall or the User-ID agent using the XML API.

To enable an external system to send user mapping information to the User-ID agent or directly to the firewall, you can create scripts that extract the user login and logout events and use them for input to the User-ID XML API request format. Then define the mechanisms for submitting the XML API request(s) to the firewall using cURL or wget using the firewall's API key for secure communication. For more details, refer to the [PAN-OS XML API Usage Guide](#).

# Configure a Firewall to Share User Mapping Data with Other Firewalls

Because policy is local to each firewall, each firewall needs current user mapping and group mapping information to accurately enforce policy by user and group. To simplify administration, you can configure one firewall to be the *redistribution firewall* that collects all the mapping information and shares it with other firewalls. The redistribution firewall can share only the information it collects using local methods (for example, the PAN-OS integrated User-ID agent or Captive Portal); it can't share the information collected from the Windows-based User-ID and Terminal Services agents. You configure the receiving firewalls to retrieve the mapping information from the redistribution firewall; they don't need to communicate directly with domain servers.



The following procedure describes how to set up redistribution of User-ID information.

## Configure a Firewall to Share User Mapping Data with Other Firewalls

<p><b>Step 1</b> Configure the redistribution firewall.</p> <p><b>!</b> User-ID configurations apply to a single virtual system only. To redistribute User-ID mappings from multiple virtual systems, you must configure the user mapping settings on each virtual system separately, using a unique pre-shared key in each configuration.</p>	<ol style="list-style-type: none"> <li>Select <b>Device &gt; User Identification &gt; User Mapping</b> and edit the Palo Alto Networks User-ID Agent Setup section.</li> <li>Select <b>Redistribution</b>.</li> <li>Enter a <b>Collector Name</b>.</li> <li>Enter and confirm the <b>Pre-Shared Key</b> that will enable other firewalls to connect to this firewall to retrieve user mapping information.</li> <li>Click <b>OK</b> to save the redistribution configuration.</li> </ol>
<p><b>Step 2</b> Create an interface management profile that enables the User-ID service and attach it to the interface that the other firewalls will connect to in order to retrieve user mappings.</p>	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Network Profiles &gt; Interface Mgmt</b> and click <b>Add</b>.</li> <li>Enter a <b>Name</b> for the profile and then select the Permitted Services. At a minimum, select <b>User-ID Service</b> and <b>HTTPS</b>.</li> <li>Click <b>OK</b> to save the profile.</li> <li>Select <b>Network &gt; Interfaces &gt; Ethernet</b> and select the interface you plan to use for redistribution.</li> <li>On the <b>Advanced &gt; Other Info</b> tab, select the <b>Management Profile</b> you just created.</li> <li>Click <b>OK</b> and <b>Commit</b>.</li> </ol>

### Configure a Firewall to Share User Mapping Data with Other Firewalls (Continued)

<p><b>Step 3</b> Configure the other firewalls to retrieve user mappings from the redistribution firewall.</p> <p> If the redistribution firewall has multiple virtual systems configured for redistribution, make sure you are using the pre-shared key that corresponds to the virtual system from which you want this firewall to retrieve User-ID mappings.</p>	<p>Perform the following steps on each firewall that you want to be able to retrieve user mappings:</p> <ol style="list-style-type: none"> <li>1. Select <b>Device &gt; User Identification &gt; User-ID Agents</b>.</li> <li>2. Click <b>Add</b> and enter a User-ID agent <b>Name</b> for the redistribution firewall.</li> <li>3. Enter the hostname or IP address of the firewall interface that you configured for redistribution in the <b>Host</b> field.</li> <li>4. Enter 5007 as the <b>Port</b> number on which the redistribution firewall will listen for User-ID requests.</li> <li>5. Enter the <b>Collector Name</b> that you specified in the redistribution firewall configuration (<a href="#">Step 1-3</a>).</li> <li>6. Enter and confirm the <b>Collector Pre-Shared Key</b>. The key value you enter here must match the value configured on the redistribution firewall (<a href="#">Step 1-4</a>).</li> <li>7. (Optional) If you are using the redistribution firewall to retrieve group mappings in addition to user mappings, select the <b>Use as LDAP Proxy</b> check box.</li> <li>8. (Optional) If you are using the redistribution firewall for Captive Portal authentication, select the <b>Use for NTLM Authentication</b> check box.</li> <li>9. Make sure that the configuration is <b>Enabled</b> and then click <b>OK</b>.</li> <li>10. <b>Commit</b> the changes.</li> </ol>
<p><b>Step 4</b> Verify the configuration.</p>	<p>On the <b>User-ID Agents</b> tab, verify that the redistribution firewall entry you just added shows a green icon in the <b>Connected</b> column. If a red icon appears, check traffic logs (<b>Monitor &gt; Logs &gt; Traffic</b>) to identify the issue. You can also check to see if any user mapping data has been received by running the following operational commands from the CLI:</p> <pre>show user ip-user-mapping (to view user mapping information on the dataplane) show user ip-user-mapping-mp (to view mappings on the management plane).</pre>

## Enable User- and Group-Based Policy

To enable security policy based on users and user groups, you must enable User-ID for each zone that contains users you want to identify. You can then define policy rules that allow or deny traffic based on username or group membership. Additionally, you can create Captive Portal rules to enable identification for IP addresses that don't yet have any user data associated with them.



For users with multiple usernames, see [Enable Policy for Users with Multiple Accounts](#).

### Enable User- and Group-Based Policy

<b>Step 1</b>	Enable User-ID on the source zones that contain the users who will send requests that require user-based access controls.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Zones</b> and click the Name of the zone.</li><li>2. Select the <b>Enable User Identification</b> check box and click <b>OK</b>.</li></ol>
<b>Step 2</b>	(Optional) Configure the firewall to read the IP addresses of users from the X-Forwarded-For (XFF) header in client requests for web services when the firewall is between the Internet and a proxy server that would otherwise hide the user IP addresses.  The firewall matches the IP addresses with usernames that your policy rules reference so that those rules can control and log access for the associated users and groups. For details, see <a href="#">Identify Users Connected through a Proxy Server</a> .	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Content-ID</b> and edit the X-Forwarded-For Headers settings.</li><li>2. Select the <b>X-Forwarded-For Header in User-ID</b> check box.  Selecting the <b>Strip-X-Forwarded-For Header</b> check box doesn't disable the use of XFF headers for user attribution in policy rules; the firewall zeroes out the XFF value only after using it for user attribution.</li><li>3. Click <b>OK</b> to save your changes.</li></ol>

<b>Enable User- and Group-Based Policy (Continued)</b>	
<p><b>Step 3</b> Create security rules based on user and user group.</p>  <p>As a best practice, create rules based on group rather than user whenever possible. This prevents you from having to continually update your rules (which requires a commit) whenever your user base changes.</p>	<ol style="list-style-type: none"> <li>After configuring User-ID, you will be able to choose a user name or group name when defining the source or destination of a security rule:             <ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and click <b>Add</b> to create a new rule or click on an existing rule name to open the Security Policy Rule dialog.</li> <li>Specify which users and/or groups to match in the rule in one of the following ways:                   <ul style="list-style-type: none"> <li>If you want to specify specific users/groups as matching criteria, select the <b>User</b> tab and click the <b>Add</b> button in the Source User section to display a list of users and groups discovered by the firewall group mapping function. Select the users and/or groups to add to the rule.</li> <li>If you want the rule to match any user who has or has not successfully authenticated and you don't need to know the specific user or group name, select <b>known-user</b> or <b>unknown</b> from the drop-down above the <b>Source User</b> list.</li> </ul> </li> </ol> </li> <li>Configure the rest of the rule as appropriate and then click <b>OK</b> to save it. For details on other fields in the security rule, see <a href="#">Set Up Basic Security Policies</a>.</li> </ol>
<p><b>Step 4</b> Create your Captive Portal rules.</p>	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Captive Portal</b>.</li> <li>Click <b>Add</b> and enter a <b>Name</b> for the rule.</li> <li>Define the matching criteria for the rule by completing the <b>Source</b>, <b>Destination</b>, and <b>Service/URL Category</b> tabs as appropriate to match the traffic you want to authenticate. The matching criteria on these tabs is the same as the criteria you define when creating a security rule. See <a href="#">Set Up Basic Security Policies</a> for details.</li> <li>Define the <b>Action</b> to take on traffic that matches the rule:             <ul style="list-style-type: none"> <li><b>no-captive-portal</b>—Allow traffic to pass without presenting a Captive Portal page for authentication.</li> <li><b>web-form</b>—Present a Captive Portal page for the user to explicitly enter authentication credentials or use client certificate authentication.</li> <li><b>browser-challenge</b>—Transparently obtain user authentication credentials. If you select this action, you must enable <a href="#">Kerberos Single Sign-On (SSO)</a> or <a href="#">NT LAN Manager (NTLM)</a> authentication when you <a href="#">Configure Captive Portal</a>. If Kerberos SSO authentication fails, the firewall falls back to NTLM authentication. If you didn't configure NTLM, or NTLM authentication fails, the firewall falls back to <b>web-form</b> authentication.</li> </ul> </li> <li>Click <b>OK</b> and <b>Commit</b>.</li> </ol>

## Enable Policy for Users with Multiple Accounts

If a user in your organization has multiple responsibilities, that user might have multiple usernames (accounts), each with distinct privileges for accessing a particular set of services, but with all the usernames sharing the same IP address (the client system of the user). However, the User-ID agent can map any one IP address (or IP address and port range for terminal server users) to only one username for enforcing policy, and you can't predict which username the agent will map. To control access for all the usernames of a user, you must make adjustments to the rules, user groups, and User-ID agent.

For example, say the firewall has a rule that allows username corp\_user to access email and a rule that allows username admin\_user to access a MySQL server. The user logs in with either username from the same client IP address. If the User-ID agent maps the IP address to corp\_user, then whether the user logs in as corp\_user or admin\_user, the firewall identifies that user as corp\_user and allows access to email but not the MySQL server. On the other hand, if the User-ID agent maps the IP address to admin\_user, the firewall always identifies the user as admin\_user regardless of login and allows access to the MySQL server but not email. The following steps describe how to enforce both rules in this example.

### Enable Policy for a User with Multiple Accounts

<p><b>Step 1</b> Configure a user group for each service that requires distinct access privileges.</p> <p>In this example, each group is for a single service (email or MySQL server). However, it is common to configure each group for a set of services that require the same privileges (for example, one group for all basic user services and one group for all administrative services).</p>	<p>If your organization already has user groups that can access the services that the user requires, simply add the username that is used for less restricted services to those groups. In this example, the email server requires less restricted access than the MySQL server, and corp_user is the username for accessing email. Therefore, you add corp_user to a group that can access email (corp_employees) and to a group that can access the MySQL server (network_services).</p> <p>If adding a username to a particular existing group would violate your organizational practices, you can create a custom group based on an LDAP filter. For this example, say network_services is a custom group, which you configure as follows:</p> <ol style="list-style-type: none"><li>1. Select <b>Device &gt; User Identification &gt; Group Mapping Settings</b> and <b>Add</b> a group mapping configuration with a unique <b>Name</b>.</li><li>2. Select an <b>LDAP Server Profile</b> and ensure the <b>Enabled</b> check box is enabled.</li><li>3. Select the <b>Custom Group</b> tab and <b>Add</b> a custom group with network_services as a <b>Name</b>.</li><li>4. Specify an <b>LDAP Filter</b> that matches an LDAP attribute of corp_user and click <b>OK</b>.</li><li>5. Click <b>OK</b> and <b>Commit</b>.</li></ol> <p> Later, if other users that are in the group for less restricted services are given additional usernames that access more restricted services, you can add those usernames to the group for more restricted services. This scenario is more common than the inverse; a user with access to more restricted services usually already has access to less restricted services.</p>
---	--

<b>Enable Policy for a User with Multiple Accounts (Continued)</b>	
<b>Step 2</b> Configure the rules that control user access based on the groups you just configured.	<p><b>Enable User- and Group-Based Policy:</b></p> <ol style="list-style-type: none"> <li>Configure a security rule that allows the corp_employees group to access email.</li> <li>Configure a security rule that allows the network_services group to access the MySQL server.</li> </ol>
<b>Step 3</b> Configure the ignore list of the User-ID agent.  This ensures that the User-ID agent maps the client IP address only to the username that is a member of the groups assigned to the rules you just configured. The ignore list must contain all the usernames of the user that are not members of those groups.	<p>In this example, you add admin_user to the ignore list of the Windows-based User-ID agent to ensure that it maps the client IP address to corp_user. This guarantees that, whether the user logs in as corp_user or admin_user, the firewall identifies the user as corp_user and applies both rules that you configured because corp_user is a member of the groups that the rules reference.</p> <ol style="list-style-type: none"> <li>Create an <code>ignore_user_list.txt</code> file.</li> <li>Open the file and add admin_user. If you later add more usernames, each must be on a separate line.</li> <li>Save the file to the User-ID agent folder on the domain server where the agent is installed.</li> </ol> <p> If you use the PAN-OS integrated User-ID agent, perform <a href="#">Step 6</a> under <a href="#">Configure User Mapping Using the PAN-OS Integrated User-ID Agent</a> to configure the ignore list.</p>
<b>Step 4</b> Configure endpoint authentication for the restricted services.  This enables the endpoint to verify the credentials of the user and preserves the ability to enable access for users with multiple usernames.	<p>In this example, you have configured a firewall rule that allows corp_user, as a member of the network_services group, to send a service request to the MySQL server. You must now configure the MySQL server to respond to any unauthorized username (such as corp_user) by prompting the user to enter the login credentials of an authorized username (admin_user).</p> <p> If the user logs in to the network as admin_user, the user can then access the MySQL server without it prompting for the admin_user credentials again.</p> <p>In this example, both corp_user and admin_user have email accounts, so the email server won't prompt for additional credentials regardless of which username the user entered when logging in to the network.</p> <p>The firewall is now ready to enforce rules for a user with multiple usernames.</p>

## Verify the User-ID Configuration

After you configure group mapping and user mapping and enable User-ID on your security rules and Captive Portal rules, you should verify that it is working properly.

Verify the User-ID Configuration																																			
Step 1 Verify that group mapping is working.	<p>From the CLI, enter the following command:</p> <pre><b>show user group-mapping statistics</b></pre>																																		
Step 2 Verify that user mapping is working.	<p>If you are using the on-device User-ID agent, you can verify this from the CLI using the following command:</p> <pre><b>show user ip-user-mapping-mp all</b></pre> <table> <thead> <tr> <th>IP (sec)</th> <th>Vsys</th> <th>From</th> <th>User</th> <th>Timeout</th> </tr> </thead> <tbody> <tr> <td>192.168.201.1</td> <td>vsys1</td> <td>UIA</td> <td>acme\george</td> <td>210</td> </tr> <tr> <td>192.168.201.11</td> <td>vsys1</td> <td>UIA</td> <td>acme\duane</td> <td>210</td> </tr> <tr> <td>192.168.201.50</td> <td>vsys1</td> <td>UIA</td> <td>acme\betsy</td> <td>210</td> </tr> <tr> <td>192.168.201.10</td> <td>vsys1</td> <td>UIA</td> <td>acme\administrator</td> <td>210</td> </tr> <tr> <td>192.168.201.100</td> <td>vsys1</td> <td>AD</td> <td>acme\administrator</td> <td>748</td> </tr> <tr> <td colspan="2">Total: 5 users</td></tr> <tr> <td colspan="2">*: WMI probe succeeded</td></tr> </tbody> </table>	IP (sec)	Vsys	From	User	Timeout	192.168.201.1	vsys1	UIA	acme\george	210	192.168.201.11	vsys1	UIA	acme\duane	210	192.168.201.50	vsys1	UIA	acme\betsy	210	192.168.201.10	vsys1	UIA	acme\administrator	210	192.168.201.100	vsys1	AD	acme\administrator	748	Total: 5 users		*: WMI probe succeeded	
IP (sec)	Vsys	From	User	Timeout																															
192.168.201.1	vsys1	UIA	acme\george	210																															
192.168.201.11	vsys1	UIA	acme\duane	210																															
192.168.201.50	vsys1	UIA	acme\betsy	210																															
192.168.201.10	vsys1	UIA	acme\administrator	210																															
192.168.201.100	vsys1	AD	acme\administrator	748																															
Total: 5 users																																			
*: WMI probe succeeded																																			
Step 3 Test your security rule.	<ul style="list-style-type: none"> <li>From a machine in the zone where User-ID is enabled, attempt to access sites and applications to test the rules you defined in your policy and ensure that traffic is allowed and denied as expected.</li> <li>You can also use the <code>test security-policy-match</code> command to determine whether the policy is configured correctly. For example, suppose you have a rule that blocks user duane from playing World of Warcraft; you could test the policy as follows:</li> </ul> <pre>test security-policy-match application worldofwarcraft source-user acme\duane source any destination any destination-port any protocol 6 "deny worldofwarcraft" {     from corporate;     source any;     source-region any;     to internet;     destination any;     destination-region any;     user acme\duane;     category any;     application/service worldofwarcraft;     action deny;     terminal no; }</pre>																																		

### Verify the User-ID Configuration (Continued)

**Step 4** Test your Captive Portal configuration.

1. From the same zone, go to a machine that is not a member of your directory, such as a Mac OS system, and try to ping to a system external to the zone. The ping should work without requiring authentication.
2. From the same machine, open a browser and navigate to a web site in a destination zone that matches a Captive Portal rule you defined. You should see the Captive Portal web form.

3. Log in using the correct credentials and confirm that you are redirected to the requested page.
4. You can also test your Captive Portal policy using the `test cp-policy-match` command as follows:

```
test cp-policy-match from corporate to internet
source 192.168.201.10 destination 8.8.8.8
Matched rule: 'captive portal' action: web-form
```

**Step 5** Verify that user names are displayed in the log files (**Monitor > Logs**).

Receive Time	Category	URL	From Zone	To Zone	Source	Source User
12/18 15:16:17	computer-and-internet-info	*.urbanairship.com/	I3-trust	I3-untrust	10.31.32.18	acme\jdonaldson
12/18 15:16:01	social-networking	graph.facebook.com/	I3-trust	I3-untrust	10.31.32.18	acme\gbalfour
12/18 15:16:01	social-networking	graph.facebook.com/	I3-trust	I3-untrust	10.31.32.18	acme\jdonaldson
12/18 15:04:15	social-networking	ocart.facebook.com/	I3-trust	I3-untrust	10.31.32.18	acme\jparker
12/18 15:04:15	web-based-email	*.mg.mail.yahoo.com/	I3-trust	I3-untrust	10.31.32.18	acme\jreddick
12/18 14:51:13	search-engines	www.google.com/	I3-trust	I3-untrust	10.31.32.18	acme\jparker
12/18 14:49:06	search-engines	*.google.com/	I3-trust	I3-untrust	10.31.32.18	acme\jreddick
12/18 14:48:10	search-engines	www.google.com/	I3-trust	I3-untrust	10.31.32.18	acme\gbalfour
12/18 14:43:53	web-based-email	*.mg.mail.yahoo.com/	I3-trust	I3-untrust	10.31.32.18	acme\jreddick
12/18 14:43:51	internet-portals	android.register.push.mobile.yahoo.com/	I3-trust	I3-untrust	10.31.32.18	acme\jparker
12/18 14:43:51	web-based-email	*.mg.mail.yahoo.com/	I3-trust	I3-untrust	10.31.32.18	acme\jdonaldson
12/18 14:43:51	internet-portals	login.yahoo.com/	I3-trust	I3-untrust	10.31.32.18	acme\jparker
12/18 14:43:50	computer-and-internet-info	*.crittercism.com/	I3-trust	I3-untrust	10.31.32.18	acme\jreddick
12/18 14:36:35	computer-and-internet-info	mdmbeta.paloaltonetworks.com/	I3-trust	I3-untrust	10.31.32.18	acme\gbalfour
12/18 14:36:35	internet-portals	android.connector.push.mobile.yahoo.com/	I3-trust	I3-untrust	10.31.32.18	acme\jdonaldson
12/18 14:36:35	computer-and-internet-info	settings.crashlytics.com/	I3-trust	I3-untrust	10.31.32.18	acme\jparker

### Verify the User-ID Configuration (Continued)

- Step 6** Verify that user names are displayed in reports (**Monitor > Reports**). For example, when drilling down into the denied applications report, you should see a list of the users who attempted to access the applications as in the following example.

The screenshot displays three main sections of the Palo Alto Networks interface:

- Application Information:** Shows details for the application "zynga-games". Key fields include Name: zynga-games, Description: "This application can be used to identify and control the browser-based games created by Zynga that are available as widgets on social networking sites such as Facebook, Yahoo, and MySpace, as apps on iOS and Android mobile devices, and as independent web properties.", Standard Ports: tcp/80,443, Capable of File Transfer: no, Used by Malware: no, Excessive Bandwidth Use: yes, Evasive: no, Tunnels Other Applications: no, Depends on Applications: facebook-apps, ssl, web-browsing, and Additional Information: Wikipedia, Zynga, Google, Yahoo!.
- Top Applications:** A table showing the top applications based on risk and sessions. The first entry is "zynga-games" with Risk: 1, Sessions: 564, and Bytes: 4.2 M.
- Top Sources:** A table showing the top sources based on bytes and sessions. The first entry is "10.154.63.185" with Source Address: 10.154.63.185, Source Host Name: 10.154.63.185, Source User: pancademo\yamiro.ja..., Bytes: 921.4 K, and Sessions: 170.

## Deploy User-ID in a Large-Scale Network

The following topics describe a User-ID deployment in which you use Windows Log Forwarding and Global Catalog servers to simplify user and group mapping in a large-scale network of Microsoft Active Directory (AD) domain controllers or Exchange servers:

- ▲ [Windows Log Forwarding and Global Catalog Servers](#)
- ▲ [Plan Your User-ID Implementation for a Large-Scale Network](#)
- ▲ [Configure Windows Log Forwarding](#)
- ▲ [Configure User-ID for a Large-Scale Network](#)

### Windows Log Forwarding and Global Catalog Servers

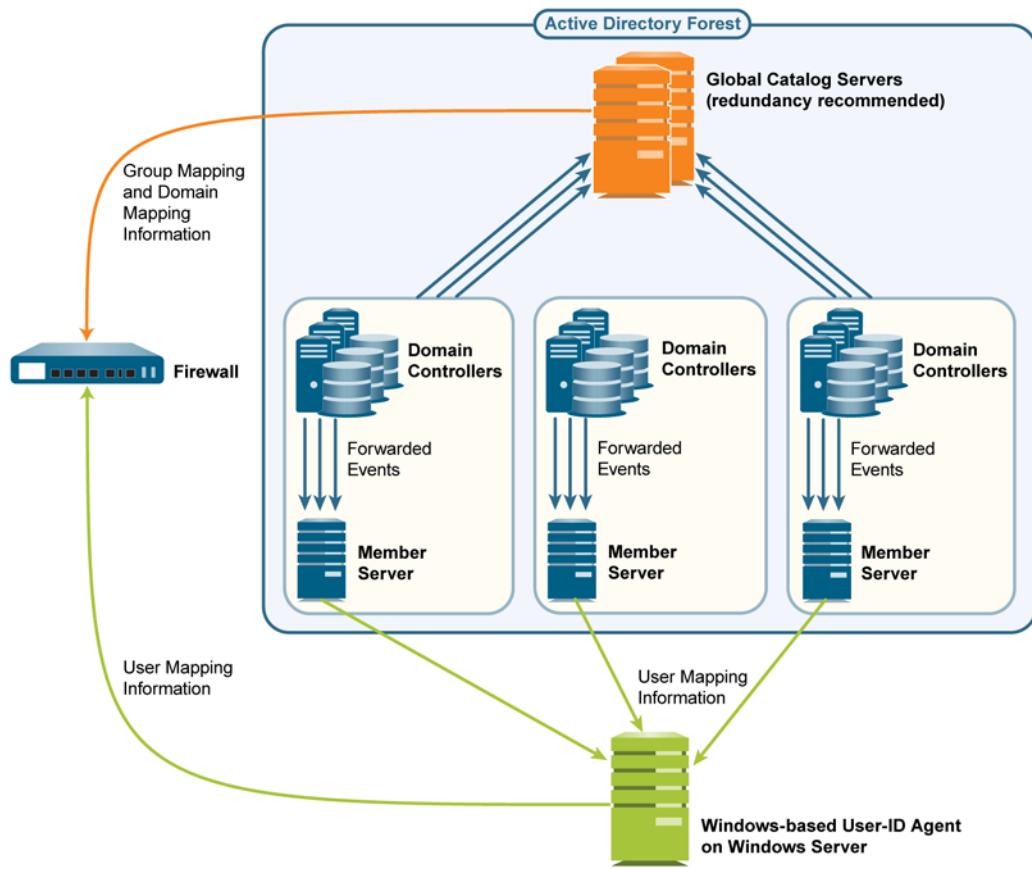
Because each User-ID agent can monitor up to 100 servers, you need multiple User-ID agents to monitor a network with hundreds of AD domain controllers or Exchange servers. Creating and managing numerous User-ID agents involves considerable administrative overhead, especially in expanding networks where tracking new domain controllers is difficult. Windows Log Forwarding enables you to minimize the administrative overhead by reducing the number of servers to monitor and thereby reducing the number of User-ID agents to manage. When you configure Windows Log Forwarding, multiple domain controllers export their login events to a single domain member from which a User-ID agent collects the user mapping information.



You can configure Windows Log Forwarding for Windows Server versions 2003, 2008, 2008 R2, 2012, and 2012 R2. Windows Log Forwarding is not available for non-Microsoft servers.

To collect username to group mapping information in a large-scale network, you can configure the firewall to query a Global Catalog server that receives account information from the domain controllers.

The following figure illustrates user mapping and group mapping for a large-scale network in which the firewall uses a Windows-based User-ID agent. See [Plan Your User-ID Implementation for a Large-Scale Network](#) to determine if this deployment suits your network.



## Plan Your User-ID Implementation for a Large-Scale Network

When deciding whether to use Windows Log Forwarding and Global Catalog servers for your User-ID implementation, consult your system administrator to determine:

- Bandwidth required for domain controllers to forward login events to member servers. The bandwidth is a multiple of the login rate (number of logins per minute) of the domain controllers and the byte size of each login event.

Note that domain controllers won't forward their entire security logs; they forward only the events that the user mapping process requires per login: three events for Windows Server 2003 or four events for Windows Server 2008/2012 and MS Exchange.

- Whether the following network elements support the required bandwidth:

- Domain controllers—They must support the processing load associated with forwarding the events.
- Member Servers—They must support the processing load associated with receiving the events.
- Connections—The geographic distribution (local or remote) of the domain controllers, member servers, and Global Catalog servers is a factor. Generally, a remote distribution supports less bandwidth.

## Configure Windows Log Forwarding

To configure Windows Log Forwarding, you need administrative privileges for configuring group policies on Windows servers. Configure Windows Log Forwarding on every member server that will collect login events from domain controllers. The following is an overview of the tasks; consult your [Windows Server documentation](#) for the specific steps.

### Configure Windows Log Forwarding

**Step 1** On every member server that will collect security events, enable event collection, add the domain controllers as event sources, and configure the event collection query (subscription). The events you specify in the subscription vary by domain controller platform:

- Windows Server 2003—The event IDs for the required events are 672 (Authentication Ticket Granted), 673 (Service Ticket Granted), and 674 (Ticket Granted Renewed).
- Windows Server 2008/2012 (including R2) or MS Exchange—The event IDs for the required events are 4768 (Authentication Ticket Granted), 4769 (Service Ticket Granted), 4770 (Ticket Granted Renewed), and 4624 (Logon Success).



You must forward events to the security logs location on the member servers, not to the default forwarded logs location.



To forward events as quickly as possible, select the **Minimize Latency** option when configuring the subscription.

**Step 2** Configure a group policy to enable Windows Remote Management (WinRM) on the domain controllers.

**Step 3** Configure a group policy to enable Windows Event Forwarding on the domain controllers.

## Configure User-ID for a Large-Scale Network

### Configure User-ID for a Large-Scale Network

<b>Step 1</b> Configure Windows Log Forwarding on the member servers that will collect login events.	<a href="#">Configure Windows Log Forwarding</a> . This step requires administrative privileges for configuring group policies on Windows servers.
<b>Step 2</b> Install the Windows-based User-ID agent.	<a href="#">Install the User-ID Agent</a> on a Windows server that can access the member servers. The Windows server can be inside or outside the Active Directory forest; it doesn't need to be a member server itself.

<b>Configure User-ID for a Large-Scale Network (Continued)</b>	
<b>Step 3</b> Configure the User-ID agent to collect user mapping information from the member servers.	<ol style="list-style-type: none"> <li>1. Start the Windows-based User-ID agent.</li> <li>2. Select <b>User Identification &gt; Discovery</b> and perform the following steps for each member server that will receive events from domain controllers:             <ol style="list-style-type: none"> <li>a. In the Servers section, click <b>Add</b> and enter a <b>Name</b> to identify the member server.</li> <li>b. In the <b>Server Address</b> field, enter the FQDN or IP address of the member server.</li> <li>c. For the <b>Server Type</b>, select <b>Microsoft Active Directory</b>.</li> <li>d. Click <b>OK</b> to save the server entry.</li> </ol> </li> <li>3. Configure the remaining User-ID agent settings: see <a href="#">Configure the User-ID Agent for User Mapping</a>.</li> </ol>
<b>Step 4</b> Configure an LDAP server profile to specify how the firewall connects to the Global Catalog servers (up to four) for group mapping information.	<p> To improve availability, use at least two Global Catalog servers for redundancy.</p> <p> You can collect group mapping information only for universal groups, not local domain groups (subdomains).</p> <ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Server Profiles &gt; LDAP</b>, click <b>Add</b>, and enter a <b>Name</b> for the profile.</li> <li>2. In the Servers section, for each Global Catalog, click <b>Add</b> and enter the server <b>Name</b>, IP address (<b>LDAP Server</b>), and <b>Port</b>. For a plaintext or Start Transport Layer Security (<a href="#">Start TLS</a>) connection, use <b>Port</b> 3268. For an LDAP over SSL connection, use <b>Port</b> 3269. If the connection will use Start TLS or LDAP over SSL, select the <b>Require SSL/TLS secured connection</b> check box.</li> <li>3. In the <b>Base DN</b> field, enter the Distinguished Name (DN) of the point in the Global Catalog server where the firewall will start searching for group mapping information (for example, <code>DC=acbdomain,DC=com</code>).</li> <li>4. For the <b>Type</b>, select <b>active-directory</b>.</li> <li>5. Configure the remaining fields as necessary: see <a href="#">Add an LDAP server profile</a>.</li> </ol>
<b>Step 5</b> Configure an LDAP server profile to specify how the firewall connects to the servers (up to four) that contain domain mapping information.	<p>The steps are the same as for the LDAP server profile you created for Global Catalogs in the <a href="#">Step 4</a>, except for the following fields:</p> <ul style="list-style-type: none"> <li>• <b>LDAP Server</b>—Enter the IP address of the domain controller that contains the domain mapping information.</li> <li>• <b>Port</b>—For a plaintext or Start TLS connection, use <b>Port</b> 389. For an LDAP over SSL connection, use <b>Port</b> 636. If the connection will use Start TLS or LDAP over SSL, select the <b>Require SSL/TLS secured connection</b> check box.</li> <li>• <b>Base DN</b>—Select the DN of the point in the domain controller where the firewall will start searching for domain mapping information. The value must start with the string: <code>cn=partitions,cn=configuration</code> (for example, <code>cn=partitions,cn=configuration,DC=acbdomain,DC=com</code>).</li> </ul>

**Configure User-ID for a Large-Scale Network (Continued)**

- Step 6** Create a group mapping configuration for each LDAP server profile you created.

1. Select **Device > User Identification > Group Mapping Settings**.
2. Click **Add** and enter a **Name** to identify the group mapping configuration.
3. Select the LDAP **Server Profile** and ensure the **Enabled** check box is selected.
4. Configure the remaining fields as necessary: see [Map Users to Groups](#).



If the Global Catalog and domain mapping servers reference more groups than your security rules require, configure the **Group Include List** and/or **Custom Group** list to limit the groups for which User-ID performs mapping.

5. Click **OK** and **Commit**.





# App-ID

---

To safely enable applications on your network, the Palo Alto Networks next-generation firewalls provide both an application and web perspective—App-ID and URL Filtering—to protect against a full spectrum of legal, regulatory, productivity, and resource utilization risks.

App-ID enables visibility into the applications on the network, so you can learn how they work and understand their behavioral characteristics and their relative risk. This application knowledge allows you to create and enforce security policy rules to enable, inspect, and shape desired applications and block unwanted applications. When you define policy rules to allow traffic, App-ID begins to classify traffic without any additional configuration.

- ▲ [App-ID Overview](#)
- ▲ [Manage Custom or Unknown Applications](#)
- ▲ [Manage New App-IDs Introduced in Content Releases](#)
- ▲ [Use Application Objects in Policy](#)
- ▲ [Applications with Implicit Support](#)
- ▲ [Application Level Gateways](#)
- ▲ [Disable the SIP Application-level Gateway \(ALG\)](#)

## App-ID Overview

App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.

Here's how App-ID identifies applications traversing your network:

- Traffic is matched against policy to check whether it is allowed on the network.
- Signatures are then applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics. The signature also determines if the application is being used on its default port or it is using a non-standard port. If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly.
- If App-ID determines that encryption (SSL or SSH) is in use, and a [Decryption](#) policy rule is in place, the session is decrypted and application signatures are applied again on the decrypted flow.
- Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). Decoders validate that the traffic conforms to the protocol specification and provide support for NAT traversal and opening dynamic pinholes for applications such as SIP and FTP.
- For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavioral analysis may be used to determine the identity of the application.

When the application is identified, the policy check determines how to treat the application, for example—block, or allow and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS.

## Manage Custom or Unknown Applications

Palo Alto Networks provides weekly application updates to identify new App-ID signatures. By default, App-ID is always enabled on the firewall, and you don't need to enable a series of signatures to identify well-known applications. Typically, the only applications that are classified as *unknown traffic*—*tcp*, *udp* or *non-syn-tcp*—in the ACC and the traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.

On occasion, the firewall may report an application as unknown for the following reasons:

- Incomplete data—A handshake took place, but no data packets were sent prior to the timeout.
- Insufficient data—A handshake took place followed by one or more data packets; however, not enough data packets were exchanged to identify the application.

The following choices are available to handle unknown applications:

- Create security policies to control unknown applications by unknown TCP, unknown UDP or by a combination of source zone, destination zone, and IP addresses.
- Request an App-ID from Palo Alto Networks—if you would like to inspect and control the applications that traverse your network, for any unknown traffic, you can record a packet capture. If the packet capture reveals that the application is a commercial application, you can submit this packet capture to Palo Alto Networks for App-ID development. If it is an internal application, you can create a custom App-ID and/or define an application override policy.
- [Create a Custom Application](#) with a signature and attach it to a security policy, or create a custom application and define an application override policy—A custom application allows you to customize the definition of the internal application—its characteristics, category and sub-category, risk, port, timeout—and exercise granular policy control in order to minimize the range of unidentified traffic on your network. Creating a custom application also allows you to correctly identify the application in the **ACC** and traffic logs and is useful in auditing/reporting on the applications on your network. For a custom application you can specify a signature and a pattern that uniquely identifies the application and attach it to a security policy that allows or denies the application.

Alternatively, if you would like the firewall to process the custom application using fast path (Layer-4 inspection instead of using App-ID for Layer-7 inspection), you can reference the custom application in an application override policy rule. An application override with a custom application will prevent the session from being processed by the App-ID engine, which is a Layer-7 inspection. Instead it forces the firewall to handle the session as a regular stateful inspection firewall at Layer-4, and thereby saves application processing time.

For example, if you build a custom application that triggers on a host header *www.mywebsite.com*, the packets are first identified as *web-browsing* and then are matched as your custom application (whose parent application is *web-browsing*). Because the parent application is *web-browsing*, the custom application is inspected at Layer-7 and scanned for content and vulnerabilities.

If you define an application override, the firewall stops processing at Layer-4. The custom application name is assigned to the session to help identify it in the logs, and the traffic is not scanned for threats.

For more details, refer to the following articles:

- [Identifying Unknown Applications](#)
- [Video: How to Configure a Custom App-ID](#)
- [Custom Application Signatures](#)

## Manage New App-IDs Introduced in Content Releases

Installing new App-IDs included in a content release version can sometimes cause a change in policy enforcement for the now uniquely-identified application. Before installing a new content release, review the policy impact for new App-IDs and stage any necessary policy updates. Assess the treatment an application receives both before and after the new content is installed. You can then modify existing security policy rules using the new App-IDs contained in a downloaded content release (prior to installing the App-IDs). This enables you to simultaneously update your security policies and install new content, and allows for a seamless shift in policy enforcement. Alternatively, you can also choose to disable new App-IDs when installing a new content release version; this enables protection against the latest threats, while giving you the flexibility to enable the new App-IDs after you've had the chance to prepare any policy changes.

The following options enable you to assess the impact of new App-IDs on existing policy enforcement, disable (and enable) App-IDs, and seamlessly update policy rules to secure and enforce newly-identified applications:

- ▲ [Review New App-IDs](#)
- ▲ [Disable or Enable App-IDs](#)
- ▲ [Prepare Policy Updates For Pending App-IDs](#)

## Review New App-IDs

Review new App-ID signatures introduced in a Applications and/or Threats content update. For each new application signature introduced, you can preview the App-ID details, including a description of the application identified by the App-ID, other existing App-IDs that the new signature is dependent on (such as SSL or HTTP), and the category the application traffic received before the introduction of the new App-ID (for example, an application might be classified as web-browsing traffic before a App-ID signature is introduced that uniquely identifies the traffic). After reviewing the description and details for a new App-ID signature, review the App-ID signature impact on existing policy enforcement. When new application signatures are introduced, the newly-identified application traffic might no longer match to policies that previously enforced the application. Reviewing the policy impact for new application signatures enables you to identify the policies that will no longer enforce the application when the new App-ID is installed.

After downloading a new content release version, review the new App-IDs included in the content version and assess the impact of the new App-IDs on existing policy rules:

- ▲ [Review New App-IDs Since Last Content Version](#)
- ▲ [Review New App-ID Impact on Existing Policy Rules](#)

## Review New App-IDs Since Last Content Version

### Review New App-IDs Available Since the Last Installed Content Release Version

- Step 1 Select **Device > Dynamic Updates** and select **Check Now** to refresh the list of available content updates.
- Step 2 **Download** the latest Applications and Threats content update. When the content update is downloaded, an **Apps** link will appear in the Features column for that content update.
- Step 3 Click the **Apps** link in the **Features** column to view details on newly-identified applications:

▼ Applications and Threats		Last checked:	2015/04/23 12:50:27 PDT	Schedule:	None
488-2590	panupv2-all-contents-488-2590	Apps, Threats	Full	23 MB	2015/02/24 16:25:58 PST
497-2683	panupv2-all-apps-497-2683	Apps	Full	25 MB	2015/04/23 01:05:37 PDT

A list of App-IDs shows all new App-IDs introduced from the content version installed on the firewall, to the selected **Content Version**.

App-ID details that you can use to assess possible impact to policy enforcement include:

- **Depends on**—Lists the application signatures that this App-ID relies on to uniquely identify the application. If one of the application signatures listed in the **Depends On** field is disabled, the dependent App-ID is also disabled.
- **Previously Identified As**—Lists the App-IDs that matched to the application before the new App-ID was installed to uniquely identify the application.
- **App-ID Enabled**—All App-IDs display as enabled when a content release is downloaded, unless you choose to manually disable the App-ID signature before installing the content update (see [Disable or Enable App-IDs](#)).

Multi-vsyst firewalls display App-ID status as **vsys-specific**. This is because the status is not applied across virtual systems and must be individually enabled or disabled for each virtual system. To view the App-ID status for a specific virtual system, select **Objects > Applications**, select a **Virtual System**, and select the App-ID.

The screenshot shows the 'New Applications since last installed content' interface. On the left, a sidebar lists various application names. In the center, detailed information for the 'adobe-cloud' application is shown. The 'Previously Identified As' field is highlighted with a red box, showing 'ssl, web-browsing'. At the bottom right, the 'App-ID Enabled' field is also highlighted with a red box, showing 'yes'.

### Next Steps...

- [Disable or Enable App-IDs](#).
- [Prepare Policy Updates For Pending App-IDs](#).

## Review New App-ID Impact on Existing Policy Rules

### Review the Impact of New App-ID Signatures on Existing Policy Rules

**Step 1** Select **Device > Dynamic Updates**.

**Step 2** You can review the policy impact of new content release versions that are downloaded to the firewall. **Download** a new content release version, and click the **Review Policies** in the Action column. The **Policy review based on candidate configuration** dialog allows you to filter by **Content Version** and view App-IDs introduced in a specific release (you can also filter the policy impact of new App-IDs according to **Rulebase** and **Virtual System**).

**Step 3** Select a new App-ID from the **Application** drop-down to view policy rules that currently enforce the application. The rules displayed are based on the applications signatures that match to the application before the new App-ID is installed (view application details to see the list of application signatures that an application was **Previously Identified As** before the new App-ID).

**Step 4** Use the detail provided in the policy review to plan policy rule updates to take effect when the App-ID is installed and enabled to uniquely identify the application.

You can continue to [Prepare Policy Updates For Pending App-IDs](#), or you can directly add the new App-ID to policy rules that the application was previously matched to by continuing to use the policy review dialog.

In the following example, the new App-ID adobe-cloud is introduced in a content release. Adobe-cloud traffic is currently identified as SSL and web-browsing traffic. Policy rules configured to enforce SSL or web-browsing traffic are listed to show what policy rules will be affected when the new App-ID is installed. In this example, the rule Allow SSL App currently enforces SSL traffic. To continue to allow adobe-cloud traffic when it is uniquely identified, and no longer identified as SSL traffic.

Policy review based on candidate configuration											
Content Version: 497-2683		Rulebase: Security		Virtual System: AAA (vsys2)		Application: adobe-cloud		Include rules with Application 'Any'			
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Allow SSL App	none	universal	trust	any	any	any	untrust	any	ssl	application-d...	Allow

Add the new App-ID to existing policy rules, to allow the application traffic to continue to be enforced according to your existing security requirements when the App-ID is installed.

In this example, to continue to allow adobe-cloud traffic when it is uniquely identified by the new App-ID, and no longer identified as SSL traffic, add the new App-ID to the security policy rule Allow SSL App.

Policy review based on candidate configuration											
Content Version: 497-2683		Rulebase: Security		Virtual System: AAA (vsys2)		Application: adobe-cloud		Include rules with Application 'Any'			
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Allow SSL App	none	universal	trust	any	any	any	untrust	any	ssl	application-d...	Allow

The policy rule updates take effect only when the application updates are installed.

#### Next Steps...

- [Disable or Enable App-IDs](#).
- [Prepare Policy Updates For Pending App-IDs](#).

## Disable or Enable App-IDs

Disable new App-IDs included in a content release to immediately benefit from protection against the latest threats while continuing to have the flexibility to later enable App-IDs after preparing necessary policy updates. You can disable all App-IDs introduced in a content release, set scheduled content updates to automatically disable new App-IDs, or disable App-IDs for specific applications.

Policy rules referencing App-IDs only match to and enforce traffic based on enabled App-IDs.

Certain App-IDs cannot be disabled and only allow a status of enabled. App-IDs that cannot be disabled included some application signatures implicitly used by other App-IDs (such as unknown-tcp). Disabling a base App-ID could cause App-IDs which depend on the base App-ID to also be disabled. For example, disabling facebook-base will disable all other Facebook App-IDs.

### Disable and Enable App-IDs

Disable all App-IDs in a content release or for scheduled content updates.	<ul style="list-style-type: none"><li>To disable all new App-IDs introduced in a content release, select <b>Device &gt; Dynamic Updates</b> and <b>Install</b> an Application and Threats content release. When prompted, select <b>Disable new apps in content update</b>. Select the check box to disable apps and continue installing the content update; this allows you to be protected against threats, and gives you the option to enable the apps at a later time.</li><li>On the <b>Device &gt; Dynamic Updates</b> page, select Schedule. Choose to <b>Disable new apps in content update</b> for downloads and installations of content releases.</li></ul>
Disable App-IDs for one application or multiple applications at a single time.	<ul style="list-style-type: none"><li>To quickly disable a single application or multiple applications at the same time, click <b>Objects &gt; Applications</b>. Select one or more application check box and click <b>Disable</b>.</li><li>To review details for a single application, and then disable the App-ID for that application, select <b>Objects &gt; Applications</b> and <b>Disable App-ID</b>. You can use this step to disable both pending App-IDs (where the content release including the App-ID is downloaded to the firewall but not installed) or installed App-IDs.</li></ul>
Enable App-IDs.	Enable App-IDs that you previously disabled by selecting <b>Objects &gt; Applications</b> . Select one or more application check box and click <b>Enable</b> or open the details for a specific application and click <b>Enable App-ID</b> .

## Prepare Policy Updates For Pending App-IDs

You can now stage seamless policy updates for new App-IDs. Release versions prior to PAN-OS 7.0 required you to install new App-IDs (as part of a content release) and then make necessary policy updates. This allowed for a period during which the newly-identified application traffic was not enforced, either by existing rules (that the traffic had matched to before being uniquely identified) or by rules that had yet to be created or modified to use the new App-ID.

*Pending* App-IDs can now be added to policy rules to prevent gaps in policy enforcement that could occur during the period between installing a content release and updating security policy. Pending App-IDs includes App-IDs that have been manually disabled, or App-IDs that are downloaded to the firewall but not installed. Pending App-IDs can be used to update policies both before and after installing a new content release. Though they can be added to policy rules, pending App-IDs are not enforced until the App-IDs are both installed and enabled on the firewall.

The names of App-IDs that have been manually disabled display as gray and italicized, to indicate the disabled status:

- Disabled App-ID listed on the **Objects > Applications** page:



- Disabled App-ID included in a security policy rule:



 App-IDs that are included in a downloaded content release version might have an App-ID status of enabled, but App-IDs are not enforced until the corresponding content release version is installed.

## Perform Seamless Policy Updates for New App-IDs

To install the content release version now and then update policies:

-  Do this to benefit from new threat signatures immediately, while you review new application signatures and update your policies.
- 1. Select **Device > Dynamic Updates** and **Download** the latest content release version.
- 2. Review the [Impact of New App-ID Signatures on Existing Policy Rules](#) to assess the policy impact of new App-IDs.
- 3. **Install** the latest content release version. Before the content release is installed, you are prompted to **Disable new apps in content update**. Select the check box and continue to install the content release. Threat signatures included in the content release will be installed and effective, while new or updated App-IDs are disabled.
- 4. Select **Policies** and update **Security, QoS, and Policy Based Forwarding** rules to match to and enforce the now uniquely identified application traffic, using the pending App-IDs.
- 5. Select **Objects > Applications** and select one or multiple disabled App-IDs and click **Enable**.
- 6. **Commit** your changes to seamlessly update policy enforcement for new App-IDs.

To update policies now and then install the content release version:

- 1. Select **Device > Dynamic Updates** and **Download** the latest content release version.
- 2. Review the [Impact of New App-ID Signatures on Existing Policy Rules](#) to assess the policy impact of new App-IDs.
- 3. While reviewing the policy impact for new App-IDs, you can use the **Policy Review based on candidate configuration** to add a new App-ID to existing policy rules: .
- 4. The new App-ID is added to the existing rules as a disabled App-ID.
- 5. Continue to review the policy impact for all App-IDs included in the latest content release version by selecting App-IDs in the **Applications** drop-down. Add the new App-IDs to existing policies as needed. Click **OK** to save your changes.
- 6. **Install** the latest content release version.
- 7. **Commit** your changes to seamlessly update policy enforcement for new App-IDs.

# Use Application Objects in Policy

- ▲ Create an Application Group
- ▲ Create an Application Filter
- ▲ Create a Custom Application

## Create an Application Group

An application group is an object that contains applications that you want to treat similarly in policy. Application groups are useful for enabling access to applications that you explicitly sanction for use within your organization. Grouping sanctioned applications simplifies administration of your rulebases.: instead of having to update individual policy rules when there is a change in the applications you support, you can instead update only the affected application groups.

When deciding how to group applications, consider how you plan to enforce access to your sanctioned applications and create an application group that aligns with each of your policy goals. For example, you might have some applications that you will only allow your IT administrators to access, and other applications that you want to make available for any known user in your organization. In this case, you would create separate application groups for each of these policy goals. Although you generally want to enable access to applications on the default port only, you may want to group applications that are an exception to this and enforce access to those applications in a separate rule.

---

### Create an Application Group

---

Step 1 Select **Objects > Application Groups**.

---

Step 2 **Add** a group and give it a descriptive **Name**.

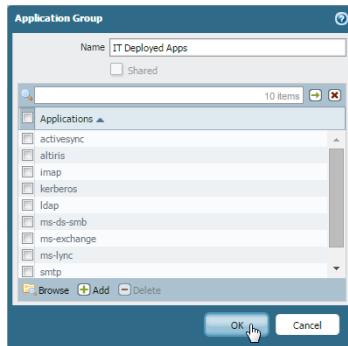
---

Step 3 (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.

---

Step 4 **Add** the applications you want in the group and then click **OK**.

---



Step 5 **Commit** the configuration.

---

## Create an Application Filter

An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category **business-systems** and the Subcategory **office-programs**. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.

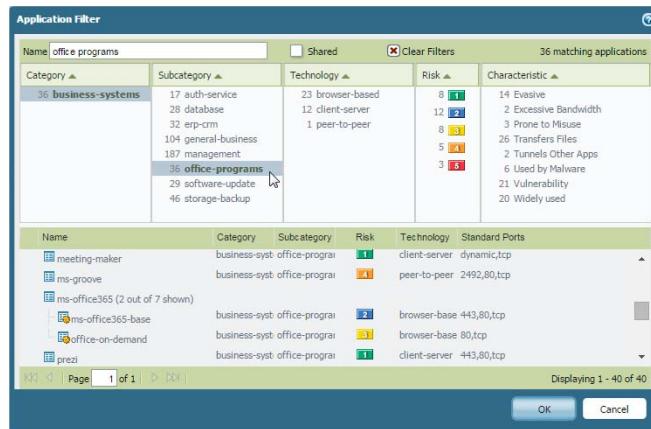
### Create an Application Filter

**Step 1** Select **Objects > Application Filters**.

**Step 2** Add a filter and give it a descriptive **Name**.

**Step 3** (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.

**Step 4** Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections. As you select values, notice that the list of matching applications at the bottom of the dialog narrows. When you have adjusted the filter attributes to match the types of applications you want to safely enable, click **OK**.



**Step 5** Commit the configuration.

## Create a Custom Application

To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic—tcp, udp or non-syn-tcp—in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.



If you are seeing unknown traffic for a commercial application that does not yet have an App-ID, you can submit a request for a new App-ID here:  
<http://researchcenter.paloaltonetworks.com/submit-an-application/>.

To ensure that your internal custom applications do not show up as unknown traffic, create a custom application. You can then exercise granular policy control over these applications in order to minimize the range of unidentified traffic on your network, thereby reducing the attack surface. Creating a custom application also allows you to correctly identify the application in the ACC and Traffic logs, which enables you to audit/report on the applications on your network.

To create a custom application, you must define the application attributes: its characteristics, category and sub-category, risk, port, timeout. In addition, you must define patterns or values that the firewall can use to match to the traffic flows themselves (the *signature*). Finally, you can attach the custom application to a security policy that allows or denies the application (or add it to an application group or match it to an application filter). You can also create custom applications to identify ephemeral applications with topical interest, such as ESPN3-Video for world cup soccer or March Madness.



In order to collect the right data to create a custom application signature, you'll need a good understanding of packet captures and how datagrams are formed. If the signature is created too broadly, you might inadvertently include other similar traffic; if it is defined too narrowly, the traffic will evade detection if it does not strictly match the pattern.

Custom applications are stored in a separate database on the firewall and this database is not impacted by the weekly App-ID updates.

The supported application protocol decoders that enable the firewall to detect applications that may be tunneling inside of the protocol include the following as of content update 424: HTTP, HTTPS, DNS, FTP, IMAP SMTP, Telnet, IRC (Internet Relay Chat), Oracle, RTMP, RTSP, SSH, GNU-Debugger, GIOP (Global Inter-ORB Protocol), Microsoft RPC, Microsoft SMB (also known as CIFS).

The following is a basic example of how to create a custom application.

## Create a Custom Application

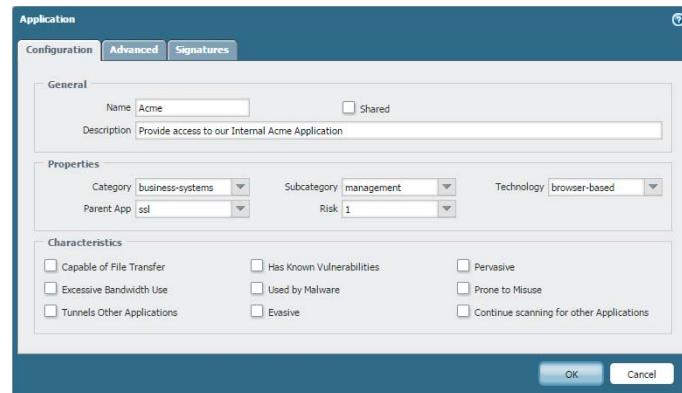
- Step 1** Gather information about the application that you will be able to use to write custom signatures.

To do this, you must have an understanding of the application and how you want to control access to it. For example, you may want to limit what operations users can perform within the application (such as uploading, downloading, or live streaming). Or you may want to allow the application, but enforce QoS policing.

- Capture application packets so that you can find unique characteristics about the application on which to base your custom application signature. One way to do this is to run a protocol analyzer, such as Wireshark, on the client system to capture the packets between the client and the server. Perform different actions in the application, such as uploading and downloading, so that you will be able to locate each type of session in the resulting packet captures (PCAPs).
- Because the firewall by default takes [packet captures for all unknown traffic](#), if the firewall is between the client and the server you can view the packet capture for the unknown traffic directly from the Traffic log.
- Use the packet captures to find patterns or values in the packet *contexts* that you can use to create signatures that will uniquely match the application traffic. For example, look for string patterns in HTTP response or request headers, URI paths, or hostnames. For information on the different string contexts you can use to create application signatures and where you can find the corresponding values in the packet, refer to [Creating Custom Threat Signatures](#).

- Step 2** Add the custom application.

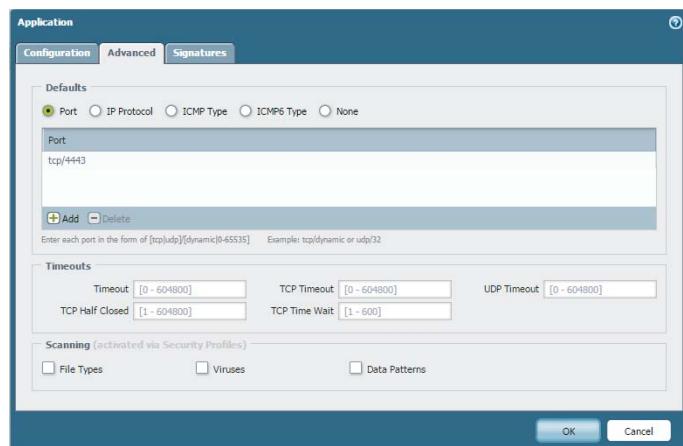
- Select **Objects > Applications** and click **Add**.
- On the **Configuration** tab, enter a **Name** and a **Description** for the custom application that will help other administrators understand why you created the application.
- (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.
- Define the application Properties and Characteristics.



### Create a Custom Application (Continued)

- Step 3** Define details about the application, such as the underlying protocol, the port number the application runs on, the timeout values, and any types of scanning you want to be able to perform on the traffic.
- On the **Advanced** tab, define settings that will allow the firewall to identify the application protocol:
- Specify the default ports or protocol that the application uses.
  - Specify the [session timeout](#) values. If you don't specify timeout values, the default timeout values will be used.
  - Indicate any type of additional scanning you plan to perform on the application traffic.

For example, to create a custom TCP-based application that runs over SSL, but uses port 4443 (instead of the default port for SSL, 443), you would specify the port number. By adding the port number for a custom application, you can create policy rules that use the default port for the application rather than opening up additional ports on the firewall. This improves your security posture.



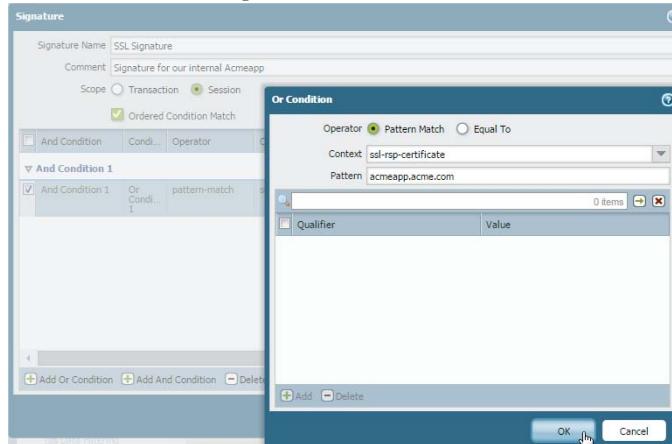
### Create a Custom Application (Continued)

- Step 4** Define the criteria that the firewall will use to match the traffic to the new application.

You will use the information you gathered from the packet captures to specify unique **string context values** that the firewall can use to match patterns in the application traffic.

1. On the **Signatures** tab, click **Add** and define a **Signature Name** and optionally a **Comment** to provide information about how you intend to use this signature.
2. Specify the **Scope** of the signature: whether it matches to a full **Session** or a single **Transaction**.
3. Specify conditions to define signatures by clicking **Add And Condition** or **Add Or Condition**.
4. Select an **Operator** to define the type of match conditions you will use: **Pattern Match** or **Equal To**.
  - If you selected **Pattern Match**, select the **Context** and then use a regular expression to define the **Pattern** to match the selected **context**. Optionally, click **Add** to define a qualifier/value pair. The **Qualifier** list is specific to the **Context** you chose.
  - If you selected **Equal To**, select the **Context** and then use a regular expression to define the **Position** of the bytes in the packet header to use match the selected **context**. Choose from **first-4bytes** or **second-4bytes**. Define the 4-byte hex value for the **Mask** (for example, 0xffffffff00) and **Value** (for example, 0xaabbccdd).

For example, if you are creating a custom application for one of your internal applications, you could use the **ssl-rsp-certificate Context** to define a pattern match for the certificate response message of a SSL negotiation from the server and create a **Pattern** to match the commonName of the server in the message as shown here:



5. Repeat step 3 and 4 for each matching condition.
6. If the order in which the firewall attempts to match the signature definitions is important, make sure the **Ordered Condition Match** check box is selected and then order the conditions so that they are evaluated in the appropriate order. Select a condition or a group and click **Move Up** or **Move Down**. You cannot move conditions from one group to another.
7. Click **OK** to save the signature definition.

Create a Custom Application (Continued)	
Step 5 Save the application.	<ol style="list-style-type: none"><li>1. Click <b>OK</b> to save the custom application definition.</li><li>2. Click <b>Commit</b>.</li></ol>
Step 6 Validate that traffic matches the custom application as expected.	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b> and <b>Add</b> a security policy rule to allow the new application.</li><li>2. Run the application from a client system that is between the firewall and the application and then check the Traffic logs (<b>Monitor &gt; Traffic</b>) to make sure that you see traffic matching the new application (and that it is being handled per your policy rule).</li></ol>

## Applications with Implicit Support

When creating a policy to allow specific applications, you must also be sure that you are allowing any other applications on which the application depends. In many cases, you do not have to explicitly allow access to the dependent applications in order for the traffic to flow because the firewall is able to determine the dependencies and allow them implicitly. This implicit support also applies to [custom applications](#) that are based on HTTP, SSL, MS-RPC, or RTSP. Applications for which the firewall cannot determine dependent applications on time will require that you explicitly allow the dependent applications when defining your policies. You can determine application dependencies in [Applipedia](#).

The following table lists the applications for which the firewall has implicit support (as of [Content Update 557](#)).

**Table: Applications with Implicit Support**

Application	Implicitly Supports
360-safeguard-update	http
apple-update	http
apt-get	http
as2	http
avg-update	http
avira-antivir-update	http, ssl
blokus	rtmp
bugzilla	http
clubcooee	http
corba	http
cubby	http, ssl
dropbox	ssl
esignal	http
evernote	http, ssl
ezhelp	http
facebook	http, ssl
facebook-chat	jabber
facebook-social-plugin	http
fastviewer	http, ssl
forticlient-update	http
good-for-enterprise	http, ssl
google-cloud-print	http, ssl, jabber
google-desktop	http

Application	Implicitly Supports
google-talk	jabber
google-update	http
gotomypc-desktop-sharing	citrix-jedi
gotomypc-file-transfer	citrix-jedi
gotomypc-printing	citrix-jedi
hipchat	http
iheartradio	ssl, http, rtmp
infront	http
instagram	http, ssl
issuu	http, ssl
java-update	http
jepptech-updates	http
kerberos	rpc
kik	http, ssl
lastpass	http, ssl
logmein	http, ssl
mcafee-update	http
megaupload	http
metatrader	http
mocha-rdp	t_120
mount	rpc
ms-frs	msrpc
ms-rdp	t_120
ms-scheduler	msrpc
ms-service-controller	msrpc
nfs	rpc
oovoo	http, ssl
paloalto-updates	ssl
panos-global-protect	http
panos-web-interface	http
pastebin	http
pastebin-posting	http

Application	Implicitly Supports
pinterest	http, ssl
portmapper	rpc
prezi	http, ssl
rdp2tcp	t_120
renren-im	jabber
roboform	http, ssl
salesforce	http
stumbleupon	http
supremo	http
symantec-av-update	http
trendmicro	http
trillian	http, ssl
twitter	http
whatsapp	http, ssl
xm-radio	rtsp

## Application Level Gateways

The Palo Alto Networks firewall does not classify traffic by port and protocol; instead it identifies the application based on its unique properties and transaction characteristics using the App-ID technology. Some applications, however, require the firewall to dynamically open *pinholes* to establish the connection, determine the parameters for the session and negotiate the ports that will be used for the transfer of data; these applications use the application-layer payload to communicate the dynamic TCP or UDP ports on which the application opens data connections. For such applications, the firewall serves as an Application Level Gateway (ALG), and it opens a pinhole for a limited time and for exclusively transferring data or control traffic. The firewall also performs a NAT rewrite of the payload when necessary.

As of Content Release version 504, the Palo Alto Networks firewall provides NAT ALG support for the following protocols: FTP, H.225, H.248, MGCP, MySQL, Oracle/SQLNet/TNS, RPC, RTSP, SCCP, SIP, and UNISim.



When the firewall serves as an ALG for the Session Initiation Protocol (SIP), by default it performs NAT on the payload and opens dynamic pinholes for media ports. In some cases, depending on the SIP applications in use in your environment, the SIP endpoints have NAT intelligence embedded in their clients. In such cases, you might need to disable the SIP ALG functionality to prevent the firewall from modifying the signaling sessions. When SIP ALG is disabled, if App-ID determines that a session is SIP, the payload is not translated and dynamic pinholes are not opened. See [Disable the SIP Application-level Gateway \(ALG\)](#).

The firewall provides IPv6-to-IPv6 Network Prefix Translation (NPTv6) ALG support for the following protocols: FTP, Oracle, and RTSP. The SIP ALG is not supported for NPTv6 or NAT64.

## Disable the SIP Application-level Gateway (ALG)

The Palo Alto Networks firewall uses the Session Initiation Protocol (SIP) application-level gateway (ALG) to open dynamic pinholes in the firewall where NAT is enabled. However, some applications—such as VoIP—have NAT intelligence embedded in the client application. In these cases, the SIP ALG on the firewall can interfere with the signaling sessions and cause the client application to stop working.

One solution to this problem is to define an Application Override Policy for SIP, but using this approach disables the App-ID and threat detection functionality. A better approach is to disable the SIP ALG, which does not disable App-ID or threat detection.

The following procedure describes how to disable the SIP ALG.

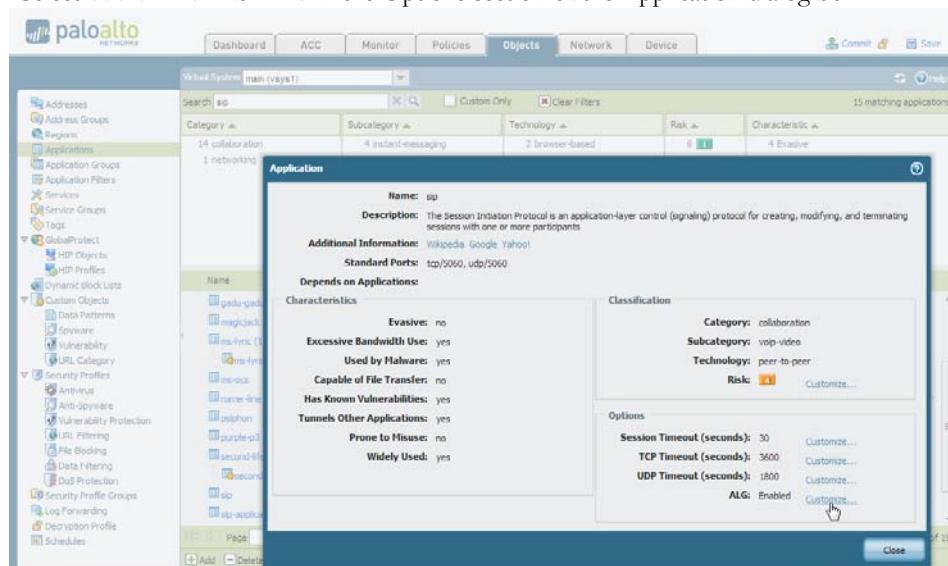
### Disable the SIP ALG

**Step 1** Select **Objects > Applications**.

**Step 2** Select the **sip** application.

You can type **sip** in the **Search** box to help find the sip application.

**Step 3** Select **Customize...** for **ALG** in the Options section of the Application dialog box.



**Step 4** Select the **Disable ALG** check box in the Application - **sip** dialog box and click **OK**.



**Step 5** Close the Application dialog box and **Commit** the change.





# Threat Prevention

---

---

The Palo Alto Networks next-generation firewall protects and defends your network from commodity threats and advanced persistent threats (APTs). The firewall's multi-pronged detection mechanisms include a signature-based (IPS/Command and Control/Antivirus) approach, heuristics-based (bot detection) approach, sandbox-based (WildFire) approach, and Layer 7 protocol analysis-based (App-ID) approach.

Commodity threats are exploits that are less sophisticated and more easily detected and prevented using a combination of the antivirus, anti-spyware, vulnerability protection and the URL filtering/Application identification capabilities on the firewall.

Advanced threats are perpetuated by organized cyber criminals or malicious groups that use sophisticated attack vectors to target your network, most commonly for intellectual property theft and financial data theft. These threats are more evasive and require intelligent monitoring mechanisms for detailed host and network forensics on malware. The Palo Alto Networks next-generation firewall in conjunction with [WildFire](#) and [Panorama](#) provides a comprehensive solution that intercepts and breaks the attack chain and provides visibility to prevent security infringement on your network—including mobile and virtualized—infrastructure.

- ▲ [Set Up Security Profiles and Policies](#)
- ▲ [Prevent Brute Force Attacks](#)
- ▲ [Customize the Action and Trigger Conditions for a Brute Force Signature](#)
- ▲ [Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions](#)
- ▲ [Enable Passive DNS Collection for Improved Threat Intelligence](#)
- ▲ [Use DNS Queries to Identify Infected Hosts on the Network](#)
- ▲ [Content Delivery Network Infrastructure for Dynamic Updates](#)
- ▲ [Threat Prevention Resources](#)

# Set Up Security Profiles and Policies

The following sections provide basic threat prevention configuration examples:

- ▲ [Set Up Antivirus, Anti-Spyware, and Vulnerability Protection](#)
- ▲ [Set Up Data Filtering](#)
- ▲ [Set Up File Blocking](#)

For information on controlling web access as part of your threat prevention strategy, see [URL Filtering](#).

## Set Up Antivirus, Anti-Spyware, and Vulnerability Protection

The following describes the steps needed to set up the default Antivirus, Anti-Spyware, and Vulnerability Protection [Security Profiles](#).



All anti-spyware and vulnerability protection signatures have a default action defined by Palo Alto Networks. You can view the default action by navigating to **Objects > Security Profiles > Anti-Spyware** or **Objects > Security Profiles > Vulnerability Protection** and then selecting a profile. Click the **Exceptions** tab and then click **Show all signatures** and you will see a list of the signatures with the default action in the Action column. To change the default action, you must create a new profile and then create rules with a non-default action, and/or add individual signature exceptions to **Exceptions** in the profile.

### Set up Antivirus/Anti-Spyware/Vulnerability Protection

<b>Step 1</b> Verify that you have a Threat Prevention license.	<ul style="list-style-type: none"><li>• The Threat Prevention license bundles the antivirus, anti-spyware, and the vulnerability protection features in one license.</li><li>• Select <b>Device &gt; Licenses</b> to verify that the <b>Threat Prevention</b> license is installed and check the expiration date.</li></ul>
<b>Step 2</b> Download the latest antivirus threat signatures.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Dynamic Updates</b> and click <b>Check Now</b> at the bottom of the page to retrieve the latest signatures. In the <b>Actions</b> column, click <b>Download</b> to install the latest Antivirus and Applications and Threats signatures.</li></ol>
<b>Step 3</b> Schedule signature updates.	<ol style="list-style-type: none"><li>1. From <b>Device &gt; Dynamic Updates</b>, click the text to the right of <b>Schedule</b> to automatically retrieve signature updates for <b>Antivirus</b> and <b>Applications and Threats</b>.</li><li>2. Specify the frequency and timing for the updates and whether the update will be downloaded and installed or only downloaded. If you select <b>Download Only</b>, you would need to manually go in and click the <b>Install</b> link in the <b>Action</b> column to install the signature. When you click <b>OK</b>, the update is scheduled. No commit is required.</li><li>3. (Optional) You can also enter the number of hours in the <b>Threshold</b> field to indicate the minimum age of a signature before a download will occur. For example, if you entered <b>10</b>, the signature must be at least 10 hours old before it will be downloaded, regardless of the schedule.</li><li>4. In an HA configuration, you can also click the <b>Sync To Peer</b> option to synchronize the content update with the HA peer after download/install. This will not push the schedule settings to the peer device, you need to configure the schedule on each device.</li></ol>

## Set up Antivirus/Anti-Spyware/Vulnerability Protection (Continued)

### Best Practices for Antivirus Schedules

The general recommendation for antivirus signature update schedules is to perform a **download-and-install** on a daily basis for antivirus and weekly for applications and vulnerabilities.

### Recommendations for HA Configurations:

- **Active/Passive HA**—If the MGT port is used for antivirus signature downloads, you should configure a schedule on both devices and both devices will download/install independently. If you are using a data port for downloads, the passive device will not perform downloads while it is in the passive state. In this case you would set a schedule on both devices and then select the **Sync To Peer** option. This will ensure that whichever device is active, the updates will occur and will then push to the passive device.
- **Active/Active HA**—If the MGT port is used for antivirus signature downloads on both devices, then schedule the download/install on both devices, but do not select the **Sync To Peer** option. If you are using a data port, schedule the signature downloads on both devices and select **Sync To Peer**. This will ensure that if one device in the active/active configuration goes into the active-secondary state, the active device will download/install the signature and will then push it to the active-secondary device.

**Step 4** Attach the security profiles to a security policy.

1. Select **Policies > Security**, select the desired policy to modify it and then click the **Actions** tab.
2. In **Profile Settings**, click the drop-down next to each security profile you would like to enable. In this example we choose default for **Antivirus, Vulnerability Protection, and Anti-Spyware**.



If no security profiles have been previously defined, select **Profiles** from the **Profile Type** drop-down. You will then see the list of options to select the security profiles.

**Step 5** Save the configuration.

Click **Commit**.

## Set Up Data Filtering

The following describes the steps needed to configure a data filtering profile that will detect Social Security Numbers and a custom pattern identified in .doc and .docx documents.

Data Filtering Configuration Example	
Step 1 Create a Data Filtering security profile.	<ol style="list-style-type: none"><li>1. Select <b>Objects &gt; Security Profiles &gt; Data Filtering</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> and a <b>Description</b> for the profile. In this example the name is <i>DF_Profile1</i> with the description <i>Detect Social Security Numbers</i>.</li><li>3. (Optional) If you want to collect data that is blocked by the filter, select the <b>Data Capture</b> check box.  You must set a password as described in <a href="#">Step 2</a> if you are using the data capture feature.</li></ol>
Step 2 (Optional) Secure access to the data filtering logs to prevent other administrators from viewing sensitive data.  When you enable this option, you will be prompted for the password when you view logs in <b>Monitor &gt; Logs &gt; Data Filtering</b> .	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Content-ID</b>.</li><li>2. Click <b>Manage Data Protection</b> in the Content-ID Features section.</li><li>3. Set the password that will be required to view the data filtering logs.</li></ol>

### Data Filtering Configuration Example (Continued)

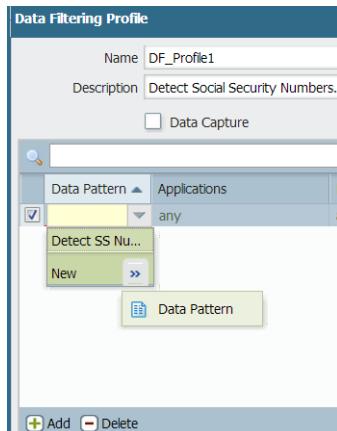
- Step 3** Define the data pattern that will be used in the Data Filtering Profile.

In this example, we will use the keyword **confidential** and will set the option to search for SSN numbers with dashes (Example - 987-654-4320).



It is helpful to set the appropriate thresholds and define keywords within documents to reduce false positives.

- From the Data Filtering Profile page click **Add** and select **New** from the **Data Pattern** drop-down. You can also configure data patterns from **Objects > Custom Signatures > Data Patterns**.
- For this example, name the Data Pattern signature **Detect SS Numbers** and add the description **Data Pattern to detect Social Security numbers**.
- In the **Weight** section for **SSN#** enter 3. See **Weight and Threshold Values** for more details.

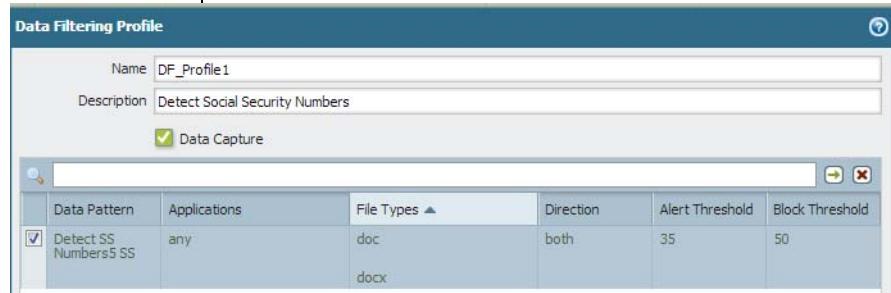


- (Optional) You can also set **Custom Patterns** that will be subject to this profile. In this case, you specify a pattern in the custom patterns **Regex** field and set a weight. You can add multiple match expressions to the same data pattern profile. In this example, we will create a **Custom Pattern** named **SSN\_Custom** with a custom pattern of **confidential** (the pattern is case sensitive) and use a weight of **20**. The reason we use the term **confidential** in this example is because we know that our social security Word docs contain this term, so we define that specifically.



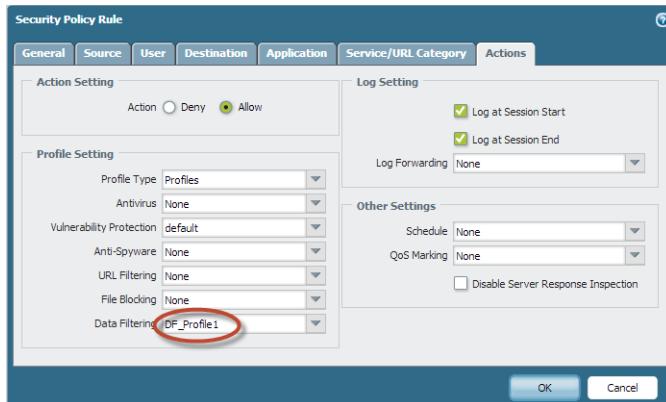
### Data Filtering Configuration Example (Continued)

- |   |   |
|---|---|
| <p><b>Step 4</b> Specify which applications to filter and set the file types.</p>         | <ol style="list-style-type: none"> <li>1. Set <b>Applications</b> to <b>Any</b>. This will detect any supported application such as: web-browsing, FTP, or SMTP. If you want to narrow down the application, you can select it from the list. For applications such as Microsoft Outlook Web App that uses SSL, you will need to enable decryption. Also make sure you understand the naming for each application. For example, Outlook Web App, which is the Microsoft name for this application is identified as the application <b>outlook-web</b> in the PAN-OS list of applications. You can check the logs for a given application to identify the name defined in PAN-OS.</li> <li>2. Set <b>File Types</b> to <b>doc</b> and <b>docx</b> to only scan doc and docx files.</li> </ol>  |
| <p><b>Step 5</b> Specify the direction of traffic to filter and the threshold values.</p> | <ol style="list-style-type: none"> <li>1. Set the <b>Direction</b> to <b>Both</b>. Files that are uploaded or downloaded will be scanned.</li> <li>2. Set the <b>Alert Threshold</b> to <b>35</b>. In this case, an alert will be triggered if 5 instances of Social Security Numbers exist and 1 instance of the term <b>confidential</b> exists. The formula is 5 SSN instances with a weight of 3 = 15 plus 1 instance of the term confidential with a weight of 20 = 35.</li> <li>3. Set the <b>Block Threshold</b> to <b>50</b>. The file will be blocked if the threshold of 50 instances of a SSN and/or the term confidential exists in the file. In this case, if the doc contained 1 instance of the word <b>confidential</b> with a weight of 20 that equals 20 toward the threshold, and the doc has 15 Social Security Numbers with a weight of 3 that equals 45. Add 20 and 45 and you have 65, which will exceed the block threshold of 50.</li> </ol> |



**Data Filtering Configuration Example (Continued)**

- Step 6** Attach the Data Filtering profile to the security rule.
1. Select **Policies > Security** and select the security policy rule to which to apply the profile.
  2. Click the security policy rule to modify it and then click the **Actions** tab. In the **Data Filtering** drop-down, select the new data filtering profile you created and then click **OK** to save. In this example, the data filtering rule name is **DF\_Profile1**.



- Step 7** **Commit** the configuration.

- Step 8** Test the data filtering configuration.

If you have problems getting Data Filtering to work, you can check the Data Filtering log or the Traffic log to verify the application that you are testing with and make sure your test document has the appropriate number of unique Social Security Number instances. For example, an application such as Microsoft Outlook Web App may seem to be identified as web-browsing, but if you look at the logs, the application is **outlook-web**. Also increase the number of SSNs, or your custom pattern to make sure you are hitting the thresholds.

When testing, you must use real Social Security Numbers and each number must be unique. Also, when defining Custom Patterns as we did in this example with the word **confidential**, the pattern is case sensitive. To keep your test simple, you may want to just test using a data pattern first, then test using SSNs.

1. Access a client PC in the trust zone of the firewall and send an HTTP request to upload a .doc or .docx file that contains the exact information you defined for filtering.
2. Create a Microsoft Word document with one instance of the term **confidential** and five Social Security numbers with dashes.
3. Upload the file to a website. Use an HTTP site unless you have decryption configured, in which case you can use HTTPS.
4. Select **Monitoring > Logs > Data Filtering** logs.
5. Locate the log that corresponds to the file you just uploaded. To help filter the logs, use the source of your client PC and the destination of the web server. The action column in the log will show **reset-both**. You can now increase the number of Social Security Numbers in the document to test the block threshold.

	Receive Time	File Name	Name	From Zone	To Zone	Source	Sou. User	Destination	To Port	Application
	10/25 14:03:06	DataFilter-Test.docx	Detect SS Numbers5 SS	I3-vlan-trust	I3-untrust	192.168.2.10		10.101.2.49	443	clearspace
	10/25 14:00:14	1351198789213	Detect SS Numbers5 SS	I3-vlan-trust	I3-untrust	192.168.2.10		10.101.2.49	443	clearspace

## Set Up File Blocking

This example will describe the basic steps needed to set up file blocking. In this configuration, we will configure the options needed to prompt users to continue before downloading .exe files from websites. When testing this example, be aware that you may have other systems between you and the source that may be blocking content.

Configure File Blocking	
Step 1 Create the file blocking profile.	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Security Profiles &gt; File Blocking</b> and click <b>Add</b>.</li> <li>Enter a <b>Name</b> for the file blocking profile, for example <i>Block_EXE</i>. Optionally enter a <b>Description</b>, such as <i>Block users from downloading exe files from websites</i>.</li> </ol>
Step 2 Configure the file blocking options.	<ol style="list-style-type: none"> <li>Click <b>Add</b> to define the profile settings.</li> <li>Enter a <b>Name</b>, such as <i>BlockEXE</i>.</li> <li>Set the <b>Applications</b> for filtering, for example <b>web-browsing</b>.</li> <li>Set <b>File Types</b> to <b>exe</b>.</li> <li>Set the <b>Direction</b> to <b>download</b>.</li> <li>Set the <b>Action</b> to <b>continue</b>. By choosing the continue option, users will be prompted with a response page prompting them to click continue before the file will be downloaded.</li> </ol>
Step 3 Apply the file blocking profile to a security policy.	<p>7. Click <b>OK</b> to save the profile.</p> <ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and either select an existing policy or create a new policy as described in <a href="#">Set Up Basic Security Policies</a>.</li> <li>Click the <b>Actions</b> tab within the policy rule.</li> <li>In the Profile Settings section, click the drop-down and select the file blocking profile you configured. In this case, the profile name is <i>Block_EXE</i>.</li> <li><b>Commit</b> the configuration.</li> </ol> <p>If no security profiles have been previously defined, select the <b>Profile Type</b> drop-down and select <b>Profiles</b>. You will then see the list of options to select the security profiles.</p>

## Configure File Blocking (Continued)

**Step 4** To test your file blocking configuration, access a client PC in the trust zone of the firewall and attempt to download an .exe file from a website in the untrust zone. A response page should display. Click **Continue** to download the file. You can also set other actions, such as alert or block, which will not provide a continue page to the user. The following shows the default response page for File Blocking:

### Example: Default File Blocking Response Page

#### File Download Blocked

Access to the file you were trying to download has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

**File name:** Support\_services\_ds1.pdf

Please click **Continue** to download/upload the file.

**Step 5** (Optional) Define custom file blocking response pages (**Device > Response Pages**). This allows you to provide more information to users when they see a response page. You can include information such as company policy information and contact information for a Helpdesk.



When you create a file blocking profile with the action continue, you can only choose the application web-browsing. If you choose any other application, traffic that matches the security policy will not flow through the firewall due to the fact that the users will not be prompted with a continue page. Also, if the website uses HTTPS, you will need to have a decryption policy in place.

You may want to check your logs to confirm what application is being used when testing this feature. For example, if you are using Microsoft SharePoint to download files, even though you are using a web-browser to access the site, the application is actually sharepoint-base, or sharepoint-document. You may want to set the application type to **Any** for testing.

## Prevent Brute Force Attacks

A brute force attack uses a large volume of requests/responses from the same source or destination IP address to break into a system. The attacker employs a trial-and-error method to guess the response to a challenge or a request.

The Vulnerability Protection profile on the firewall includes signatures to protect you from brute force attacks. Each signature has an ID, Threat Name, Severity and is triggered when a pattern is recorded. The pattern specifies the conditions and interval at which the traffic is identified as a brute-force attack; some signatures are associated with another child signature that is of a lower severity and specifies the pattern to match against. When a pattern matches against the signature or child signature, it triggers the default action for the signature.

To enforce protection:

- Attach the vulnerability profile to a security rule. See [Set Up Antivirus, Anti-Spyware, and Vulnerability Protection](#).
- Install content updates that include new signatures to protect against emerging threats. See [Manage Content Updates](#).

# Customize the Action and Trigger Conditions for a Brute Force Signature

The firewall includes two types of predefined brute force signatures—parent signature and child signature. A child signature is a single occurrence of a traffic pattern that matches the signature. A parent signature is associated with a child signature and is triggered when multiple events occur within a time interval and match the traffic pattern defined in the child signature.

Typically, a child signature is of default action *allow* because a single event is not indicative of an attack. In most cases, the action for a child signature is set to allow so that legitimate traffic is not blocked and threat logs are not generated for non-noteworthy events. Therefore, Palo Alto Networks recommends that you only change the default action after careful consideration.

In most cases, the brute force signature is a noteworthy event because of its recurrent pattern. If you would like to customize the action for a brute-force signature, you can do one of the following:

- Create a rule to modify the default action for all signatures in the brute force category. You can define the action to allow, alert, block, reset, or drop the traffic.
- Define an exception for a specific signature. For example, you can search for a CVE and define an exception for it.

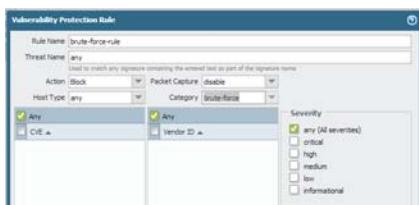
For a parent signature, you can modify both the trigger conditions and the action; for a child signature only the action can be modified.



To effectively mitigate an attack, the **block-ip address** action is recommended over the drop or reset action for most brute force signatures.

## Customize the Threshold and Action for a Signature

<b>Step 1</b> Create a new Vulnerability Protection profile.	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Security Profiles &gt; Vulnerability Protection</b>.</li> <li>2. Click <b>Add</b> and enter a <b>Name</b> for the Vulnerability Protection profile.</li> </ol>
<b>Step 2</b> Create a rule that defines the action for all signatures in a category.	<ol style="list-style-type: none"> <li>1. Select <b>Rules</b>, click <b>Add</b> and enter a <b>Name</b> for the rule.</li> <li>2. Set the <b>Action</b>. In this example, it is set to <b>Block</b>.</li> <li>3. Set <b>Category</b> to <b>brute-force</b>.</li> <li>4. (Optional) If blocking, specify whether to block server or client, the default is any.</li> <li>5. See <b>Step 3</b> to customize the action for a specific signature.</li> <li>6. See <b>Step 4</b> to customize the trigger threshold for a parent signature.</li> <li>7. Click <b>OK</b> to save the rule and the profile.</li> </ol>



### Customize the Threshold and Action for a Signature

**Step 3** (Optional) Customize the action for a specific signature.

1. Select **Exceptions** and click **Show all signatures** to find the signature you want to modify.

To view all the signatures in the brute-force category, search for (category contains 'brute-force').

2. To edit a specific signature, click the predefined default action in the **Action** column.

3. Set the action to **allow**, **alert** or **block-ip**.

4. If you select **block-ip**, complete these additional tasks:

a. Specify the **Time** period (in seconds) after which to trigger the action.

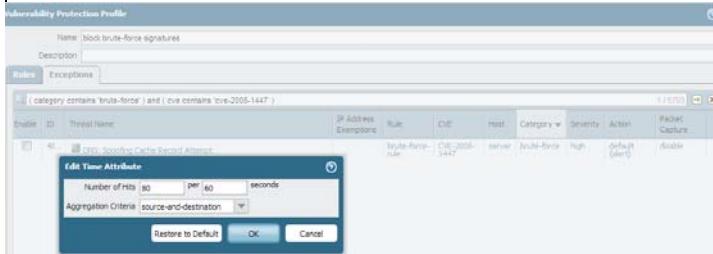
b. In the **Track By** field, define whether to block the IP address by **IP source** or by **IP source and destination**.

5. Click **OK**

6. For each modified signature, select the check box in the **Enable** column.

7. Click **OK**.

### Customize the Threshold and Action for a Signature

<p><b>Step 4</b> Customize the trigger conditions for a parent signature.</p> <p>A parent signature that can be edited is marked with this icon: .</p> <p>In this example, the search criteria was brute force category and CVE-2008-1447.</p>	<ol style="list-style-type: none"> <li>1. Click  to edit the time attribute and the aggregation criteria for the signature.</li> </ol>  <ol style="list-style-type: none"> <li>2. To modify the trigger threshold specify the <b>Number of Hits per x seconds</b>.</li> <li>3. Specify whether to aggregate the number of hits by <b>source</b>, <b>destination</b> or by <b>source and destination</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>
<p><b>Step 5</b> Attach this new profile to a security rule.</p>	
<p><b>Step 6</b> Save your changes.</p>	<ol style="list-style-type: none"> <li>1. Click <b>Commit</b>.</li> </ol>

# Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions

To monitor and protect your network from most Layer 4 and Layer 7 attacks, here are a few recommendations.

- Upgrade to the most current PAN-OS software version and content release version to ensure that you have the latest security updates. See [Manage Content Updates](#) and [Install Software Updates](#).
- For servers, create security policy rules to only allow the application(s) that you sanction on each server. Verify that the standard port for the application matches the listening port on the server. For example, to ensure that only SMTP traffic is allowed to your email server set the Application to smtp and the Service to application-default. If your server uses only a subset of the standard ports (for example, if your SMTP server uses only port 587 while the smtp application has standard ports defined as 25 and 587), you should create a new custom service that only includes port 587 and use that new service in your security policy rule instead of using application-default. Additionally, make sure to restrict access to specific source and destinations zones and sets of IP addresses.
- Attach the following security profiles to your security policies to provide signature-based protection.
  - Create a Vulnerability Protection profile to block all vulnerabilities with severity low and higher.
  - Create an Anti-Spyware profile to block all spyware.
  - Create an antivirus profile to block all content that matches an antivirus signature.
- Block all unknown applications/traffic using security policy. Typically, the only applications that are classified as unknown traffic are internal or custom applications on your network, or potential threats. Because unknown traffic can be a non-compliant application or protocol that is anomalous or abnormal, or a known application that is using non-standard ports, unknown traffic should be blocked. See [Manage Custom or Unknown Applications](#).
- Create a file blocking profile that blocks Portable Executable (PE) file types for Internet-based SMB (Server Message Block) traffic from traversing the trust to untrust zones, (ms-ds-smb applications).
- Create a zone protection profile that is configured to protect against packet-based attacks:
  - Remove TCP timestamps on SYN packets before the firewall forwards the packet—When you remove the TCP timestamp option in a SYN packet, the TCP stack on both ends of the TCP connection will not support TCP timestamps. Therefore, by disabling the TCP timestamp for a SYN packet, you can prevent an attack that uses different timestamps on multiple packets for the same sequence number.
  - Drop malformed packets.
  - Drop mismatched and overlapping TCP segments—By deliberately constructing connections with overlapping but different data in them, attackers can attempt to cause misinterpretation of the intent of the connection. This can be used to deliberately induce false positives or false negatives. An attacker can use IP spoofing and sequence number prediction to intercept a user's connection and inject his/her own data into the connection. PAN-OS uses this field to discard such frames with mismatched and overlapping data. The scenarios where the received segment will be discarded are when the segment received is contained within another segment, the segment received overlaps with part of another segment, or the segment completely contains another segment.

- Verify that support for IPv6 is enabled, if you have configured IPv6 addresses on your network hosts.

**(Network > Interfaces > Ethernet> IPv6)**

This allows access to IPv6 hosts and filters IPv6 packets that are encapsulated in IPv4 packets. Enabling support for IPv6 prevents IPv6 over IPv4 multicast addresses from being leveraged for network reconnaissance.

- Enable support for multicast traffic so that the firewall can enforce policy on multicast traffic. **(Network > Virtual Router > Multicast)**

- Enable the following CLI command to clear the URG bit flag in the TCP header and disallow out-of-band processing of packets.

The urgent pointer in the TCP header is used to promote a packet for immediate processing by removing it from the processing queue and expediting it through the TCP/IP stack on the host. This process is called out-of-band processing. Because the implementation of the urgent pointer varies by host, to eliminate ambiguity, use the following CLI command to disallow out-of-band processing; the out-of-band byte in the payload becomes part of the payload and the packet is not processed urgently. Making this change allows you to remove ambiguity in how the packet is processed on the firewall and the host, and the firewall sees the exact same stream in the protocol stack as the host for whom the packet is destined.

```
set deviceconfig setting tcp urgent-data clear
```

- If you configure the firewall to clear the URG bit flag and the packet has no other flags set in the TCP header, use the following CLI command to configure the firewall to drop packets with no flags:

```
set deviceconfig setting tcp drop-zero-flag yes
```

- Enable the following CLI command for disabling the bypass-exceed-queue.

The bypass exceed queue is required for out of order packets. This scenario is most common in an asymmetric environment where the firewall receives packets out of order. For identification of certain applications (App-ID) the firewall performs heuristic analysis. If the packets are received out of order, the data must be copied to a queue in order to complete the analysis for the application.

```
set deviceconfig setting application bypass-exceed-queue no
```

- Enable the following CLI commands for disabling the inspection of packets when the out-of-order packet limit is reached. The Palo Alto Networks firewall can collect up to 64 out-of-order packets per session. This counter identifies that packets have exceeded the 64-packet limit. When the bypass setting is set to **no**, the device drops the out-of-order packets that exceed the 64-packet limit. A commit is required.

```
set deviceconfig setting tcp bypass-exceed-oo-queue no  
set deviceconfig setting ctd tcp-bypass-exceed-queue no  
set deviceconfig setting ctd udp-bypass-exceed-queue no
```

- Enable the following CLI commands for checking the TCP timestamp. The TCP timestamp records when the segment was sent and allows the firewall to verify that the timestamp is valid for that session. Packets with invalid timestamps are dropped with this setting is enabled.

```
set deviceconfig setting tcp check-timestamp-option yes
```

- Disable the HTTP Range option. The HTTP Range option allows a client to fetch part of a file only. When a next-generation firewall in the path of a transfer identifies and drops a malicious file, it terminates the TCP session with a RST packet. If the web browser implements the HTTP Range option, it can start a new session to fetch only the remaining part of the file. This prevents the firewall from triggering the same signature again due to the lack of context into the initial session, while at the same time allowing the web browser to reassemble the file and deliver the malicious content. To prevent this, disable the HTTP Range option as follows:

```
set deviceconfig setting ctd skip-block-http-range no
```

# Enable Passive DNS Collection for Improved Threat Intelligence

Passive DNS is an opt-in feature that enables the firewall to act as a passive DNS sensor and send select DNS information to Palo Alto Networks for analysis in order to improve threat intelligence and threat prevention capabilities. The data collected includes non-recursive (i.e. originating from the local recursive resolver, not individual clients) DNS query and response packet payloads. Data submitted via the Passive DNS Monitoring feature consists solely of mappings of domain names to IP addresses. Palo Alto Networks retains no record of the source of this data and does not have the ability to associate it with the submitter at a future date.

The Palo Alto Networks threat research team uses this information to gain insight into malware propagation and evasion techniques that abuse the DNS system. Information gathered through this data collection is used to improve accuracy and malware detection abilities within PAN-DB URL filtering, DNS-based command-and-control signatures, and WildFire.

DNS responses are only forwarded to the Palo Alto Networks and will only occur when the following requirements are met:

- DNS response bit is set
- DNS truncated bit is not set
- DNS recursive bit is not set
- DNS response code is 0 or 3 (NX)
- DNS question count bigger than 0
- DNS Answer RR count is bigger than 0 or if it is 0, the flags need to be 3 (NX)
- DNS query record type are A, NS, CNAME, AAAA, MX

Passive DNS monitoring is disabled by default, but it is recommended that you enable it to facilitate enhanced threat intelligence. Use the following procedure to enable Passive DNS:

## Enable Passive DNS

**Step 1** Select **Objects > Security Profiles > Anti-Spyware**.

**Step 2** Select an existing profile to modify it or configure a new profile.



The Anti-Spyware profile must be attached to a security policy that governs your DNS server's external DNS traffic.

**Step 3** Select the **DNS Signatures** tab and click the **Enable Passive DNS Monitoring** check box.

**Step 4** Click **OK** and then **Commit**.

## Use DNS Queries to Identify Infected Hosts on the Network

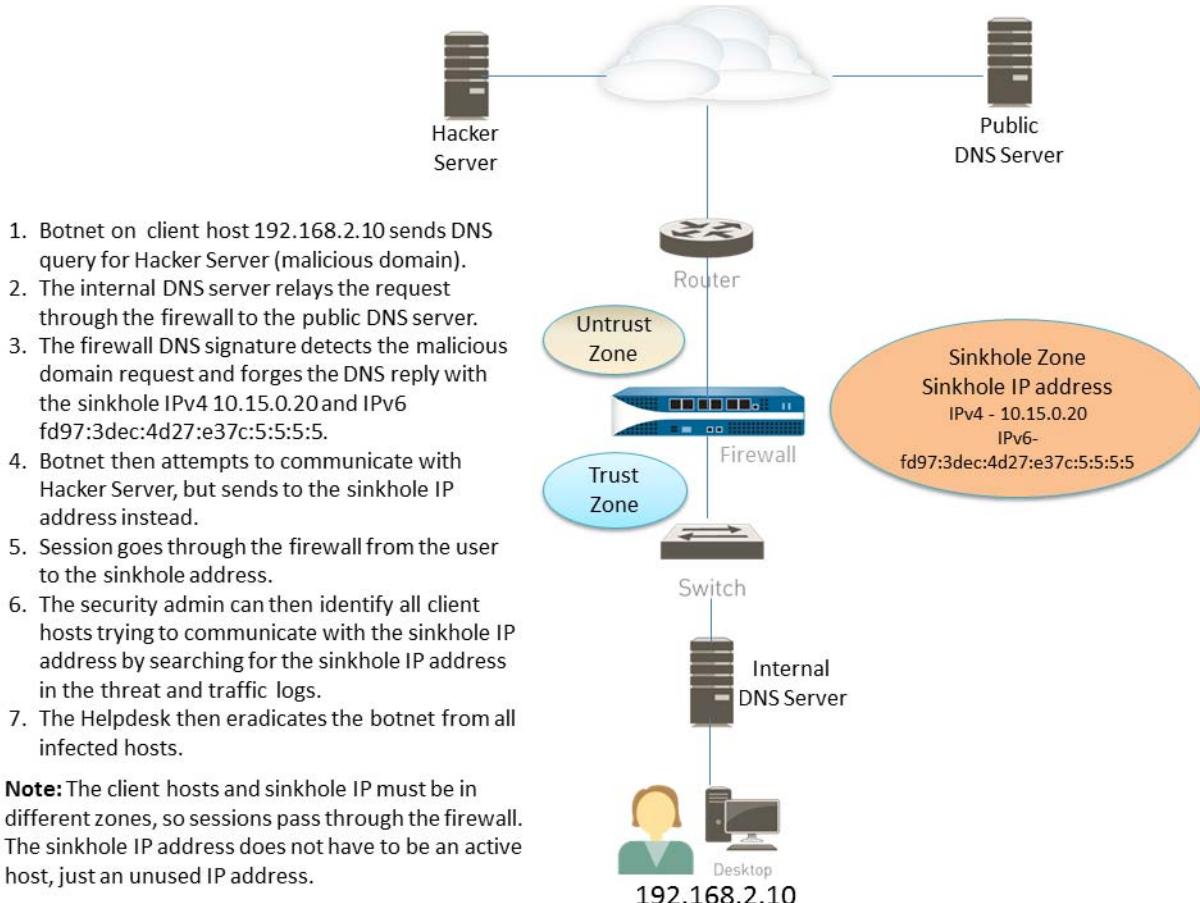
The DNS sinkhole action in Anti-Spyware profiles enables the firewall to forge a response to a DNS query for a known malicious domain, causing the malicious domain name to resolve to an IP address that you define. This allows you to identify hosts on your network that have been infected with malware. The following topics describe the DNS sinkhole action and provide instructions for enabling it and monitoring logs to identify infected hosts.

- ▲ [DNS Sinkholing](#)
- ▲ [Configure DNS Sinkholing](#)
- ▲ [Identify Infected Hosts](#)

## DNS Sinkholing

DNS sinkholing helps you to identify infected hosts on the protected network using DNS traffic in situations where the firewall cannot see the infected client's DNS query (that is, the firewall cannot see the originator of the DNS query). In a typical deployment where the firewall is north of the local DNS server, the threat log will identify the local DNS resolver as the source of the traffic rather than the actual infected host. Sinkholing malware DNS queries solves this visibility problem by forging responses to the client host queries directed at malicious domains, so that clients attempting to connect to malicious domains (for command-and-control, for example) will instead attempt to connect to a sinkhole IP address you define as illustrated in [Configure DNS Sinkholing](#). Infected hosts can then be easily identified in the traffic logs because any host that attempts to connect to the sinkhole IP address are most likely infected with malware.

**Figure: DNS Sinkholing Example**



## Configure DNS Sinkholing

To enable DNS Sinkholing, you must enable the action in an Anti-Spyware profile and attach the profile to a security rule. When a client host attempts to access a malicious domain, the firewall forges the destination IP address in the packet using the IP address you configure as the DNS sinkhole address.

<b>Configure DNS Sinkholing</b>	
<p><b>Step 1</b> Obtain both an IPv4 and IPv6 address to use as the sinkhole IP addresses.</p> <p>The DNS sinkhole address must be in a different zone than the client hosts to ensure that when an infected host attempts to start a session with the sinkhole IP address, it will be routed through the firewall. The reason both IPv4 and IPv6 are needed is because malicious software may perform DNS queries using one or both of these protocols.</p> <p> This sinkhole addresses must be reserved for this purpose and do not need to be assigned to a physical host. You can optionally use a honey-pot server as a physical host to further analyze the malicious traffic.</p>	<p>The configuration steps that follow use the following example DNS sinkhole addresses:</p> <p>IPv4 DNS sinkhole address—10.15.0.20 IPv6 DNS sinkhole address—fd97:3dec:4d27:e37c:5:5:5:5</p>
<p><b>Step 2</b> Configure the sinkhole interface and zone.</p> <p>Traffic from the zone where the client hosts reside must route to the zone where the sinkhole IP address is defined, so traffic will be logged.</p> <p> Use a dedicated zone for sinkhole traffic, because the infected host will be sending traffic to this zone.</p>	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Interfaces</b> and select an interface to configure as your sinkhole interface.</li> <li>In the <b>Interface Type</b> drop-down, select <b>Layer3</b>.</li> <li>To add an IPv4 address, select the <b>IPv4</b> tab and select <b>Static</b> and then click <b>Add</b>. In this example, add 10.15.0.20 as the IPv4 DNS sinkhole address.</li> <li>Select the <b>IPv6</b> tab and click <b>Static</b> and then click <b>Add</b> and enter an IPv6 address and subnet mask. In this example, enter fd97:3dec:4d27:e37c::/64 as the IPv6 sinkhole address.</li> <li>Click <b>OK</b> to save.</li> <li>To add a zone for the sinkhole, select <b>Network &gt; Zones</b> and click <b>Add</b>.</li> <li>Enter zone <b>Name</b>.</li> <li>In the <b>Type</b> drop-down select <b>Layer3</b>.</li> <li>In the <b>Interfaces</b> section, click <b>Add</b> and add the interface you just configured.</li> <li>Click <b>OK</b>.</li> </ol>

### Configure DNS Sinkholing (Continued)

<p><b>Step 3</b> Enable DNS sinkholing on the Anti-Spyware profile.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Security Profiles &gt; Anti-Spyware</b>.</li> <li>2. Modify an existing profile, or select one of the existing defaults and clone it.</li> <li>3. <b>Name</b> the profile and then select the <b>DNS Signatures</b> tab.</li> <li>4. In the <b>Action on DNS queries</b> drop-down, select <b>sinkhole</b>.</li> <li>5. In the <b>Sinkhole IPv4</b> field enter the sinkhole IPv4 sinkhole address you configured in <a href="#">Step 2</a> (10.15.0.20 in this example).</li> <li>6. In the <b>Sinkhole IPv6</b> field enter the IPv6 sinkhole address you configured in <a href="#">Step 2</a> (fd97:3dec:4d27:e37c:5:5:5:5 in this example).</li> </ol> <p> The default sinkhole address is the loopback address (127.0.0.1 for IPv4 and ::1 for IPv6).</p> <ol style="list-style-type: none"> <li>7. (Optional) In the <b>Packet Capture</b> drop-down, select <b>single-packet</b> or <b>extended-capture</b>. The single-packet option will capture the first packet of the session or select extended to set between 1-50 packets. You can then use the packet captures for further analysis.</li> <li>8. Click <b>OK</b> to save the profile.</li> </ol>
<p><b>Step 4</b> Edit the security policy rule that allows traffic from client hosts in the trust zone to the untrust zone to include the sinkhole zone as a destination and attach the Anti-Spyware profile.</p> <p>To ensure that you are identifying traffic from infected hosts, make these changes to the security rule(s) that allow traffic from client hosts in the trust zone to the untrust zone. By adding the sinkhole zone as a destination on the rule, you enable infected clients to send bogus DNS queries to the DNS sinkhole.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b>.</li> <li>2. Select an existing rule that allows traffic from the client host zone to the untrust zone.</li> <li>3. On the <b>Destination</b> tab, <b>Add</b> the Sinkhole zone. This allows client host traffic to flow to the sinkhole zone.</li> <li>4. On the <b>Actions</b> tab, select the <b>Log at Session Start</b> check box to enable logging. This will ensure that traffic from client hosts in the Trust zone will be logged when accessing the Untrust or Sinkhole zones.</li> <li>5. In the <b>Profile Setting</b> section, select the <b>Anti-Spyware</b> profile in which you enabled DNS sinkholing.</li> <li>6. Click <b>OK</b> to save the security rule and then <b>Commit</b>.</li> </ol>

### Configure DNS Sinkholing (Continued)

<p><b>Step 5</b> To ensure that you will be able to identify infected hosts, verify that traffic going from the client host in the Trust zone to the new Sinkhole zone is being logged.</p> <p>In this example, the infected client host is 192.168.2.10 and the Sinkhole IPv4 address is 10.15.0.20.</p>	<ol style="list-style-type: none"> <li>1. From a client host in the trust zone, open a command prompt and run the following command:  <pre>C:\&gt;ping &lt;sinkhole address&gt;</pre> <p>The following example output shows the ping request to the DNS sinkhole address at 10.15.0.2 and the result, which is Request timed out because in this example the sinkhole IP address is not assigned to a physical host:</p> <pre>C:\&gt;ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of data: Request timed out. Request timed out.  Ping statistics for 10.15.0.20: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)</pre> </li> <li>2. On the firewall, select <b>Monitor &gt; Logs &gt; Traffic</b> and find the log entry with the Source 192.168.2.10 and Destination 10.15.0.20. This will confirm that the traffic to the sinkhole IP address is traversing the firewall zones.</li> </ol> <p> You can search and/or filter the logs and only show logs with the destination 10.15.0.20. To do this, click the IP address (10.15.0.20) in the <b>Destination</b> column, which will add the filter (addr.dst in 10.15.0.20) to the search field. Click the Apply Filter icon to the right of the search field to apply the filter.</p>
<p><b>Step 6</b> Identify a malicious domain that you can use to verify that the DNS sinkhole functionality is configured properly.</p> <p>You must test this feature using a malicious domain that is included in the firewall's current antivirus signature database. The DNS Signatures used to identify malicious domains is only part of the full antivirus signature database, which contains hundreds of thousands of signatures.</p>	<p>To find a malicious domain for testing:</p> <ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Dynamic Updates</b> and in the <b>Antivirus</b> section click the <b>Release Notes</b> link for the current antivirus DB that is installed. You can also find the antivirus release notes on the support site in Dynamic Updates. In most cases, the signature update is an incremental update, so only new viruses and DNS signatures are listed. There are many antivirus signatures and DNS signatures that will already be installed on the firewall.</li> <li>2. In the second column of the release note, locate a line item with a domain extension (for example, .com, .edu, or .net). The left column displays the domain name. For example, in Antivirus release 1117-1560, there is an item in the left column named <b>tbsbana</b> and the right column lists <b>net</b>.</li> </ol> <p>The following shows the content in the release note for this line item:</p> <pre>conficker:tbsbanal variants: net</pre> <p>Because this domain shows up in the current database, it will work for testing.</p>

**Configure DNS Sinkholing (Continued)**

<p><b>Step 7</b> Test the sinkhole action</p> <p>This is similar to the action that would be performed if the client host was infected and the malicious application was attempting to reach a hacker server using DNS queries.</p>	<ol style="list-style-type: none"><li>1. From the client host, open a command prompt.</li><li>2. Perform an NSLOOKUP to a URL that you identified as a known malicious domain in <a href="#">Step 6</a>.</li></ol> <p>For example, using the URL track.bidtrk.com:</p> <pre>C:\&gt;nslookup track.bidtrk.com Server: my-local-dns.local Address: 10.0.0.222 Non-authoritative answer: Name: track.bidtrk.com.org Addresses: fd97:3dec:4d27:e37c:5:5:5:5 10.15.0.20</pre> <p>In the output, note that the NSLOOKUP to the malicious domain has been forged using the sinkhole IP addresses that we configured (10.15.0.20). Because the domain matched a malicious DNS signature, the sinkhole action was performed.</p> <ol style="list-style-type: none"><li>3. Select <b>Monitor &gt; Logs &gt; Threat</b> and locate the corresponding threat log entry to verify that the correct action was taken on the NSLOOKUP request.</li><li>4. Perform a ping to track.bidtrk.com, which will generate network traffic to the sinkhole address.</li></ol>
---	---

## Identify Infected Hosts

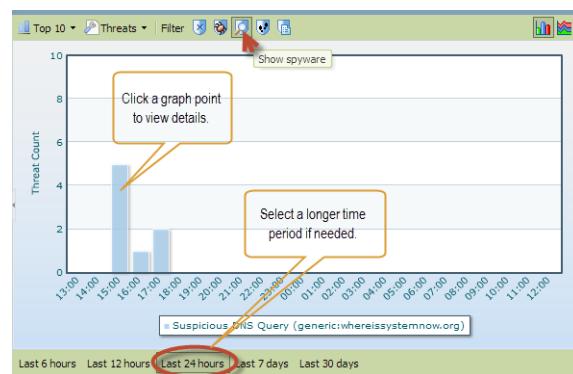
After you have configured DNS sinkholing and verified that traffic to a malicious domain goes to the sinkhole address, you should regularly monitor traffic to the sinkhole address, so that you can track down the infected hosts and eliminate the threat.

### DNS Sinkhole Verification and Reporting

**Step 1** Use App Scope to identify infected client hosts.

1. Select **Monitor > App Scope** and select **Threat Monitor**.
2. Click the **Show spyware** button along the top of the display page.
3. Select a time range.

The following screenshot shows three instances of Suspicious DNS queries, which were generated when the test client host performed an NSLOOKUP on a known malicious domain. Click the graph to see more details about the event.



### DNS Sinkhole Verification and Reporting (Continued)

- Step 2** Configure a custom report to identify all client hosts that have sent traffic to the sinkhole IP address, which is 10.15.0.20 in this example.

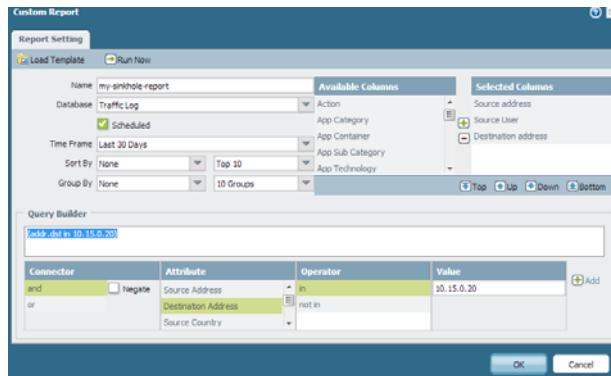


Forward to an SNMP manager, Syslog server and/or Panorama to enable alerts on these events.

In this example, the infected client host performed an NSLOOKUP to a known malicious domain that is listed in the Palo Alto Networks DNS Signature database. When this occurred, the query was sent to the local DNS server, which then forwarded the request through the firewall to an external DNS server. The firewall security policy with the Anti-Spyware profile configured matched the query to the DNS Signature database, which then forged the reply using the sinkhole address of 10.15.0.20 and fd97:3dec:4d27:e37c:5:5:5. The client attempts to start a session and the traffic log records the activity with the source host and the destination address, which is now directed to the forged sinkhole address.

Viewing the traffic log on the firewall allows you to identify any client host that is sending traffic to the sinkhole address. In this example, the logs show that the source address 192.168.2.10 sent the malicious DNS query. The host can then be found and cleaned. Without the DNS sinkhole option, the administrator would only see the local DNS server as the system that performed the query and would not see the client host that is infected. If you attempted to run a report on the threat log using the action “Sinkhole”, the log would show the local DNS server, not the infected host.

1. Select **Monitor > Manage Custom Reports**.
2. Click **Add** and **Name** the report.
3. Define a custom report that captures traffic to the sinkhole address as follows:
  - **Database**—Select **Traffic Log**.
  - **Scheduled**—Enable **Scheduled** and the report will run every night.
  - **Time Frame**—30 days
  - **Selected Columns**—Select **Source address** or **Source User** (if you have User-ID configured), which will identify the infected client host in the report, and **Destination address**, which will be the sinkhole address.
  - In the section at the bottom of the screen, create a custom query for traffic to the sinkhole address (10.15.0.20 in this example). You can either enter the destination address in the **Query Builder** window (**addr.dst in 10.15.0.20**) or select the following in each column and click **Add**: Connector = and, Attribute = Destination Address, Operator = in, and Value = 10.15.0.20. Click **Add** to add the query.



4. Click **Run Now** to run the report. The report will show all client hosts that have sent traffic to the sinkhole address, which indicates that they are most likely infected. You can now track down the hosts and check them for spyware.

Custom Report				
Report Setting		my-sinkhole-report	Infected client host	Sinkhole IP address
Source	Source Host Name	Source User	Destination	Destination Host Name
1   192.168.2.10	192.168.2.10		10.15.0.20	10.15.0.20

5. To view scheduled reports that have run, select **Monitor > Reports**.

# Content Delivery Network Infrastructure for Dynamic Updates

Palo Alto Networks maintains a Content Delivery Network (CDN) infrastructure for delivering content updates to the Palo Alto Networks devices. The devices access the web resources in the CDN to perform various App-ID and Content-ID functions. For enabling and scheduling the content updates, see [Manage Content Updates](#).

The following table lists the web resources that the firewall accesses for a feature or application:

Resource	URL	Static Addresses (If a static server is required)
Application Database	<ul style="list-style-type: none"> <li>updates.paloaltonetworks.com:443</li> </ul>	staticupdates.paloaltonetworks.com or the IP address 199.167.52.15
Threat/Antivirus Database	<ul style="list-style-type: none"> <li>updates.paloaltonetworks.com:443</li> <li>downloads.paloaltonetworks.com:443</li> </ul> <p>As a best practice, set the update server to updates.paloaltonetworks.com. This allows the Palo Alto Networks device to receive content updates from the server closest to it in the CDN infrastructure.</p>	staticupdates.paloaltonetworks.com or the IP address 199.167.52.15
PAN-DB URL Filtering	*.urlcloud.paloaltonetworks.com Resolves to the primary URL s0000.urlcloud.paloaltonetworks.com and is then redirected to the regional server that is closest: <ul style="list-style-type: none"> <li>s0100.urlcloud.paloaltonetworks.com</li> <li>s0200.urlcloud.paloaltonetworks.com</li> <li>s0300.urlcloud.paloaltonetworks.com</li> <li>s0500.urlcloud.paloaltonetworks.com</li> </ul>	Static IP addresses are not available. However, you can manually resolve a URL to an IP address and allow access to the regional server IP address.
BrightCloud URL Filtering	<ul style="list-style-type: none"> <li>database.brightcloud.com:443/80</li> <li>service.brightcloud.com:80</li> </ul>	Contact BrightCloud Customer Support.

Resource	URL	Static Addresses (If a static server is required)
WildFire	<ul style="list-style-type: none"> <li>• beta.wildfire.paloaltonetworks.com:443/80</li> <li>• beta-s1.wildfire.paloaltonetworks.com:443/80           <div style="display: flex; align-items: center; gap: 10px;">  <p>Beta sites are only accessed by a firewall running a Beta release version.</p> </div> </li> <li>• mail.wildfire.paloaltonetworks.com:25</li> <li>• wildfire.paloaltonetworks.com:443/80</li> </ul>	<ul style="list-style-type: none"> <li>• mail.wildfire.paloaltonetworks.com:25 or the IP address 54.241.16.83</li> <li>• wildfire.paloaltonetworks.com:443/80 or 54.241.8.199</li> </ul> <p>The regional URL/IP addresses are as follows:</p> <ul style="list-style-type: none"> <li>• ca-s1.wildfire.paloaltonetworks.com:44 or 54.241.34.71</li> <li>• va-s1.wildfire.paloaltonetworks.com:443 or 174.129.24.252</li> <li>• eu-s1.wildfire.paloaltonetworks.com:443 or 54.246.95.247</li> <li>• sg-s1.wildfire.paloaltonetworks.com:443 or 54.251.33.241</li> <li>• jp-s1.wildfire.paloaltonetworks.com:443 or 54.238.53.161</li> <li>• portal3.wildfire.paloaltonetworks.com:443/80 or 54.241.8.199</li> <li>• ca-s3.wildfire.paloaltonetworks.com:443 or 54.241.34.71</li> <li>• va-s3.wildfire.paloaltonetworks.com:443 or 23.21.208.35</li> <li>• eu-s3.wildfire.paloaltonetworks.com:443 or 54.246.95.247</li> <li>• sg-s3.wildfire.paloaltonetworks.com:443 or 54.251.33.241</li> <li>• jp-s3.wildfire.paloaltonetworks.com:443 or 54.238.53.161</li> <li>• wildfire.paloaltonetworks.com.jp:443/80 or 180.37.183.53</li> <li>• wf1.wildfire.paloaltonetwrks.jp:443 or 180.37.180.37</li> <li>• wf2.wildfire.paloaltonetworks.jp:443 or 180.37.181.18</li> <li>• portal3.wildfire.paloaltonetworks.jp:443/80 or 180.37.183.53</li> </ul>

## Threat Prevention Resources

For more information on Threat Prevention, refer to the following sources:

- [Creating Custom Threat Signatures](#)
- [Threat Prevention Deployment](#)
- [Understanding DoS Protection](#)

To view a list of Threats and Applications that Palo Alto Networks products can identify, use the following links:

- [Applipedia](#)—Provides details on the applications that Palo Alto Networks can identify.
- [Threat Vault](#)—Lists threats that Palo Alto Networks products can identify. You can search by Vulnerability, Spyware, or Virus. Click the Details icon next to the ID number for more information about a threat.





# Decryption

---

Palo Alto Networks firewalls provide the capability to decrypt and inspect traffic for visibility, control, and granular security. Decryption on a Palo Alto Networks firewall includes the capability to enforce security policies on encrypted traffic, where otherwise the encrypted traffic might not be blocked and shaped according to your configured security settings. Use decryption on a firewall to prevent malicious content from entering your network or sensitive content from leaving your network concealed as encrypted traffic. Enabling decryption on a Palo Alto Networks firewall can include preparing the keys and certificates required for decryption, creating a decryption policy, and configuring decryption port mirroring. See the following topics to learn about and configure decryption:

- ▲ [Decryption Overview](#)
- ▲ [Decryption Concepts](#)
- ▲ [Configure SSL Forward Proxy](#)
- ▲ [Configure SSL Inbound Inspection](#)
- ▲ [Configure SSH Proxy](#)
- ▲ [Configure Decryption Exceptions](#)
- ▲ [Enable Users to Opt Out of SSL Decryption](#)
- ▲ [Configure Decryption Port Mirroring](#)
- ▲ [Temporarily Disable SSL Decryption](#)

## Decryption Overview

Secure Sockets Layer (SSL) and Secure Shell (SSH) are encryption protocols used to secure traffic between two entities, such as a web server and a client. SSL and SSH encapsulate traffic, encrypting data so that it is meaningless to entities other than the client and server with the keys to decode the data and the certificates to affirm trust between the devices. Traffic that has been encrypted using the protocols SSL and SSH can be decrypted to ensure that these protocols are being used for the intended purposes only, and not to conceal unwanted activity or malicious content.

Palo Alto Networks firewalls decrypt encrypted traffic by using keys to transform strings (passwords and shared secrets) from ciphertext to plaintext (decryption) and from plaintext back to ciphertext (re-encrypting traffic as it exits the device). Certificates are used to establish the firewall as a trusted third party and to create a secure connection. SSL decryption (both forward proxy and inbound inspection) requires certificates to establish trust between two entities in order to secure an SSL/TLS connection. Certificates can also be used when excluding servers from SSL decryption. You can integrate a hardware security module (HSM) with a firewall to enable enhanced security for the private keys used in SSL forward proxy and SSL inbound inspection decryption. To learn more about storing and generating keys using an HSM and integrating an HSM with your firewall, see [Secure Keys with a Hardware Security Module](#). SSH decryption does not require certificates.

Palo Alto Networks firewall decryption is policy-based, and can be used to decrypt, inspect, and control both inbound and outbound SSL and SSH connections. Decryption policies allow you to specify traffic for decryption according to destination, source, or URL category and in order to block or restrict the specified traffic according to your security settings. The firewall uses certificates and keys to decrypt the traffic specified by the policy to plaintext, and then enforces App-ID and security settings on the plaintext traffic, including Decryption, Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking profiles. After traffic is decrypted and inspected on the firewall, the plaintext traffic is re-encrypted as it exits the firewall to ensure privacy and security. Use policy-based decryption on the firewall to achieve outcomes such as the following:

- Prevent malware concealed as encrypted traffic from being introduced into an corporate network.
- Prevent sensitive corporate information from moving outside the corporate network.
- Ensure the appropriate applications are running on a secure network.
- Selectively decrypt traffic; for example, exclude traffic for financial or healthcare sites from decryption by configuring a decryption exception.

The three decryption policies offered on the firewall, [SSL Forward Proxy](#), [SSL Inbound Inspection](#), and [SSH Proxy](#), all provide methods to specifically target and inspect SSL outbound traffic, SSL inbound traffic, and SSH traffic, respectively. The decryption policies provide the settings for you to specify what traffic to decrypt and decryption profiles can be selected when creating a policy, in order to apply more granular security settings to decrypted traffic, such as checks for server certificates, unsupported modes, and failures. This policy-based decryption on the firewall gives you visibility into and control of SSL and SSH encrypted traffic according to configurable parameters.

You can also choose to extend a decryption configuration on the firewall to include [Decryption Mirroring](#), which allows for decrypted traffic to be forwarded as plaintext to a third party solution for additional analysis and archiving.

## Decryption Concepts

To learn about keys and certificates for decryption, decryption policies, and decryption port mirroring, see the following topics:

- ▲ [Keys and Certificates for Decryption Policies](#)
- ▲ [SSL Forward Proxy](#)
- ▲ [SSL Inbound Inspection](#)
- ▲ [SSH Proxy](#)
- ▲ [Decryption Exceptions](#)
- ▲ [Decryption Mirroring](#)

## Keys and Certificates for Decryption Policies

Keys are strings of numbers that are typically generated using a mathematical operation involving random numbers and large primes. Keys are used to transform other strings—such as passwords and shared secrets—from plaintext to ciphertext (called *encryption*) and from ciphertext to plaintext (called *decryption*). Keys can be symmetric (the same key is used to encrypt and decrypt) or asymmetric (one key is used for encryption and a mathematically related key is used for decryption). Any system can generate a key.

X.509 certificates are used to establish trust between a client and a server in order to establish an SSL connection. A client attempting to authenticate a server (or a server authenticating a client) knows the structure of the X.509 certificate and therefore knows how to extract identifying information about the server from fields within the certificate, such as its FQDN or IP address (called a *common name* or *CN* within the certificate) or the name of the organization, department, or user to which the certificate was issued. All certificates must be issued by a certificate authority (CA). After the CA verifies a client or server, the CA issues the certificate and signs it using its private key.

With a decryption policy configured, an SSL/TLS session between the client and the server is established only if the firewall trusts the CA that signed the server certificate. In order to establish trust, the firewall must have the server root CA certificate in its certificate trust list (CTL) and use the public key contained in that root CA certificate to verify the signature. The firewall then presents a copy of the server certificate signed by the Forward Trust certificate for the client to authenticate. You can also configure the firewall to use an enterprise CA as a forward trust certificate for SSL Forward Proxy. If the firewall does not have the server root CA certificate in its CTL, the firewall will present a copy of the server certificate signed by the Forward Untrust certificate to the client. The Forward Untrust certificate ensures that clients are prompted with a certificate warning when attempting to access sites hosted by a server with untrusted certificates.

For detailed information on certificates, see [Certificate Management](#).



To control the trusted CAs that your device trusts, use the **Device > Certificate Management > Certificates > Default Trusted Certificate Authorities** tab on the firewall web interface.

**Table: Palo Alto Networks Device Keys and Certificates** describes the different keys and certificates used by Palo Alto Networks devices for decryption. As a best practice, use different keys and certificates for each usage.

**Table: Palo Alto Networks Device Keys and Certificates**

Key/Certificate Usage	Description
Forward Trust	The certificate the firewall presents to clients during decryption if the site the client is attempting to connect to has a certificate that is signed by a CA that the firewall trusts. To configure a Forward Trust certificate on the firewall, see <a href="#">Step 2</a> in the <a href="#">Configure SSL Forward Proxy</a> task. By default, the firewall determines the key size to use for the client certificate based on the key size of the destination server. However, you can also set a specific key size for the firewall to use. See <a href="#">Configure the Key Size for SSL Forward Proxy Server Certificates</a> . For added security, store the forward trust certificate on a Hardware Security Module (HSM), see <a href="#">Store Private Keys on an HSM</a> .
Forward Untrust	The certificate the firewall presents to clients during decryption if the site the client is attempting to connect to has a certificate that is signed by a CA that the firewall does not trust. To configure a Forward Untrust certificate on the firewall, see <a href="#">Step 3</a> in the <a href="#">Configure SSL Forward Proxy</a> task.

Key/Certificate Usage	Description
SSL Exclude Certificate	Certificates for servers that you want to exclude from SSL decryption. For example, if you have SSL decryption enabled, but have certain servers that you do not want included in SSL decryption, such as the web services for your HR systems, you would import the corresponding certificates onto the firewall and configure them as SSL Exclude Certificates. See <a href="#">Exclude a Server from Decryption</a> .
SSL Inbound Inspection	The certificate used to decrypt inbound SSL traffic for inspection and policy enforcement. For this application, you would import the server certificate for the servers for which you are performing SSL inbound inspection, or store them on an HSM (see <a href="#">Store Private Keys on an HSM</a> ).

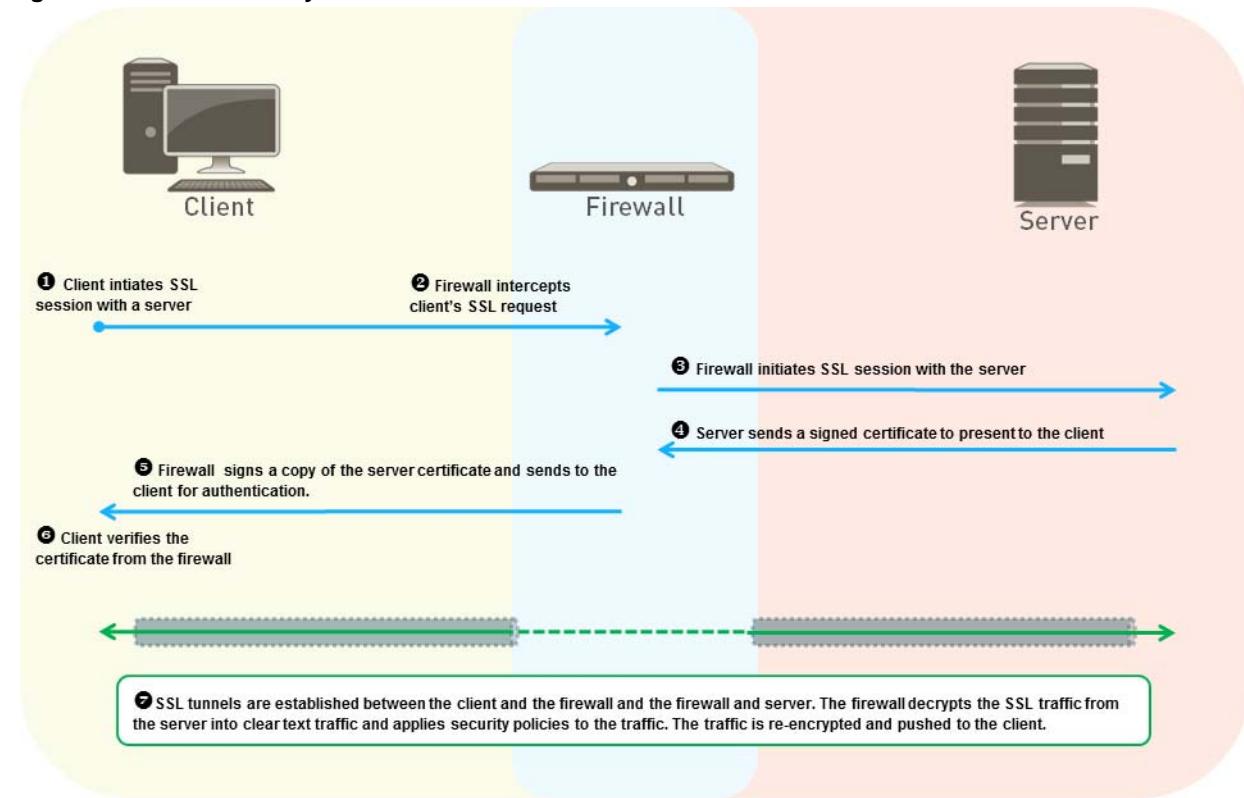
## SSL Forward Proxy

Use an SSL Forward Proxy decryption policy to decrypt and inspect SSL/TLS traffic from internal users to the web. SSL Forward Proxy decryption prevents malware concealed as SSL encrypted traffic from being introduced to your corporate network; for example, if an employee is using her Gmail account from her corporate office and opens an email attachment that contains a virus, SSL Forward Proxy decryption will prevent the virus from infecting the client system and entering the corporate network.

With SSL Forward Proxy decryption, the firewall resides between the internal client and outside server. The firewall uses Forward Trust or Forward Untrust certificates to establish itself as a trusted third party to the session between the client and the server (For details on certificates, see [Keys and Certificates for Decryption Policies](#)). When the client initiates an SSL session with the server, the firewall intercepts the client SSL request and forwards the SSL request to the server. The server sends a certificate intended for the client that is intercepted by the firewall. If the server certificate is signed by a CA that the firewall trusts, the firewall creates a copy of the server certificate signed by the Forward Trust certificate and sends the certificate to the client to authenticate. If the server certificate is signed by a CA that the firewall does not trust, the firewall creates a copy of the server certificate and signs it with the Forward Untrust certificate and sends it to the client. In this case, the client sees a block page warning that the site they're attempting to connect to is not trusted and the client can choose to proceed or terminate the session. When the client authenticates the certificate, the SSL session is established with the firewall functioning as a trusted forward proxy to the site that the client is accessing.

As the firewall continues to receive SSL traffic from the server that is destined for the client, it decrypts the SSL traffic into clear text traffic and applies security policies to the traffic. The traffic is then re-encrypted on the firewall and the firewall forwards the encrypted traffic to the client.

Figure: SSL Forward Proxy shows this process in detail.

**Figure: SSL Forward Proxy**

See [Configure SSL Forward Proxy](#) for details on configuring SSL Forward Proxy.

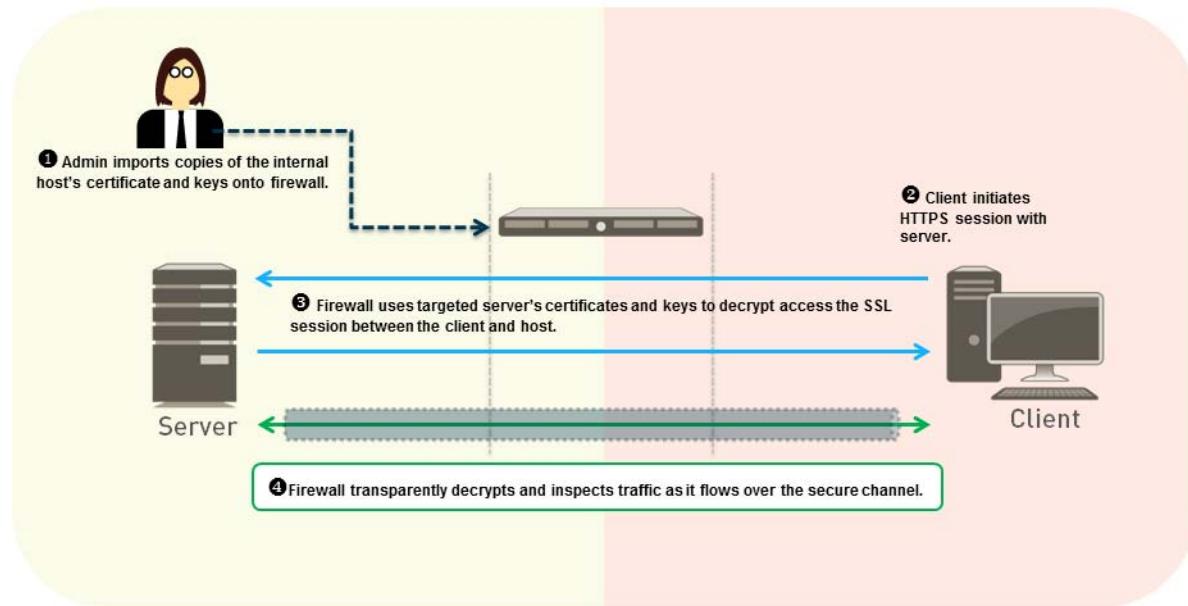
## SSL Inbound Inspection

Use SSL Inbound Inspection to decrypt and inspect inbound SSL traffic from a client to a targeted server (any server you have the certificate for and can import it onto the firewall). For example, if an employee is remotely connected to a web server hosted on the company network and is attempting to add restricted internal documents to his Dropbox folder (which uses SSL for data transmission), SSL Inbound Inspection can be used to ensure that the sensitive data does not move outside the secure company network by blocking or restricting the session.

Configuring SSL Inbound Inspection includes importing the targeted server certificate and key on to the firewall. Because the targeted server certificate and key are imported on the firewall, the firewall is able to access the SSL session between the server and the client and decrypt and inspect traffic transparently, rather than functioning as a proxy. The firewall is able to apply security policies to the decrypted traffic, detecting malicious content and controlling applications running over this secure channel.

Figure: SSL Inbound Inspection shows this process in detail.

**Figure: SSL Inbound Inspection**



See [Configure SSL Inbound Inspection](#) for details on configuring SSL Inbound Inspection.

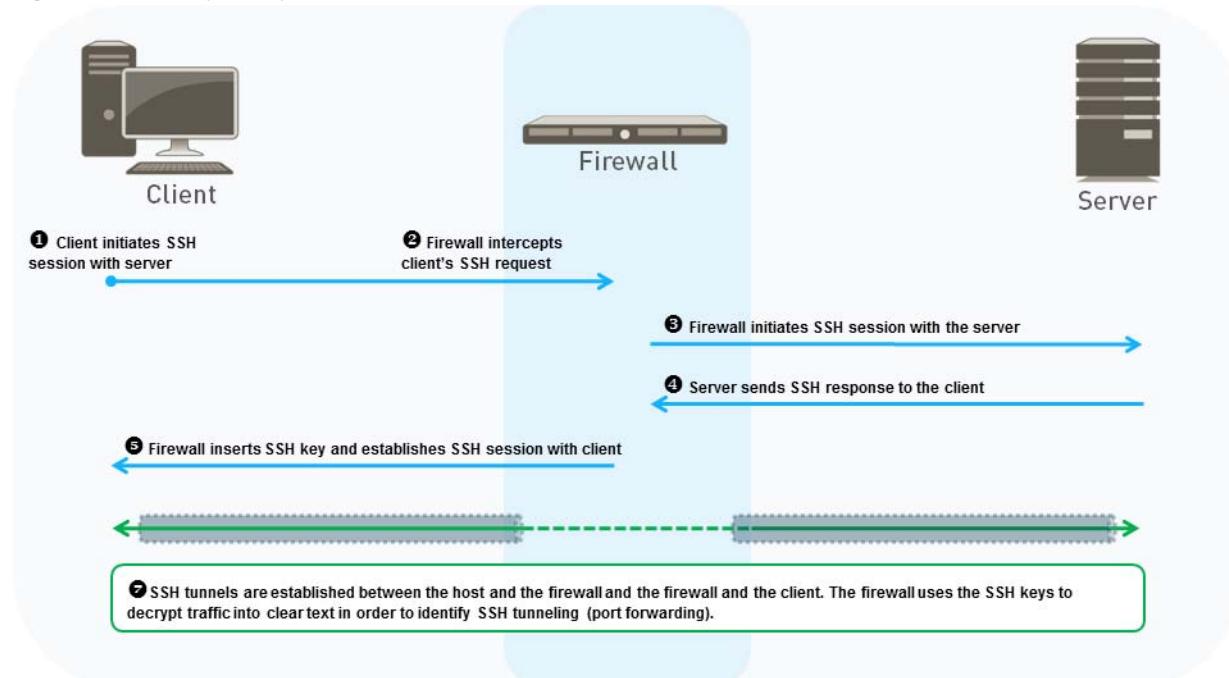
## SSH Proxy

SSH Proxy provides the capability for the firewall to decrypt inbound and outbound SSH connections passing through the firewall, in order to ensure that SSH is not being used to tunnel unwanted applications and content. SSH decryption does not require any certificates and the key used for SSH decryption is automatically generated when the firewall boots up. During the boot up process, the firewall checks to see if there is an existing key. If not, a key is generated. This key is used for decrypting SSH sessions for all virtual systems configured on the device. The same key is also used for decrypting all SSH v2 sessions.

In an SSH Proxy configuration, the firewall resides between a client and a server. When the client sends an SSH request to the server, the firewall intercepts the request and forwards the SSH request to the server. The firewall then intercepts the server response and forwards the response to the client, establishing an SSH tunnel between the firewall and the client and an SSH tunnel between the firewall and the server, with firewall functioning as a proxy. As traffic flows between the client and the server, the firewall is able to distinguish whether the SSH traffic is being routed normally or if it is using SSH tunneling (port forwarding). Content and threat inspections are not performed on SSH tunnels; however, if SSH tunnels are identified by the firewall, the SSH tunneled traffic is blocked and restricted according to configured security policies.

[Figure: SSH Proxy Decryption](#) shows this process in detail.

**Figure: SSH Proxy Decryption**



See [Configure SSH Proxy](#) for details on configuring an SSH Proxy policy.

## Decryption Exceptions

Traffic can also be excluded from decryption according to matching criteria (using a decryption policy), a targeted server traffic can be excluded from decryption (using certificates), and some applications are excluded from decryption by default.

Applications that do not function properly when decrypted by the firewall and are automatically excluded from SSL decryption. The applications that are excluded from SSL decryption by default are excluded because these applications often fail when decrypted due to the application looking for specific details in the certificate that might not be present in the certificate generated for SSL Forward Proxy. Refer to the KB article [List of Applications Excluded from SSL Decryption](#) for a current list of applications excluded by default from SSL decryption on the firewall.

You can configure decryption exceptions for certain URL categories or applications that either do not work properly with decryption enabled or for any other reason, including for legal or privacy purposes. You can use a decryption policy to exclude traffic from decryption based on source, destination, URL category, service (port or protocol), and TCP port numbers. For example, with SSL decryption enabled, you can exclude traffic that is categorized as financial or health-related from decryption using the URL category selection.

You can also exclude servers from SSL decryption based on the Common Name (CN) in the server certificate. For example, if you have SSL decryption enabled but have certain servers that you do not want included in SSL decryption, such as the web services for your HR systems, you can exclude those servers from decryption by importing the server certificate onto the firewall and modifying the certificate to be an **SSL Exclude Certificate**.

To exclude traffic from decryption based on application, source, destination, URL category or to exclude a specific server from decryption, see [Configure Decryption Exceptions](#).

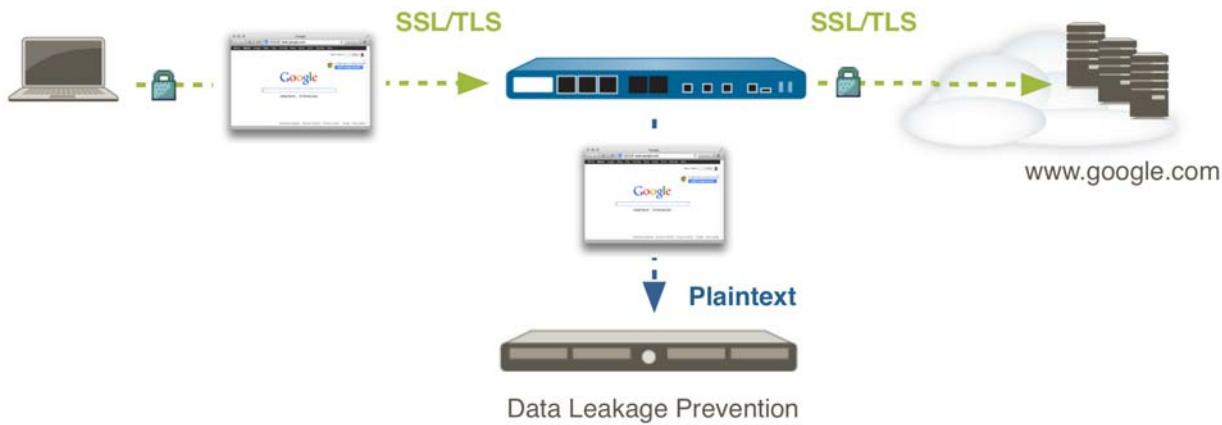
## Decryption Mirroring

The decryption mirroring feature provides the capability to create a copy of decrypted traffic from a firewall and send it to a traffic collection tool that is capable of receiving raw packet captures—such as NetWitness or Solera—for archiving and analysis. This feature is necessary for organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality. Decryption mirroring is available on PA-7000 Series, PA-5000 Series and PA-3000 Series platforms only and requires that a free license be installed to enable this feature.

Keep in mind that the decryption, storage, inspection, and/or use of SSL traffic is governed in certain countries and user consent might be required in order to use the decryption mirror feature. Additionally, use of this feature could enable malicious users with administrative access to the firewall to harvest usernames, passwords, social security numbers, credit card numbers, or other sensitive information submitted using an encrypted channel. Palo Alto Networks recommends that you consult with your corporate counsel before activating and using this feature in a production environment.

Figure: [Decryption Port Mirroring](#) shows the process for mirroring decrypted traffic and the section [Configure Decryption Port Mirroring](#) describes how to license and enable this feature.

**Figure: Decryption Port Mirroring**



# Configure SSL Forward Proxy

Configuring [SSL Forward Proxy](#) decryption on the firewall requires setting up the certificates needed for SSL Forward Proxy decryption and creating an SSL Forward Proxy decryption policy. The firewall can use self-signed certificates or certificates signed by an enterprise CA to perform SSL Forward Proxy decryption.



By default, the firewall determines the key size to use for the client certificates it generates based on the key size of the destination server certificate. You can optionally set a static key size to use regardless of the key size of the destination server certificate. See [Configure the Key Size for SSL Forward Proxy Server Certificates](#).

Use the following task to configure SSL Forward Proxy, including how to set up the certificates and create a decryption policy.

## Configure SSL Forward Proxy

<b>Step 1</b>	Ensure that the appropriate interfaces are configured as either virtual wire, Layer 2, or Layer 3 interfaces.	View configured interfaces on the <b>Network &gt; Interfaces &gt; Ethernet</b> tab. The <b>Interface Type</b> column displays if an interface is configured to be a <b>Virtual Wire</b> or <b>Layer 2</b> , or <b>Layer 3</b> interface. You can select an interface to modify its configuration, including what type of interface it is.
---------------	---	---

## Configure SSL Forward Proxy

**Step 2** Configure the forward trust certificate. Use either a self-signed certificate or a certificate signed by an enterprise CA.

### Using self-signed certificates

When the certificate of the server that the client is connecting to is signed by a CA that is on the firewall trusted CA list, the firewall signs a copy of the server certificate with a self-signed forward trust certificate to present to the client for authentication. In this case, the self-signed certificate must be imported onto each client system so that the client recognizes the firewall as a trusted CA.

Use self-signed certificates for SSL Forward Proxy decryption if you do not use an enterprise CA or if you are only intended to perform decryption for a limited number of client systems (or if you are planning to use a centralized deployment).

#### To use a self-signed certificate:

1. Select **Device > Certificate Management > Certificates**.
2. Click **Generate** at the bottom of the window.
3. Enter a **Certificate Name**, such as *my-fwd-trust*.
4. Enter a **Common Name**, such as **192.168.2.1**. This should be the IP or FQDN that will appear in the certificate. In this case, we are using the IP of the trust interface. Avoid using spaces in this field.
5. Leave the **Signed By** field blank.
6. Click the **Certificate Authority** check box to enable the firewall to issue the certificate. Selecting this check box creates a certificate authority (CA) on the firewall that is imported to the client browsers, so clients trust the firewall as a CA.
7. Click **Generate** to generate the certificate.
8. Click the new certificate *my-fwd-trust* to modify it and enable the **Forward Trust Certificate** option.
9. Export the forward trust certificate for import into client systems by highlighting the certificate and clicking **Export** at the bottom of the window. Choose PEM format, and do not select the **Export private key** option. Because the certificate is self-signed, import it into the browser trusted root CA list on the client systems in order for the clients to trust it. When importing to the client browser, ensure the certificate is added to the Trusted Root Certification Authorities certificate store. On Windows systems, the default import location is the Personal certificate store. You can also simplify this process by using a centralized deployment, such as an Active Directory Group Policy Object (GPO).



If the forward trust certificate is not imported on the client systems, users will see certificate warnings for each SSL site they visit.

10. Click **OK** to save.

## Configure SSL Forward Proxy

### Using an Enterprise CA

An enterprise CA can issue a signing certificate which the firewall can use to then sign the certificates for sites requiring SSL decryption. Send a Certificate Signing Request (CSR) for the enterprise CA to sign and validate. The firewall can then use the signed enterprise CA certificate for SSL Forward Proxy decryption. Because the enterprise CA is already trusted by the client systems, with this option, you do not need to distribute the certificate to client systems prior to configuring decryption.

To use an enterprise CA signed certificate, generate a CSR:

1. Select **Device > Certificate Management > Certificates** and click **Generate**.
2. Enter a **Certificate Name**, such as *my-fwd-proxy*.
3. In the **Signed By** drop-down, select **External Authority (CSR)**.
4. **(Optional)** If your enterprise CA requires it, add **Certificate Attributes** to further identify the firewall details, such as Country or Department.
5. Click **OK** to save the CSR. The pending certificate is now displayed on the **Device Certificates** tab.
6. Export the CSR:
  - a. Select the pending certificate displayed on the **Device Certificates** tab.
  - b. Click **Export** to download and save the certificate file.  
 Leave **Export private key** unselected in order to ensure that the private key remains securely on the firewall.
  - c. Click **OK**.
7. Import the signed enterprise CA onto the firewall:
  - a. Select **Device > Certificate Management > Certificates** and click **Import**.
  - b. Enter the pending **Certificate Name** exactly (in this case, *my-fwd-trust*). The **Certificate Name** that you enter must exactly match the pending certificate name in order for the pending certificate to be validated.
  - c. Select the signed **Certificate File** that you received from your enterprise CA.
  - d. Click **OK**. The certificate is displayed as valid with the Key and CA check boxes selected.
  - e. Select the validated certificate, in this case, *my-fwd-proxy*, to enable it as a **Forward Trust Certificate** to be used for SSL Forward Proxy decryption.
  - f. Click **OK**.

Configure SSL Forward Proxy	
<b>Step 3</b> Configure the forward untrust certificate.	<ol style="list-style-type: none"> <li>Click <b>Generate</b> at the bottom of the certificates page.</li> <li>Enter a <b>Certificate Name</b>, such as <i>my-fwd-untrust</i>.</li> <li>Set the <b>Common Name</b>, for example <b>192.168.2.1</b>. Leave <b>Signed By</b> blank.</li> <li>Click the <b>Certificate Authority</b> check box to enable the firewall to issue the certificate.</li> <li>Click <b>Generate</b> to generate the certificate.</li> <li>Click <b>OK</b> to save.</li> <li>Click the new <i>my-ssl-fw-untrust</i> certificate to modify it and enable the <b>Forward Untrust Certificate</b> option.</li> </ol> <p> Do not export the forward untrust certificate for import into client systems. If the forward trust certificate is imported on client systems, the users will not see certificate warnings for SSL sites with untrusted certificates.</p>
<b>Step 4</b> <b>(Optional)</b> Set the key size of the SSL Forward Proxy certificates that the firewall presents to clients.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; Session</b> and, in the Decryption Settings section, click <b>Forward Proxy Server Certificate Settings</b>.</li> <li>Select a <b>Key Size: Defined by destination host</b> (default), <b>1024-bit RSA</b>, or <b>2048-bit RSA</b>.</li> </ol>
<b>Step 5</b> <b>(Optional)</b> Create a decryption profile.	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Decryption Profile</b> and click <b>Add</b>.</li> <li>Select <b>SSL Decryption &gt; SSL Forward Proxy</b> to block and control specific aspects of SSL tunneled traffic. For example, you can choose to terminate sessions if system resources are not available to process decryption by selecting <b>Block sessions if resources not available</b>.</li> <li>Click <b>OK</b> to save the profile.</li> </ol>

<b>Configure SSL Forward Proxy</b>	
<b>Step 6</b> Configure a decryption policy.	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Decryption</b> and click <b>Add</b>.</li> <li>2. On the <b>General</b> tab, give the policy a descriptive <b>Name</b>.</li> <li>3. On the <b>Source</b> and <b>Destination</b> tabs, select <b>Any</b> for the <b>Source Zone</b> and <b>Destination Zone</b> to decrypt all SSL traffic destined for an external server. If you want to specify traffic from or to certain sources or destinations for decryption, click <b>Add</b>.</li> <li>4. On the <b>URL Category</b> tab, select <b>Any</b> to decrypt all traffic. Alternatively, <b>Add</b> URL categories to apply the profile to only those websites that fall under the selected categories.</li> </ol> <p> The option to decrypt traffic based on URL category is also useful when excluding certain sites (such as financial or healthcare-related sites) from decryption. See <a href="#">Configure Decryption Exceptions</a>.</p> <ol style="list-style-type: none"> <li>5. On the <b>Options</b> tab, select <b>Decrypt</b> and select <b>SSL Forward Proxy</b> as the <b>Type</b> of decryption to perform.</li> <li>6. <b>(Optional)</b> Select a <b>Decryption Profile</b> to apply additional settings to decrypted traffic (see <a href="#">Step 5</a>).</li> <li>7. Click <b>OK</b> to save.</li> </ol>
<b>Step 7</b> Enable the firewall to forward decrypted SSL traffic for WildFire analysis.	<p><b>On a firewall with no virtual systems configured:</b></p> <ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Content-ID</b>.</li> <li>2. Edit the Content-ID settings and <b>Allow Forwarding of Decrypted Content</b>.</li> <li>3. Click <b>OK</b> to save the changes.</li> </ol> <p><b>On a firewall with multiple virtual systems configured:</b></p> <p>Select <b>Device &gt; Virtual Systems</b>, select the virtual system you want to modify, and <b>Allow Forwarding of Decrypted Content</b>.</p>
<b>Step 8</b> <b>Commit</b> the configuration.	With an SSL Forward Proxy decryption policy enabled, all traffic identified by the policy is decrypted. Decrypted traffic is blocked and restricted according to the profiles configured on the firewall (including the decryption profiles associated with the policy and Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking profiles). Traffic is re-encrypted as it exits the firewall.

## Configure SSL Inbound Inspection

Configuring [SSL Inbound Inspection](#) includes installing the targeted server certificate on the firewall and creating an SSL Inbound Inspection decryption policy.

Use the following task to configure SSL Inbound Inspection.

Configure SSL Inbound Inspection	
Step 1	Ensure that the appropriate interfaces are configured as either virtual wire, Layer 2, or Layer 3 interfaces.
Step 2	Ensure that the targeted server certificate is installed on the firewall.  On the web interface, select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> to view certificates installed on the firewall.  To import the targeted server certificate onto the firewall: <ol style="list-style-type: none"><li>1. On the <b>Device Certificates</b> tab, select <b>Import</b>.</li><li>2. Enter a descriptive <b>Certificate Name</b>.</li><li>3. Browse for and select the targeted server <b>Certificate File</b>.</li><li>4. Click <b>OK</b>.</li></ol>
Step 3	(Optional) Create a Decryption profile.  Decryption profiles can be associated with a decryption policy, enabling the firewall to block and control various aspects of traffic that is being decrypted. An SSL Inbound Inspection decryption profile can be used to perform checks for unsupported protocol versions, unsupported cipher suites, and failures.  1. Select <b>Objects &gt; Decryption Profile</b> and click <b>Add</b> . 2. Select <b>SSL Decryption &gt; Inbound Inspection</b> to block and control specific aspects of inbound SSL traffic. For example, you can choose to terminate sessions if system resources are not available to process decryption by selecting <b>Block sessions if resources not available</b> . 3. Click <b>OK</b> to save the profile.

<b>Configure SSL Inbound Inspection</b>	
<b>Step 4</b> Configure a decryption policy.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Decryption</b> and click <b>Add</b>.</li> <li>On the <b>General</b> tab, give the policy a descriptive <b>Name</b>.</li> <li>On the <b>Destination</b> tab, <b>Add</b> the <b>Destination Address</b> of the targeted server.</li> <li>On the <b>URL Category</b> tab, select <b>Any</b> to decrypt all traffic. Alternatively, <b>Add</b> URL categories to apply the profile to only those websites that fall under the selected categories.</li> </ol> <p> The option to decrypt traffic based on URL category is also useful when excluding certain sites (such as financial or healthcare-related sites) from decryption. See <a href="#">Configure Decryption Exceptions</a>.</p> <ol style="list-style-type: none"> <li>On the <b>Options</b> tab, select <b>Decrypt</b> and select <b>SSL Inbound Inspection</b> as the <b>Type</b> of traffic to decrypt. Select the <b>Certificate</b> for the internal server that is the destination of the inbound SSL traffic.</li> <li>(Optional) Select a <b>Decryption Profile</b> to apply additional settings to decrypted traffic.</li> <li>Click <b>OK</b> to save.</li> </ol>
<b>Step 5</b> Enable the firewall to forward decrypted SSL traffic for WildFire analysis.	<p> This is a <a href="#">best practice</a> for firewalls enabled to forward files for WildFire analysis. To forward portable executables (PEs) only, you do not need a WildFire license; however forwarding advanced file types requires an active WildFire license.</p> <p><b>On a firewall with no virtual systems configured:</b></p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; Content-ID</b>.</li> <li>Edit the Content-ID settings and <b>Allow Forwarding of Decrypted Content</b>.</li> <li>Click <b>OK</b> to save the changes.</li> </ol> <p><b>On a firewall with multiple virtual systems configured:</b></p> <p>Select <b>Device &gt; Virtual Systems</b>, select the virtual system you want to modify, and <b>Allow Forwarding of Decrypted Content</b>.</p>
<b>Step 6</b> <b>Commit</b> the configuration.	With an SSL Inbound Inspection decryption policy enabled, all SSL traffic identified by the policy is decrypted and inspected. Decrypted traffic is blocked and restricted according to the profiles configured on the firewall (including the decryption profiles associated with the policy and Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking profiles). Traffic is re-encrypted as it exits the firewall.

## Configure SSH Proxy

Configuring [SSH Proxy](#) does not require certificates and the key used to decrypt SSH sessions is generated automatically on the firewall during boot up.

Use the following task to configure SSH Proxy decryption.

<b>Configure SSH Proxy Decryption</b>		
<b>Step 1</b>	Ensure that the appropriate interfaces are configured as either virtual wire, Layer 2, or Layer 3 interfaces. Decryption can only be performed on virtual wire, Layer 2, or Layer 3 interfaces.	
<b>Step 2</b>	(Optional) Create a Decryption profile.  Decryption profiles can be associated with a decryption policy, enabling the firewall to block and control various aspects of traffic that is being decrypted. An SSH proxy decryption profile can be used to perform checks for unsupported protocol versions, unsupported cipher suites, and for failures.	<p>View configured interfaces on the <b>Network &gt; Interfaces &gt; Ethernet</b> tab. The <b>Interface Type</b> column displays if an interface is configured to be a <b>Virtual Wire</b> or <b>Layer 2</b>, or <b>Layer 3</b> interface. You can select an interface to modify its configuration, including what type of interface it is.</p> <ol style="list-style-type: none"> <li>Select <b>Objects &gt; Decryption Profile</b> and click <b>Add</b>.</li> <li>Select the <b>SSH</b> tab to block and control specific aspects of SSH tunneled traffic. For example, you can choose to terminate sessions if system resources are not available to process decryption by selecting <b>Block sessions if resources not available</b>.</li> <li>Click <b>OK</b> to save the profile.</li> </ol>
<b>Step 3</b>	Configure a decryption policy.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Decryption</b> and click <b>Add</b>.</li> <li>On the <b>General</b> tab, give the policy a descriptive <b>Name</b>.</li> <li>On the <b>Source</b> and <b>Destination</b> tabs, select <b>Any</b> to decrypt all SSH traffic.</li> <li>On the <b>URL Category</b> tab, select <b>Any</b> to decrypt all SSH traffic.</li> <li>On the <b>Options</b> tab, select <b>Decrypt</b> and select <b>SSH Proxy</b> as the <b>Type</b> of traffic to decrypt.</li> <li>(Optional) Select a <b>Decryption Profile</b> to apply additional settings to decrypted traffic.</li> <li>Click <b>OK</b> to save.</li> </ol>
<b>Step 4</b>	<b>Commit</b> the configuration.	With the an SSH Proxy decryption policy enabled, all SSH traffic identified by the policy is decrypted and identified as either regular SSH traffic or as SSH tunneled traffic. SSH tunneled traffic is blocked and restricted according to the profiles configured on the firewall. Traffic is re-encrypted as it exits the firewall.

# Configure Decryption Exceptions

You can purposefully exclude traffic from decryption based on source, destination, URL category, and service (ports and protocols). You can also exclude a specific server from decryption. See the following topics to configure [Decryption Exceptions](#):

- ▲ [Exclude Traffic from Decryption](#)
- ▲ [Exclude a Server from Decryption](#)

## Exclude Traffic from Decryption

To exclude applications or certain traffic from decryption, create a decryption policy rule that defines the traffic to be excluded from decryption and set the policy action to **No Decrypt**. Exclude traffic from decryption based on source, destination, URL category, and service (ports and protocols). Because policy rules are compared against incoming traffic in sequence, make sure that a decryption exclusion rule is listed first in your decryption policy.

Exclude Traffic from a Decryption Policy	
Step 1	<p>(Optional) Enable the firewall to block sessions with expired certificates and/or untrusted certificate issuers, without decrypting those sessions.</p> <p>1. Select <b>Objects &gt; Decryption Profile</b> and click <b>Add</b>.</p> <p>2. Give the profile rule a descriptive <b>Name</b> such as: Block certs and issues for No Decrypt traffic.</p> <p>3. Select <b>No Decryption</b> to block and control specific aspects of traffic that you are excluding from decryption. Select <b>Block sessions with expired certificates</b> and/or <b>Block sessions with untrusted issuers</b>.</p> <p>4. Click <b>OK</b> to save the profile rule.</p>
Step 2	<p>Configure a decryption policy rule.</p> <p>Use a decryption policy rule to exclude traffic from decryption based on source and destination zones and addresses, URL categories, ports, and protocols. This example shows how to exclude traffic categorized as financial or health-related from SSL Forward Proxy decryption.</p> <p>1. Go to <b>Policies &gt; Decryption</b> and click <b>Add</b>.</p> <p>2. Give the rule a descriptive <b>Name</b>, such as <i>No-Decrypt-Finance-Health</i>.</p> <p>3. On the <b>Source</b> and <b>Destination</b> tabs, select <b>Any</b> for the <b>Source Zone</b> and <b>Destination Zone</b> to apply the <i>No-Decrypt-Finance-Health</i> rule to all SSL traffic destined for an external server.</p> <p>4. On the <b>URL Category</b> tab, <b>Add</b> the URL categories financial-services and health-and-medicine to the policy, specifying that traffic that matches these categories will not be decrypted.</p> <p>5. On the <b>Options</b> tab, select <b>No Decrypt</b>.</p> <p>6. (Optional) Attach the decryption profile created in Step 1 to the policy. A decryption profile can be attached to a No Decrypt policy, to block and control aspects of the traffic being excluded from decryption.</p> <p>7. Click <b>OK</b> to save the <i>No-Decrypt-Finance-Health</i> rule.</p>

**Exclude Traffic from a Decryption Policy**

<b>Step 3</b> Move the decryption exclusion rule to the top of your decryption policy.	On the <b>Decryption &gt; Policies</b> page, select the policy <i>No-Decrypt-Finance-Health</i> , and click <b>Move Up</b> until it appears at the top of the list (or you can drag and drop the rule).  Decryption rules are enforced against incoming traffic in sequence and the first rule to match to traffic is enforced—moving the <b>No Decrypt</b> rule to the top of the rule list ensures that traffic defined to be excluded from decryption remains encrypted, even if the traffic is also matched to criteria defined in other decryption rules.
<b>Step 4</b> Save the changes.	<b>Commit</b> the configuration.

**Exclude a Server from Decryption**

You can exclude targeted server traffic from SSL decryption based on the common name (CN) in the server certificate. For example, if you have SSL decryption enabled, you could configure a decryption exception for the server on your corporate network that hosts the web services for your HR systems.

**Exclude a Server from Decryption**

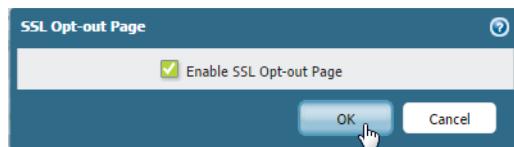
<b>Step 1</b> Import the targeted server certificate onto the firewall: <ol style="list-style-type: none"><li>1. On the <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> tab, select <b>Import</b>.</li><li>2. Enter a descriptive <b>Certificate Name</b>.</li><li>3. Browse for and select the targeted server <b>Certificate File</b>.</li><li>4. Click <b>OK</b>.</li></ol>	
<b>Step 2</b> Select the targeted server certificate on the <b>Device Certificates</b> tab and enable it as an SSL Exclude Certificate.  With the targeted server certificate imported on the firewall and designated as an SSL Exclude Certificate, the server traffic is not decrypted as it passes through the firewall.	

## Enable Users to Opt Out of SSL Decryption

In some cases, you might need to alert your users to the fact that the firewall is decrypting certain web traffic and allow them to terminate sessions that they do not want inspected. With SSL Opt Out enabled, the first time a user attempts to browse to an HTTPS site or application that matches your decryption policy, the firewall displays a response page notifying the user that it will decrypt the session. Users can either click **Yes** to allow decryption and continue to the site or click **No** to opt out of decryption and terminate the session. The choice to allow decryption applies to all HTTPS sites that users try to access for the next 24 hours, after which the firewall redisplays the response page. Users who opt out of SSL decryption cannot access the requested web page, or any other HTTPS site, for the next minute. After the minute elapses, the firewall redisplays the response page the next time the users attempt to access an HTTPS site.

The firewall includes a predefined SSL Decryption Opt-out Page that you can enable. You can optionally customize the page with your own text and/or images.

### Enable Users to Opt Out of SSL Decryption

<p><b>Step 1</b> <span style="color: #99cc33;">(Optional)</span> Customize the SSL Decryption Opt-out Page.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Response Pages</b>.</li> <li>2. Select the <b>SSL Decryption Opt-out Page</b> link.</li> <li>3. Select the <b>Predefined</b> page and click <b>Export</b>.</li> <li>4. Using the HTML text editor of your choice, edit the page.</li> <li>5. If you want to add an image, host the image on a web server that is accessible from your end user systems.</li> <li>6. Add a line to the HTML to point to the image. For example:  <pre>&lt;img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?1382722588"/&gt;</pre> </li> <li>7. Save the edited page with a new filename. Make sure that the page retains its UTF-8 encoding.</li> <li>8. Back on the firewall, select <b>Device &gt; Response Pages</b>.</li> <li>9. Select the <b>SSL Decryption Opt-out Page</b> link.</li> <li>10. Click <b>Import</b> and then enter the path and filename in the <b>Import File</b> field or <b>Browse</b> to locate the file.</li> <li>11. <span style="color: #99cc33;">(Optional)</span> Select the virtual system on which this login page will be used from the <b>Destination</b> drop-down or select shared to make it available to all virtual systems.</li> <li>12. Click <b>OK</b> to import the file.</li> <li>13. Select the response page you just imported and click <b>Close</b>.</li> </ol>
<p><b>Step 2</b> Enable SSL Decryption Opt Out.</p>	<ol style="list-style-type: none"> <li>1. On the <b>Device &gt; Response Pages</b> page, click the <b>Disabled</b> link.</li> <li>2. Select the <b>Enable SSL Opt-out Page</b> and click <b>OK</b>.</li> </ol> <div data-bbox="734 1584 1248 1731" style="text-align: center;">  </div> <ol style="list-style-type: none"> <li>3. <b>Commit</b> the changes.</li> </ol>

**Enable Users to Opt Out of SSL Decryption**

- Step 3** Verify that the Opt Out page displays when you attempt to browse to a site.

From a browser, go to an encrypted site that matches your decryption policy.

Verify that the SSL Decryption Opt-out response page displays.

**SSL Inspection**

In accordance with company security policy, the SSL encrypted connection you have initiated will be inspected for viruses, spyware, and other malware.

After the connection is inspected it will be re-encrypted and sent to its destination. No data will be lost.

IP: 31.13.69.80

Category: social-networking

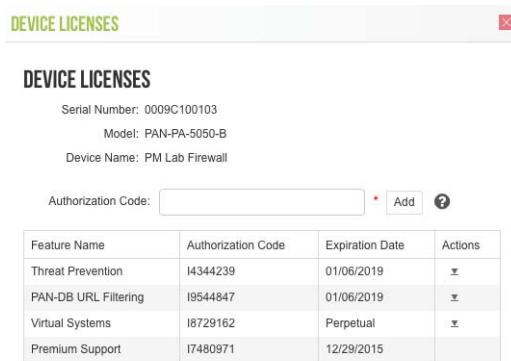
Would you like to proceed with this session?

# Configure Decryption Port Mirroring

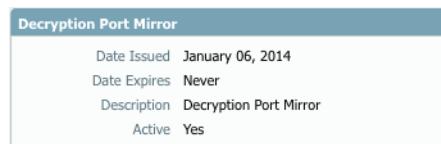
Before you can enable [Decryption Mirroring](#), you must obtain and install a Decryption Port Mirror license. The license is free of charge and can be activated through the support portal as described in the following procedure. After you install the Decryption Port Mirror license and reboot the firewall, you can enable decryption port mirroring.

## Configure Decryption Port Mirroring

- |  |  |
|--|--|
| <b>Step 1</b> Request a license for each device on which you want to enable decryption port mirroring. | <ol style="list-style-type: none"> <li>1. Log in to the <a href="#">Palo Alto Networks Support</a> site and navigate to the <b>Assets</b> tab.</li> <li>2. Select the device entry for the device you want to license and select <b>Actions</b>.</li> <li>3. Select <b>Decryption Port Mirror</b>. A legal notice displays.</li> <li>4. If you are clear about the potential legal implications and requirements, click <b>I understand and wish to proceed</b>.</li> <li>5. Click <b>Activate</b>.</li> </ol> |
|--|--|



- |   |   |
|---|---|
| <b>Step 2</b> Install the Decryption Port Mirror license on the firewall. | <ol style="list-style-type: none"> <li>1. From the firewall web interface, select <b>Device &gt; Licenses</b>.</li> <li>2. Click <b>Retrieve license keys from license server</b>.</li> <li>3. Verify that the license has been activated on the firewall.</li> </ol> |
|---|---|



- |  |   |
|--|---|
|  | <ol style="list-style-type: none"> <li>4. Reboot the firewall (<b>Device &gt; Setup &gt; Operations</b>). This feature will not be available for configuration until PAN-OS reloads.</li> </ol> |
|--|---|

<b>Configure Decryption Port Mirroring (Continued)</b>	
<b>Step 3</b> Enable the firewall to forward decrypted traffic. Superuser permission is required to perform this step.	<p><b>On a firewall with a single virtual system:</b></p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; Content - ID</b>.</li> <li>Select the <b>Allow forwarding of decrypted content</b> check box.</li> <li>Click <b>OK</b> to save.</li> </ol> <p><b>On a firewall with multiple virtual systems:</b></p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Virtual System</b>.</li> <li>Select a Virtual System to edit or create a new Virtual System by selecting <b>Add</b>.</li> <li>Select the <b>Allow forwarding of decrypted content</b> check box.</li> <li>Click <b>OK</b> to save.</li> </ol>
<b>Step 4</b> Enable an Ethernet interface to be used for decryption mirroring.	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Interfaces &gt; Ethernet</b>.</li> <li>Select the Ethernet interface that you want to configure for decryption port mirroring.</li> <li>Select <b>Decrypt Mirror</b> as the <b>Interface Type</b>. This interface type will appear only if the Decryption Port Mirror license is installed.</li> <li>Click <b>OK</b> to save.</li> </ol>
<b>Step 5</b> Enable mirroring of decrypted traffic.	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Decryption Profile</b>.</li> <li>Select an <b>Interface</b> to be used for <b>Decryption Mirroring</b>. The <b>Interface</b> drop-down contains all Ethernet interfaces that have been defined as the type: <b>Decrypt Mirror</b>.</li> <li>Specify whether to mirror decrypted traffic before or after policy enforcement. By default, the firewall will mirror all decrypted traffic to the interface before security policies lookup, which allows you to replay events and analyze traffic that generates a threat or triggers a drop action. If you want to only mirror decrypted traffic after security policy enforcement, select the <b>Forwarded Only</b> check box. With this option, only traffic that is forwarded through the firewall is mirrored. This option is useful if you are forwarding the decrypted traffic to other threat detection devices, such as a DLP device or another intrusion prevention system (IPS).</li> <li>Click <b>OK</b> to save the decryption profile.</li> </ol>
<b>Step 6</b> Attach the decryption profile rule (with decryption port mirroring enabled) to a decryption policy rule. All traffic decrypted based on the policy rule is mirrored.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Decryption</b>.</li> <li>Click <b>Add</b> to configure a decryption policy or select an existing decryption policy to edit.</li> <li>In the <b>Options</b> tab, select <b>Decrypt</b> and the <b>Decryption Profile</b> created in <b>Step 4</b>.</li> <li>Click <b>OK</b> to save the policy.</li> </ol>
<b>Step 7</b> Save the configuration.	Click <b>Commit</b> .

## Temporarily Disable SSL Decryption

In some cases you may want to temporarily disable SSL decryption. For example, if your users are having problems accessing an encrypted site or application, you may want to disable SSL decryption in order to troubleshoot the issue. Although you could disable the associated decryption policies, modifying the policies is a configuration change that requires a Commit. Instead, use the following command to temporarily disable SSL decryption and then re-enable it after you finish troubleshooting. This command does not require a commit and it does not persist in your configuration after a reboot.

### Temporarily Disable SSL Decryption

- |                            |  |
|----------------------------|--|
| • Disable SSL Decryption   | <code>set system setting ssl-decrypt skip-ssl-decrypt yes</code> |
| • Re-enable SSL Decryption | <code>set system setting ssl-decrypt skip-ssl-decrypt no</code>  |



# URL Filtering

---

---

The Palo Alto Networks URL filtering solution allows you to monitor and control how users access the web over HTTP and HTTPS.

- ▲ [URL Filtering Overview](#)
- ▲ [URL Filtering Concepts](#)
- ▲ [PAN-DB Categorization](#)
- ▲ [Enable a URL Filtering Vendor](#)
- ▲ [Determine URL Filtering Policy Requirements](#)
- ▲ [Monitor Web Activity](#)
- ▲ [Configure URL Filtering](#)
- ▲ [Customize the URL Filtering Response Pages](#)
- ▲ [Configure URL Admin Override](#)
- ▲ [Enable Safe Search Enforcement](#)
- ▲ [Set Up the PAN-DB Private Cloud](#)
- ▲ [URL Filtering Use Case Examples](#)
- ▲ [Troubleshoot URL Filtering](#)

# URL Filtering Overview

The Palo Alto Networks URL filtering solution complements [App-ID](#) by enabling you to configure the firewall to identify and control access to web (HTTP and HTTPS) traffic and to protect your network from attack.

With URL Filtering enabled, all web traffic is compared against the URL filtering database, which contains a listing of millions of websites that have been categorized into approximately 60-80 categories. You can use these URL categories as a match criteria in policies (Captive Portal, Decryption, Security, and QoS) or attach them as URL filtering profiles in security policy, to safely enable web access and control the traffic that traverses your network.

Although the Palo Alto Networks URL filtering solution supports both BrightCloud and PAN-DB, only the PAN-DB URL filtering solution allows you to choose between the *PAN-DB Public Cloud* and the *PAN-DB Private Cloud*. Use the public cloud solution if the Palo Alto Networks next-generation firewalls on your network can directly access the Internet. If the network security requirements in your enterprise prohibit the firewalls from directly accessing the Internet, you can deploy a PAN-DB private cloud on one or more M-500 appliances that function as PAN-DB servers within your network.

- ▲ [URL Filtering Vendors](#)
- ▲ [Interaction Between App-ID and URL Categories](#)
- ▲ [PAN-DB Private Cloud](#)

## URL Filtering Vendors

Palo Alto Networks firewalls support two URL filtering vendors:

- **PAN-DB**—A Palo Alto Networks developed URL filtering database that is tightly integrated into PAN-OS and the Palo Alto Networks threat intelligence cloud. PAN-DB provides high-performance local caching for maximum inline performance on URL lookups, and offers coverage against malicious URLs and IP addresses. As WildFire, which is a part of the Palo Alto Networks threat intelligence cloud, identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs), the PAN-DB database is updated with information on malicious URLs so that you can block malware downloads, and disable Command and Control (C&C) communications to protect your network from cyber threats.

To view a list of PAN-DB URL filtering categories, refer to

<https://urlfiltering.paloaltonetworks.com/CategoryList.aspx>.

- **BrightCloud**—A third-party URL database that is owned by Webroot, Inc. and is integrated into PAN-OS firewalls. For information on the BrightCloud URL database, visit <http://brightcloud.com>.

For instructions on configuring the firewall to use one of the supported URL Filtering vendors, see [Enable a URL Filtering Vendor](#).

## Interaction Between App-ID and URL Categories

The Palo Alto Networks URL filtering solution in combination with [App-ID](#) provides unprecedented protection against a full spectrum of cyber attacks, legal, regulatory, productivity, and resource utilization risks. While App-ID gives you control over what applications users can access, URL filtering provides control over related web activity. When combined with User-ID, you can enforce controls based on users and groups.

With today's application landscape and the way many applications use HTTP and HTTPS, you will need to use App-ID, URL filtering, or both in order to define comprehensive web access policies. App-ID signatures are granular and they allow you to identify shifts from one web-based application to another; URL filtering allows you to enforce actions based on a specific website or URL category. For example, while you can use URL filtering to control access to Facebook and/or LinkedIn, URL filtering cannot block the use of related applications such as email, chat, or other any new applications that are introduced after you implement policy. When combined with App-ID, you can control the use of related applications because of the granular application signatures that can identify each application and regulate access to Facebook while blocking access to Facebook chat, when defined in policy.

You can also use URL categories as a match criteria in policies. Instead of creating policies limited to either allow all or block all behavior, URL as a match criteria permits exception-based behavior and gives you more granular policy enforcement capabilities. For example, deny access to malware and hacking sites for all users, but allow access to users that belong to the IT-security group.

For some examples, see [URL Filtering Use Case Examples](#).

## PAN-DB Private Cloud

The PAN-DB private cloud is an on-premise solution that is suitable for organizations that prohibit or restrict the use of the PAN-DB public cloud service. With this on-premise solution, you can deploy one or more M-500 appliances as PAN-DB servers within your network or data center. The firewalls query the PAN-DB private cloud to perform URL lookups, instead of accessing the PAN-DB public cloud.

The process for performing URL lookups, in both the private and the public cloud is the same for the firewalls on the network. By default, the firewall is configured to access the public PAN-DB cloud. If you deploy a PAN-DB private cloud, you must configure the firewalls with a list of IP addresses or FQDNs to access the server(s) in the private cloud.



Firewalls running PAN-OS 5.0 or later versions can communicate with the PAN-DB private cloud.

When you [Set Up the PAN-DB Private Cloud](#), you can either configure the M-500 appliance(s) to have direct Internet access or keep it completely offline. Because the M-500 appliance requires database and content updates to perform URL lookups, if the appliance does not have an active Internet connection, you must manually download the updates to a server on your network and then, import the updates using SCP into each M-500 appliance in the PAN-DB private cloud. In addition, the appliances must be able to obtain the seed database and any other regular or critical content updates for the firewalls that it services.

To authenticate the firewalls that connect to the PAN-DB private cloud, a set of default server certificates are packaged with the appliance; you cannot import or use another server certificate for authenticating the firewalls. If you change the hostname on the M-500 appliance, the appliance automatically generates a new set of certificates to authenticate the firewalls.

- ▲ [M-500 Appliance for PAN-DB Private Cloud](#)
- ▲ [Differences Between the PAN-DB Public Cloud and PAN-DB Private Cloud](#)

## M-500 Appliance for PAN-DB Private Cloud

To deploy a PAN-DB private cloud, you need one or more M-500 appliances. The [M-500 appliance](#) ships in Panorama mode, and to be deployed as PAN-DB private cloud you must set it up to operate in PAN-URL-DB mode. In the PAN-URL-DB mode, the appliance provides URL categorization services for enterprises that do not want to use the PAN-DB public cloud.

The M-500 appliance when deployed as a PAN-DB private cloud uses two ports- MGT (Eth0) and Eth1; Eth2 is not available for use. The management port is used for administrative access to the appliance and for obtaining the latest content updates from the PAN-DB public cloud or from a server on your network. For communication between the PAN-DB private cloud and the firewalls on the network, you can use the MGT port or Eth1.



The M-100 appliance cannot be deployed as a PAN-DB private cloud.

The M-500 appliance in PAN-URL-DB mode:

- Does not have a web interface, it only supports a command-line interface (CLI).

- Cannot be managed by Panorama.
- Cannot be deployed in a high availability pair.
- Does not require a URL Filtering license. The firewalls must have a valid PAN-DB URL Filtering license to connect with and query the PAN-DB private cloud.
- Ships with a set of default server certificates that are used to authenticate the firewalls that connect to the PAN-DB private cloud. You cannot import or use another server certificate for authenticating the firewalls. If you change the hostname on the M-500 appliance, the appliance automatically generates a new set of certificates to authenticate the firewalls that it services.
- Can be reset to Panorama mode only. If you want to deploy the appliance as a dedicated Log Collector, switch to Panorama mode and then set it in log collector mode.

## Differences Between the PAN-DB Public Cloud and PAN-DB Private Cloud

Differences	PAN-DB Public Cloud	PAN-DB Private Cloud
Content and Database Updates	Content (regular and critical) updates and full database updates are published multiple times during the day. The firewall checks for critical updates whenever it queries the cloud servers for URL lookups.	Content updates and full URL database updates are available once a day during the work week.
URL Categorization Requests	Submit URL categorization change requests using the following options: <ul style="list-style-type: none"> <li>• Palo Alto Networks <a href="#">Test A Site</a> website.</li> <li>• URL filtering profile setup page on the firewall.</li> <li>• URL filtering log on the firewall.</li> </ul>	Submit URL categorization change requests only using the Palo Alto Networks <a href="#">Test A Site</a> website.
Unresolved URL Queries	If the firewall cannot resolve a URL query, the request is sent to the servers in the public cloud.	If the firewall cannot resolve a query, the request is sent to the M-500 appliance(s) in the PAN-DB private cloud. If there is no match for the URL, the PAN-DB private cloud sends a category <i>unknown</i> response to the firewall; the request is not sent to the public cloud unless you have configured the M-500 appliance to access the PAN-DB public cloud.  If the M-500 appliance(s) that constitute your PAN-DB private cloud is configured to be completely offline, it does not send any data or analytics to the public cloud.

# URL Filtering Concepts

- ▲ URL Categories
- ▲ URL Filtering Profile
- ▲ URL Filtering Profile Actions
- ▲ Block and Allow Lists
- ▲ Safe Search Enforcement
- ▲ Container Pages
- ▲ HTTP Header Logging
- ▲ URL Filtering Response Pages
- ▲ URL Category as Policy Match Criteria

## URL Categories

Each website defined in the URL filtering database is assigned one of approximately 60 different URL categories. There are two ways to make use of URL categorization on the firewall:

- **Block or allow traffic based on URL category**—You can create a URL Filtering profile that specifies an action for each URL category and attach the profile to a policy. Traffic that matches the policy would then be subject to the URL filtering settings in the profile. For example, to block all gaming websites you would set the block action for the URL category *games* in the URL profile and attach it to the security policy rule(s) that allow web access. See [Configure URL Filtering](#) for more information.
- **Match traffic based on URL category for policy enforcement**—If you want a specific policy rule to apply only to web traffic to sites in a specific category, you would add the category as match criteria when you create the policy rule. For example, you could use the URL category *streaming-media* in a QoS policy to apply bandwidth controls to all websites that are categorized as streaming media. See [URL Category as Policy Match Criteria](#) for more information.

By grouping websites into categories, it makes it easy to define actions based on certain types of websites. In addition to the standard URL categories, there are three additional categories:

not-resolved	<p>Indicates that the website was not found in the local URL filtering database and the firewall was unable to connect to the cloud database to check the category. When a URL category lookup is performed, the firewall first checks the dataplane cache for the URL; if no match is found, it checks the management plane cache, and if no match is found there, it queries the URL database in the cloud. In the case of the PAN-DB private cloud, the URL database in the cloud is not used for queries.</p> <p>Setting the action to block for traffic that is categorized as <i>not-resolved</i>, may be very disruptive to users. You could set the action as <a href="#">continue</a>, so that users can notify users that they are accessing a site that is blocked by company policy and provide the option to read the disclaimer and continue to the website.</p> <p>For more information on troubleshooting lookup issues, see <a href="#">Troubleshoot URL Filtering</a>.</p>
private-ip-addresses	Indicates that the website is a single domain (no sub-domains), the IP address is in the private IP range, or the URL root domain is unknown to the cloud.
unknown	<p>The website has not yet been categorized, so it does not exist in the URL filtering database on the firewall or in the URL cloud database.</p> <p>When deciding on what action to take for traffic categorized as <i>unknown</i>, be aware that setting the action to block may be very disruptive to users because there could be a lot of valid sites that are not in the URL database yet. If you do want a very strict policy, you could block this category, so websites that do not exist in the URL database cannot be accessed.</p> <p>See <a href="#">Configure URL Filtering</a>.</p>

## URL Filtering Profile

A URL filtering profile is a collection of URL filtering controls that are applied to individual security policy rules to enforce your web access policy. The firewall comes with a default profile that is configured to block threat-prone categories, such as malware, phishing, and adult. You can use the default profile in a security policy, clone it to be used as a starting point for new URL filtering profiles, or add a new URL filtering profile that will have all categories set to allow for visibility into the traffic on your network. You can then customize the newly added URL profiles and add lists of specific websites that should always be blocked or allowed, which provides more granular control over URL categories. For example, you may want to block social-networking sites, but allow some websites that are part of the social-networking category.

- ▲ [URL Filtering Profile Actions](#)
- ▲ [Block and Allow Lists](#)
- ▲ [Safe Search Enforcement](#)
- ▲ [Container Pages](#)
- ▲ [HTTP Header Logging](#)

## URL Filtering Profile Actions

The URL Filtering profile specifies an action for each known URL category. By default, all URL categories are set to allow when you [Create a new URL Filtering profile](#). This means that the users will be able to browse to all sites freely and the traffic will not be logged. The firewall also comes predefined default URL filtering profile that allows access to all categories except the following threat-prone categories, which it blocks: abused-drugs, adult, gambling, hacking, malware, phishing, questionable, and weapons.



As a best practice, if you want to create a custom URL Filtering category, clone the default URL filtering profile and change the action in all allow categories to either alert or continue so that you have visibility into the traffic. It is also a best practice to set the proxy-avoidance-and-anonymizers category to block.

Action	Description
<b>alert</b>	The website is allowed and a log entry is generated in the URL filtering log.
<b>allow</b>	The website is allowed and no log entry is generated.
<b>block</b>	The website is blocked and the user will see a response page and will not be able to continue to the website. A log entry is generated in the URL filtering log.
<b>continue</b>	<p>The user will be prompted with a response page indicating that the site has been blocked due to company policy, but the user is prompted with the option to continue to the website. The <b>continue</b> action is typically used for categories that are considered benign and is used to improve the user experience by giving them the option to continue if they feel the site is incorrectly categorized. The response page message can be customized to contain details specific to your company. A log entry is generated in the URL filtering log.</p> <p> The Continue page will not be displayed properly on client machines that are configured to use a proxy server.</p>
<b>override</b>	<p>The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security admin or helpdesk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL filtering log. See <a href="#">Configure URL Admin Override</a>.</p> <p> The Override page will not be displayed properly on client machines that are configured to use a proxy server.</p>
<b>none</b>	<p>The <b>none</b> action only applies to custom URL categories. Select <b>none</b> to ensure that if multiple URL profiles exist, the custom category will not have any impact on other profiles. For example, if you have two URL profiles and the custom URL category is set to <b>block</b> in one of the profiles, the other profile should have the action set to <b>none</b> if you do not want it to apply.</p> <p>Also, in order to delete a custom URL category, it must be set to <b>none</b> in any profile where it is used.</p>

## Block and Allow Lists

In some cases you might want to block a category, but allow a few specific sites in that category. Alternatively, you might want to allow some categories, but block individual sites in the category. You do this by adding the IP addresses or URLs of these sites in the Block list and Allow list sections of the URL Filtering profile to [Define websites that should always be blocked or allowed](#). When entering URLs in the Block List or Allow List, enter each URL or IP address in a new row separated by a new line. When using wildcards in the URLs, follow these rules:

- Do not include HTTP and HTTPS when defining URLs. For example, enter www.paloaltonetworks.com or paloaltonetworks.com instead of https://www.paloaltonetworks.com.

- Entries in the block list must be an exact match and are case-insensitive.

For example: If you want to prevent a user from accessing any website within the domain paloaltonetworks.com, you would also add \*.paloaltonetworks.com, so whatever domain prefix (http://, www, or a sub-domain prefix such as mail.paloaltonetworks.com) is added to the address, the specified action will be taken. The same applies to the sub-domain suffix; if you want to block paloaltonetworks.com/en/US, you would need to add paloaltonetworks.com/\* as well.

Further, if you want to limit access to a domain suffix such as `paloaltonetworks.com.au`, you must add a /, so that the match restricts a dot that follows .com. In this case, you need to add the entry as `*.paloaltonetworks.com/`

Block and allow lists support wildcard patterns. The following characters are considered separators:

.

/

?

&

=

;

+

Every substring that is separated by the characters listed above is considered a token. A token can be any number of ASCII characters that does not contain any separator character or \*. For example, the following patterns are valid:

`*.yahoo.com` (tokens are: "\*", "yahoo" and "com")

`www.*.com` (tokens are: "www", "\*" and "com")

`www.yahoo.com/search=*` (tokens are: "www", "yahoo", "com", "search", "\*")

The following patterns are invalid because the character "\*" is not the only character in the token.

`ww*.yahoo.com`

`www.y*.com`

## Safe Search Enforcement

Many search engines have a safe search setting that filters out adult images and videos in search query return traffic. On the firewall, you can [Enable Safe Search Enforcement](#) so that the firewall will block search results if the end user is not using the strictest safe search settings in the search query. The firewall can enforce safe search for the following search providers: Google, Yahoo, Bing, Yandex, and YouTube. This is a best-effort setting and is not guaranteed by the search providers to work with every website.

To use this feature you must enable the **Safe Search Enforcement** option in a URL filtering profile and attach it to a security policy rule. The firewall will then block any matching search query return traffic that is not using the strictest safe search settings. There are two methods for blocking the search results:

- [Block Search Results that are not Using Strict Safe Search Settings](#)—When an end user attempts to perform a search without first enabling the strictest safe search settings, the firewall blocks the search query results and displays the URL Filtering Safe Search Block Page. By default, this page will provide a URL to the search provider settings for configuring safe search.
- [Enable Transparent Safe Search Enforcement](#)—When an end user attempts to perform a search without first enabling the strict safe search settings, the firewall blocks the search results with an HTTP 503 status code and redirects the search query to a URL that includes the safe search parameters. You enable this functionality by importing a new URL Filtering Safe Search Block Page containing the JavaScript for rewriting the search URL to include the strict safe search parameters. In this configuration, users will not see the block page, but will instead be automatically redirected to a search query that enforces the strictest safe search options. This safe search enforcement method requires content release version 475 or later and is only supported for Google, Yahoo, and Bing searches.

Also, because most search providers now use SSL to return search results, you must also configure a [Decryption](#) policy rule for the search traffic to enable the firewall to inspect the search traffic and enforce safe search.



Safe search enforcement enhancements and support for new search providers is periodically added in content releases. This information is detailed in the Application and Threat Content Release Notes. How sites are judged to be safe or unsafe is performed by each search provider, not by Palo Alto Networks.

Safe search settings differ by search provider as detailed in [Table: Search Provider Safe Search Settings](#).

**Table: Search Provider Safe Search Settings**

Search Provider	Safe Search Setting Description
Google/YouTube	<p>Offers safe search on individual computers or network-wide through Google's safe search virtual IP address:</p> <p><b>Safe Search Enforcement for Google Searches on Individual Computers</b></p> <p>In the <a href="#">Google Search Settings</a>, the <b>Filter explicit results</b> setting enables safe search functionality. When enabled, the setting is stored in a browser cookie as <code>FF=</code> and passed to the server each time the user performs a Google search.</p> <p>Appending <code>safe=active</code> to a Google search query URL also enables the strictest safe search settings.</p> <p><b>Safe Search Enforcement for Google and YouTube Searches using a Virtual IP Address</b></p> <p>Google provides servers that <a href="#">Lock SafeSearch</a> (<code>forcesafesearch.google.com</code>) settings in every Google and YouTube search. By adding a DNS entry for <code>www.google.com</code> and <code>www.youtube.com</code> (and other relevant Google and YouTube country subdomains) that includes a CNAME record pointing to <code>forcesafesearch.google.com</code> to your DNS server configuration, you can ensure that all users on your network are using strict safe search settings every time they perform a Google or YouTube search. Keep in mind, however, that this solution is not compatible with Safe Search Enforcement on the firewall. Therefore, if you are using this option to force safe search on Google, the best practice is to block access to other search engines on the firewall by creating custom URL categories and adding them to the block list in the URL filtering profile.</p> <p> If you plan to use the Google Lock SafeSearch solution, consider configuring DNS Proxy (<a href="#">Network &gt; DNS Proxy</a>) and setting the inheritance source as the Layer 3 interface on which the firewall receives DNS settings from service provider via DHCP. You would configure the DNS proxy with <b>Static Entries</b> for <code>www.google.com</code> and <code>www.youtube.com</code>, using the local IP address for the <code>forcesafesearch.google.com</code> server.</p>
Yahoo	<p>Offers safe search on individual computers only. The <a href="#">Yahoo Search Preferences</a> includes three SafeSearch settings: <b>Strict</b>, <b>Moderate</b>, or <b>Off</b>. When enabled, the setting is stored in a browser cookie as <code>vm=</code> and passed to the server each time the user performs a Yahoo search.</p> <p>Appending <code>vm=r</code> to a Yahoo search query URL also enables the strictest safe search settings.</p> <p> When performing a search on Yahoo Japan (<code>yahoo.co.jp</code>) while logged into a Yahoo account, end users must also enable the <b>SafeSearch Lock</b> option.</p>
Bing	<p>Offers safe search on individual computers or through their <a href="#">Bing in the Classroom</a> program. The <a href="#">Bing Settings</a> include three SafeSearch settings: <b>Strict</b>, <b>Moderate</b>, or <b>Off</b>. When enabled, the setting is stored in a browser cookie as <code>adlt=</code> and passed to the server each time the user performs a Bing search.</p> <p>Appending <code>adlt=strict</code> to a Bing search query URL also enables the strictest safe search settings.</p> <p>The Bing SSL search engine does not enforce the safe search URL parameters and you should therefore consider blocking Bing over SSL for full safe search enforcement.</p>

## Container Pages

A container page is the main page that a user accesses when visiting a website, but additional websites may be loaded within the main page. If the **Log Container page only** option is enabled in the URL filtering profile, only the main container page will be logged, not subsequent pages that may be loaded within the container page. Because URL filtering can potentially generate a lot of log entries, you may want to turn on this option, so log entries will only contain those URIs where the requested page file name matches the specific mime-types. The default set includes the following mime-types:

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml



If you have enabled the **Log container page only** option, there may not always be a correlated URL log entry for threats detected by antivirus or vulnerability protection.

## HTTP Header Logging

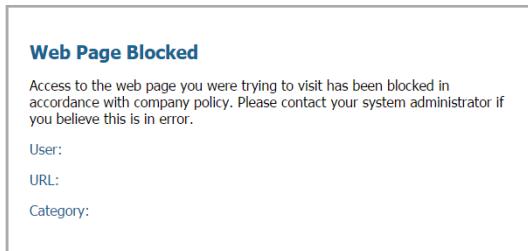
URL filtering provides visibility and control over web traffic on your network. For improved visibility into web content, you can configure the URL Filtering profile to log HTTP header attributes included in a web request. When a client requests a web page, the HTTP header includes the user agent, referer, and x-forwarded-for fields as attribute-value pairs and forwards them to the web server. When enabled for logging HTTP headers, the firewall logs the following attribute-value pairs in the URL Filtering logs:

Attribute	Description
User-Agent	The web browser that the user used to access the URL, for example, Internet Explorer. This information is sent in the HTTP request to the server.
Referer	The URL of the web page that linked the user to another web page; it is the source that redirected (referred) the user to the web page that is being requested.
X-Forwarded-For (XFF)	The option in the HTTP request header field that preserves the IP address of the user who requested the web page. If you have a proxy server on your network, the XFF allows you to identify the IP address of the user who requested the content, instead of only recording the proxy server's IP address as source IP address that requested the web page.

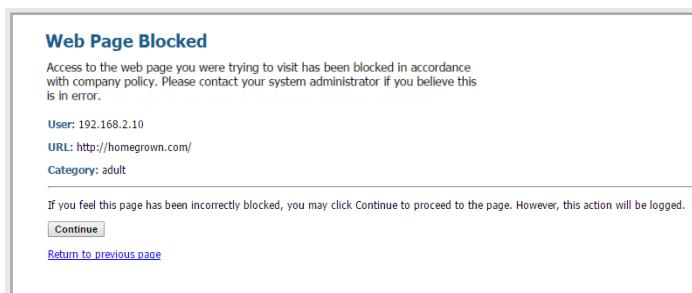
## URL Filtering Response Pages

The firewall provides three predefined response pages that display by default when a user attempts to browse to a site in a category that is configured with one of the block actions in the [URL Filtering Profile](#) (block, continue, or override) or when [Safe Search Enforcement](#) is enabled:

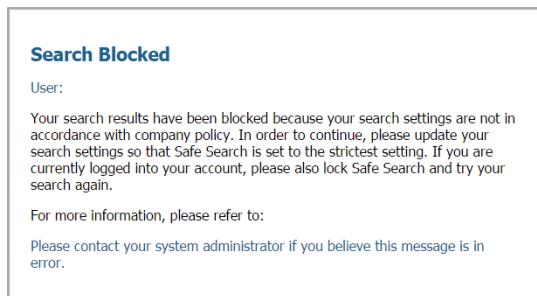
- **URL Filtering and Category Match Block Page**—Access blocked by a [URL Filtering Profile](#) or because the URL category is blocked by a security policy.



- **URL Filtering Continue and Override Page**—Page with initial block policy that allows users to bypass the block by clicking **Continue**. With URL Admin Override enabled, ([Configure URL Admin Override](#)), after clicking **Continue**, the user must supply a password to override the policy that blocks the URL.



- **URL Filtering Safe Search Block Page**—Access blocked by a security policy with a URL filtering profile that has the Safe Search Enforcement option enabled (see [Enable Safe Search Enforcement](#)). The user will see this page if a search is performed using Google, Bing, Yahoo, or Yandex and their browser or search engine account setting for Safe Search is not set to strict.



You can either use the predefined pages, or you can [Customize the URL Filtering Response Pages](#) to communicate your specific acceptable use policies and/or corporate branding. In addition, you can use the [URL Filtering Response Page Variables](#) for substitution at the time of the block event or add one of the supported [Response Page References](#) to external images, sounds, or style sheets.

**URL Filtering Response Page Variables**

Variable	Usage
<user/>	The firewall replaces the variable with the username (if available via User-ID) or IP address of the user when displaying the response page.
<url/>	The firewall replaces the variable with the requested URL when displaying the response page.
<category/>	The firewall replaces the variable with the URL filtering category of the blocked request.
<pan_form/>	HTML code for displaying the <b>Continue</b> button on the URL Filtering Continue and Override page.

You can also add code that triggers the firewall to display different messages depending on what URL category the user is attempting to access. For example, the following code snippet from a response page specifies to display Message 1 if the URL category is games, Message 2 if the category is travel, or Message 3 if the category is kids:

```
var cat = "<category/>";
switch(cat)
{
    case 'games':
        document.getElementById("warningText").innerHTML = "Message 1";
        break;
    case 'travel':
        document.getElementById("warningText").innerHTML = "Message 2";
        break;
    case 'kids':
        document.getElementById("warningText").innerHTML = "Message 3";
        break;
}
```

Only a single HTML page can be loaded into each virtual system for each type of block page. However, other resources such as images, sounds, and cascading style sheets (CSS files) can be loaded from other servers at the time the response page is displayed in the browser. All references must include a fully qualified URL.

**Response Page References**

Reference Type	Example HTML Code
Image	
Sound	<embed src="http://simplythebest.net/sounds/WAV/WAV_files/movie_WAV_files/_do_not_go.wav" volume="100" hidden="true" autostart="true">
Style Sheet	<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />
Hyperlink	<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">View Corporate Policy</a>

## URL Category as Policy Match Criteria

Use [URL Categories](#) as a match criteria in a policy rule for more granular enforcement. For example, suppose you have configured [Decryption](#), but you want to exclude traffic to certain types of websites (for example, healthcare or financial services) from being decrypted. In this case you could create a decryption policy rule that matches those categories and set the action to no-decrypt. By placing this rule above the rule to decrypt all traffic, you can ensure that web traffic with URL categories that match the no-decrypt rule, and all other traffic would match the subsequent rule.

The following table describes the policy types that accept URL category as match criteria:

Policy Type	Description
Captive Portal	To ensure that users authenticate before being allowed access to a specific category, you can attach a URL category as a match criterion for the Captive Portal policy.
Decryption	Decryption policies can use URL categories as match criteria to determine if specified websites should be decrypted or not. For example, if you have a decryption policy with the action <i>decrypt</i> for all traffic between two zones, there may be specific website categories, such as <i>financial-services</i> and/or <i>health-and-medicine</i> , that should not be decrypted. In this case, you would create a new decryption policy with the action of <i>no-decrypt</i> that precedes the <i>decrypt</i> policy and then defines a list of URL categories as match criteria for the policy. By doing this, each URL category that is part of the no-decrypt policy will not be decrypted. You could also configure a custom URL category to define your own list of URLs that can then be used in the no-decrypt policy.
QoS	QoS policies can use URL categories to allocate throughput levels for specific website categories. For example, you may want to allow the streaming-media category, but limit throughput by adding the URL category as match criteria to the QoS policy.
Security	In security policies you can use URL categories both as a match criteria in the <b>Service/URL Category</b> tab, and in URL filtering profiles that are attached in the <b>Actions</b> tab.  If for example, the IT-security group in your company needs access to the hacking category, while all other users are denied access to the category, you must create the following rules: <ul style="list-style-type: none"> <li>• A security rule that allows the IT-Security group to access content categorized as hacking. The security rule references the <i>hacking</i> category in the <b>Services/URL Category</b> tab and IT-Security group in the <b>Users</b> tab.</li> <li>• Another security rule that allows general web access for all users. To this rule you attach a URL filtering profile that blocks the hacking category.</li> </ul> The policy that allows access to hacking must be listed before the policy that blocks hacking. This is because security policy rules are evaluated top down, so when a user who is part of the security group attempts to access a hacking site, the policy rule that allows access is evaluated first and will allow the user access to the hacking sites. Users from all other groups are evaluated against the general web access rule which blocks access to the hacking sites.

# PAN-DB Categorization

- ▲ PAN-DB URL Categorization Components
- ▲ PAN-DB URL Categorization Workflow

## PAN-DB URL Categorization Components

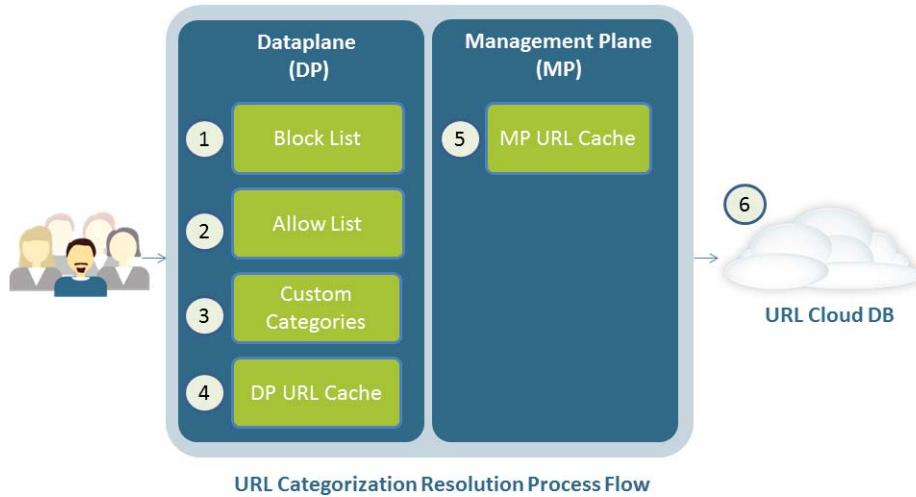
The following table describes the PAN-DB components in detail. The BrightCloud system works similarly, but does not use an initial seed database.

Component	Description
URL Filtering Seed Database	<p>The initial seed database downloaded to the firewall is a small subset of the database that is maintained on the Palo Alto Networks URL cloud servers. The reason this is done is because the full database contains millions of URLs and many of these URLs may never be accessed by your users. When downloading the initial seed database, you select a region (North America, Europe, APAC, Japan). Each region contains a subset of URLs most accessed for the given region. This allows the firewall to store a much smaller URL database for better URL lookup performance. If a user accesses a website that is not in the local URL database, the firewall queries the full cloud database and then adds the new URL to the local database. This way the local database on the firewall is continually populated/customized based on actual user activity.</p> <p>Note that re-downloading the PAN-DB seed database or switching the URL database vendor from PAN-DB to BrightCloud will clear the local database.</p>
Cloud Service  See <a href="#">Differences Between the PAN-DB Public Cloud and PAN-DB Private Cloud</a> , for information on the private cloud.	<p>The PAN-DB cloud service is implemented using Amazon Web Services (AWS). AWS provides a distributed, high-performance, and stable environment for seed database downloads and URL lookups for Palo Alto Networks firewalls and communication is performed over SSL. The AWS cloud systems hold the entire PAN-DB and is updated as new URLs are identified. The PAN-DB cloud service supports an automated mechanism to update the firewall's local URL database if the version does not match. Each time the firewall queries the cloud servers for URL lookups, it will also check for critical updates. If there have been no queries to the cloud servers for more than 30 minutes, the firewall will check for updates on the cloud systems.</p> <p>The cloud system also provides a mechanism to submit URL category change requests. This is performed through the test-a-site service and is available directly from the device (URL filtering profile setup) and from the Palo Alto Networks <a href="#">Test A Site</a> website. You can also submit a URL categorization change request directly from the URL filtering log on the firewall in the log details section.</p>

Component	Description
Management Plane (MP) URL Cache	<p>When you activate PAN-DB on the firewall, the firewall downloads a seed database from one of the PAN-DB cloud servers to initially populate the local cache for improved lookup performance. Each regional seed database contains the top URLs for the region and the size of the seed database (number of URL entries) also depends on the <a href="#">platform</a>. The URL MP cache is automatically written to the firewall's local drive every eight hours, before the firewall is rebooted, or when the cloud upgrades the URL database version on the firewall. After rebooting the firewall, the file that was saved to the local drive will be loaded to the MP cache. A least recently used (LRU) mechanism is also implemented in the URL MP cache in case the cache is full. If the cache becomes full, the URLs that have been accessed the least will be replaced by the newer URLs.</p>
Dataplane (DP) URL Cache	<p>This is a subset of the MP cache and is a customized, dynamic URL database that is stored in the dataplane (DP) and is used to improve URL lookup performance. The URL DP cache is cleared at each firewall reboot. The number of URLs that are stored in the URL DP cache varies by hardware platform and the current URLs stored in the TRIE (data structure). A least recently used (LRU) mechanism is implemented in the DP cache in case the cache is full. If the cache becomes full, the URLs that have been accessed the least will be replaced by the newer URLs. Entries in the URL DP cache expire after a specified period of time and the expiration period cannot be changed by the administrator.</p>

## PAN-DB URL Categorization Workflow

When a user attempts to access a URL and the URL category needs to be determined, the firewall will compare the URL with the following components (in order) until a match has been found:



If a URL query matches an expired entry in the URL DP cache, the cache responds with the expired category, but also sends a URL categorization query to the management plane. This is done to avoid unnecessary delays in the DP, assuming that the frequency of changing categories is low. Similarly, in the URL MP cache, if a URL query from the DP matches an expired entry in the MP, the MP responds to the DP with the expired category and will also send a URL categorization request to the cloud service. Upon getting the response from the cloud, the firewall will resend the updated response to the DP.

As new URLs and categories are defined or if critical updates are needed, the cloud database will be updated. Each time the firewall queries the cloud for a URL lookup or if no cloud lookups have occurred for 30 minutes, the database versions on the firewall be compared and if they do not match, an incremental update will be performed.

## Enable a URL Filtering Vendor

To enable URL filtering on a firewall, you must purchase and activate a URL Filtering license for one of the supported [URL Filtering Vendors](#) and then install the database for the vendor you selected.



Starting with PAN-OS 6.0, firewalls managed by Panorama do not need to be running the same URL filtering vendor that is configured on Panorama. For firewalls running PAN-OS 6.0 or later, when a mismatch is detected between the vendor enabled on the firewalls and what is enabled on Panorama, the firewalls can automatically migrate URL categories and/or URL profiles to (one or more) categories that align with that of the vendor enabled on it. For guidance on how to configure URL Filtering on Panorama if you are managing firewalls running different PAN-OS versions, refer to the [Panorama Administrator's Guide](#).

If you have valid licenses for both PAN-DB and BrightCloud, activating the PAN-DB license automatically deactivates the BrightCloud license (and vice versa). At a time, only one URL filtering license can be active on a firewall.

- ▲ [Enable PAN-DB URL Filtering](#)
- ▲ [Enable BrightCloud URL Filtering](#)

## Enable PAN-DB URL Filtering

### Enable PAN-DB URL Filtering

<p><b>Step 1</b> Obtain and install a PAN-DB URL filtering license and confirm that it is installed.</p> <p> If the license expires, PAN-DB URL Filtering continues to work based on the URL category information that exists in the dataplane and management plane caches. However, URL cloud lookups and other cloud-based updates will not function until you install a valid license.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Licenses</b> and, in the License Management section, select the license installation method:           <ul style="list-style-type: none"> <li>• <b>Retrieve license keys from license server</b></li> <li>• <b>Activate feature using authorization code</b></li> <li>• <b>Manually upload license key</b></li> </ul> </li> <li>2. After installing the license, confirm that the PAN-DB URL Filtering section, <b>Date Expires</b> field, displays a valid date.</li> </ol>
<p><b>Step 2</b> Download the initial seed database and activate PAN-DB URL Filtering.</p> <p> The firewall must have Internet access; you cannot manually upload the PAN-DB seed database.</p>	<ol style="list-style-type: none"> <li>1. In the PAN-DB URL Filtering section, <b>Download Status</b> field, click <b>Download Now</b>.</li> <li>2. Choose a region (North America, Europe, APAC, Japan) and then click <b>OK</b> to start the download.</li> <li>3. After the download completes, click <b>Activate</b>.</li> </ol> <p> If PAN-DB is already the active URL filtering vendor and you click <b>Re-Download</b>, this will reactivate PAN-DB by clearing the dataplane and management plane caches and replacing them with the contents of the new seed database. You should avoid doing this unless it is necessary, as you will lose your cache, which is customized based on the web traffic that has previously passed through the firewall based on user activity.</p>
<p><b>Step 3</b> Schedule the firewall to download dynamic updates for Applications and Threats.</p> <p> A Threat Prevention license is required to receive content updates, which covers Antivirus and Applications and Threats.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Dynamic Updates</b>.</li> <li>2. In the Schedule field in the Applications and Threats section, click the <b>None</b> link to schedule periodic updates.</li> </ol> <p> You can only schedule dynamic updates if the firewall has direct Internet access. If updates are already scheduled in a section, the link text displays the schedule settings.</p> <p>The Applications and Threats updates might contain updates for URL filtering related to the <b>Safe Search Enforcement</b> option in the URL filtering profile (<b>Objects &gt; Security Profiles &gt; URL Filtering</b>). For example, if Palo Alto Networks adds support for a new search provider vendor or if the method used to detect the Safe Search setting for an existing vendor changes, the Application and Threats updates will include that update.</p>

## Enable BrightCloud URL Filtering

Enable BrightCloud URL Filtering	
Step 1	<p>Obtain and install a BrightCloud URL filtering license and confirm that it is installed.</p> <p> BrightCloud has an option in the URL filtering profile (<b>Objects &gt; Security Profiles &gt; URL Filtering</b>) to either allow all categories or block all categories if the license expires.</p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Licenses</b> and, in the <b>License Management</b> section, select the license installation method:           <ul style="list-style-type: none"> <li>• <b>Activate feature using authorization code</b></li> <li>• <b>Retrieve license keys from license server</b></li> <li>• <b>Manually upload license key</b></li> </ul> </li> <li>After installing the license, confirm that the BrightCloud URL Filtering section, <b>Date Expires</b> field, displays a valid date.</li> </ol>
Step 2	<p>Install the BrightCloud database.</p> <p>The way you do this depends on whether or not the firewall has direct Internet access.</p> <p><b>Firewall with Direct Internet Access</b></p> <p>Select <b>Device &gt; Licenses</b> and in the BrightCloud URL Filtering section, Active field, click the <b>Activate</b> link to install the BrightCloud database. This operation automatically initiates a system reset.</p> <p><b>Firewall without Direct Internet Access</b></p> <ol style="list-style-type: none"> <li>Download the BrightCloud database to a host that has Internet access. The firewall must have access to the host:           <ol style="list-style-type: none"> <li>On a host with Internet access, go to the Palo Alto Support website (<a href="https://support.paloaltonetworks.com">https://support.paloaltonetworks.com</a>) and log in.</li> <li>In the Resources section, click <b>Dynamic Updates</b>.</li> <li>In the BrightCloud Database section, click <b>Download</b> and save the file to the host.</li> </ol> </li> <li>Upload the database to the firewall:           <ol style="list-style-type: none"> <li>Log in to the firewall, select <b>Device &gt; Dynamic Updates</b> and click <b>Upload</b>.</li> <li>For the <b>Type</b>, select <b>URL Filtering</b>.</li> <li>Enter the path to the <b>File</b> on the host or click <b>Browse</b> to find it, then click <b>OK</b>. When the Status is <b>Completed</b>, click <b>Close</b>.</li> </ol> </li> <li>Install the database:           <ol style="list-style-type: none"> <li>Select <b>Device &gt; Dynamic Updates</b> and click <b>Install From File</b>.</li> <li>For the <b>Type</b>, select <b>URL Filtering</b>. The firewall automatically selects the file you just uploaded.</li> <li>Click <b>OK</b> and, when the Result is <b>Succeeded</b>, click <b>Close</b>.</li> </ol> </li> </ol>
Step 3	<p>Enable cloud lookups for dynamically categorizing a URL if the category is not available on the local BrightCloud database.</p> <ol style="list-style-type: none"> <li><a href="#">Access the PAN-OS CLI</a>.</li> <li>Enter the following commands to enable dynamic URL filtering:</li> </ol> <pre>configure set deviceconfig setting url dynamic-url yes commit</pre>

**Enable BrightCloud URL Filtering (Continued)**

<p><b>Step 4</b> Schedule the firewall to download dynamic updates for Applications and Threats signatures and URL filtering.</p> <p>You can only schedule dynamic updates if the firewall has direct Internet access.</p> <p>The Applications and Threats updates might contain updates for URL filtering related to the <b>Safe Search Enforcement</b> option in the URL filtering profile. For example, if Palo Alto Networks adds support for a new search provider vendor or if the method used to detect the Safe Search setting for an existing vendor changes, the Application and Threats updates will include that update.</p> <p>BrightCloud updates include a database of approximately 20 million websites that are stored locally on the firewall. You must schedule URL filtering updates to receive BrightCloud database updates.</p>
<p> A Threat Prevention license is required to receive Antivirus and Applications and Threats updates.</p>

1. Select **Device > Dynamic Updates**.
2. In the Applications and Threats section, Schedule field, click the **None** link to schedule periodic updates.
3. In the URL Filtering section, Schedule field, click the **None** link to schedule periodic updates.



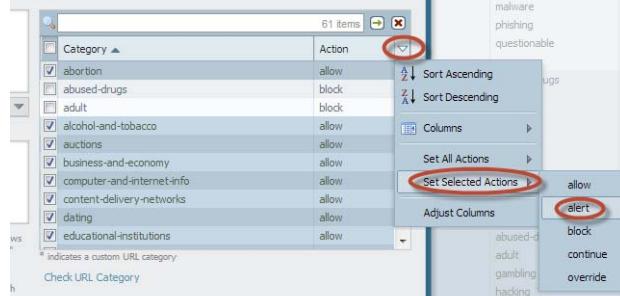
If updates are already scheduled in a section, the link text displays the schedule settings.

# Determine URL Filtering Policy Requirements

The recommended practice for deploying URL filtering in your organization is to first start with a passive URL filtering profile that will alert on most categories. After setting the alert action, you can then monitor user web activity for a few days to determine patterns in web traffic. After doing so, you can then make decisions on the websites and website categories that should be controlled.

In the procedure that follows, threat-prone sites will be set to block and the other categories will be set to alert, which will cause all websites traffic to be logged. This may potentially create a large amount of log files, so it is best to do this for initial monitoring purposes to determine the types of websites your users are accessing. After determining the categories that your company approves of, those categories should then be set to allow, which will not generate logs. You can also reduce URL filtering logs by enabling the **Log container page only** option in the URL Filtering profile, so only the main page that matches the category will be logged, not subsequent pages/categories that may be loaded within the container page.

## Configure and Apply a Passive URL Filtering Profile

<b>Step 1</b> Create a new URL Filtering profile.	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li> <li>Select the default profile and then click <b>Clone</b>. The new profile will be named <b>default-1</b>.</li> <li>Select the <b>default-1</b> profile and rename it. For example, rename it to URL-Monitoring.</li> </ol>
<b>Step 2</b> Configure the action for all categories to <b>alert</b> , except for threat-prone categories, which should remain blocked. <p><b>Tip:</b> To select all items in the category list from a Windows system, click the first category, then hold down the shift key and click the last category—this will select all categories. Hold the control key (ctrl) down and click items that should be deselected. On a Mac, do the same using the shift and command keys. You could also just set all categories to alert and manually change the recommended categories back to block.</p>	<ol style="list-style-type: none"> <li>In the section that lists all URL categories, select all categories.</li> <li>To the right of the <i>Action</i> column heading, mouse over and select the down arrow and then select <b>Set Selected Actions</b> and choose <b>alert</b>.</li> </ol>  <ol style="list-style-type: none"> <li>To ensure that you block access to threat-prone sites, select the following categories and then set the action to <b>block</b>: abused-drugs, adult, gambling, hacking, malware, phishing, questionable, weapons.</li> <li>Click <b>OK</b> to save the profile.</li> </ol>
<b>Step 3</b> Apply the URL Filtering profile to the security policy rule(s) that allows web traffic for users.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and select the appropriate security policy to modify it.</li> <li>Select the <b>Actions</b> tab and in the <b>Profile Setting</b> section, click the drop-down for <b>URL Filtering</b> and select the new profile.</li> <li>Click <b>OK</b> to save.</li> </ol>
<b>Step 4</b> Save the configuration.	Click <b>Commit</b> .

**Configure and Apply a Passive URL Filtering Profile (Continued)**

<p><b>Step 5</b> View the URL filtering logs to determine all of the website categories that your users are accessing. In this example, some categories are set to block, so those categories will also appear in the logs.</p> <p>For information on viewing the logs and generating reports, see <a href="#">Monitor Web Activity</a>.</p>	Select <b>Monitor &gt; Logs &gt; URL Filtering</b> . A log entry will be created for any website that exists in the URL filtering database that is in a category that is set to any action other than <b>allow</b> .
--	--

## Monitor Web Activity

The ACC, URL filtering logs and reports show all user web activity for URL categories that are set to **alert**, **block**, **continue**, or **override**. By monitoring the logs, you can gain a better understanding of the web activity of your user base to determine a web access policy.

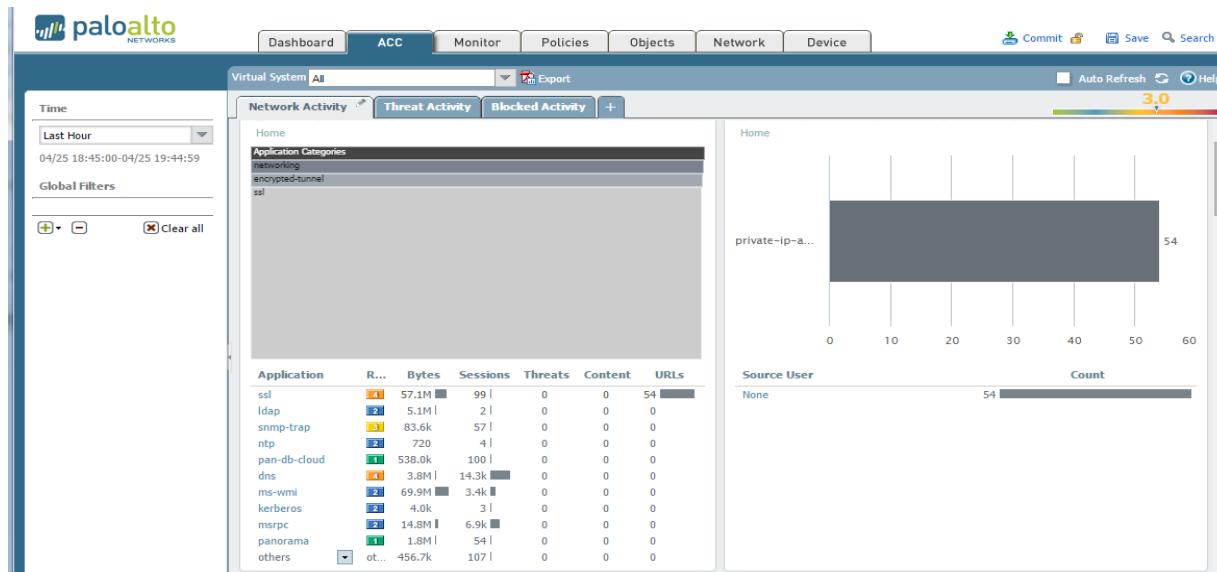
The following topics describe how to monitor web activity:

- ▲ [Monitor Web Activity of Network Users](#)
- ▲ [View the User Activity Report](#)
- ▲ [Configure Custom URL Filtering Reports](#)

## Monitor Web Activity of Network Users

You can use the ACC, and the URL filtering reports and logs that are generated on the firewall to track user activity.

For a quick view of the most common categories users access in your environment, check the **ACC** widgets. Most widgets in the Network Activity tab, allows you to sort on URLs. For example, in the Application Usage widget, you can see that the networking category is the most accessed category, followed by encrypted tunnel, and ssl. You can also view the list of **Threat Activity** and **Blocked Activity** sorted on URLs.



From the ACC, you can directly **Jump to the Logs** or you can navigate to **Monitor > Logs > URL filtering** to view the URL filtering logs. The following bullet points show examples of the URL filtering logs () .

- **Alert log**—In this log, the category is shopping and the action is alert.

Receive Time	Category	URL	Source	Destination	Destin... Country	Application	Action	Decrypted	Source User
11/25 16:05:51	shopping	www.amazon.com/	192.168.2.10	72.21.215.232	US	web-browsing	alert	no	bsimpson

- **Block log**—In this log, the category alcohol-and-tobacco was set to block, so the action is block-url and the user will see a response page indicating that the website was blocked.

Receive Time	Category	URL	Source	Destination	Destin... Country	Application	Action	Decrypted	Source User
11/25 16:11:41	alcohol-and-tobacco	www.bevmo.com/	192.168.2.10	12.24.44.212	US	web-browsing	block-url	no	bsimpson

- **Alert log on encrypted website**—In this example, the category is social-networking and the application is facebook-base, which is required to access the Facebook website and other Facebook applications. Because faceboook.com is always encrypted using SSL, the traffic was decrypted by the firewall, which allows the website to be recognized and controlled if needed.

Receive Time	Category	URL	Source	Destination	Destin... Country	Application	Action	Decrypted	Source User
11/25 16:13:44	social-networking	www.facebook.com/	192.168.2.10	69.171.237.20	US	facebook-base	alert	yes	bsimpson

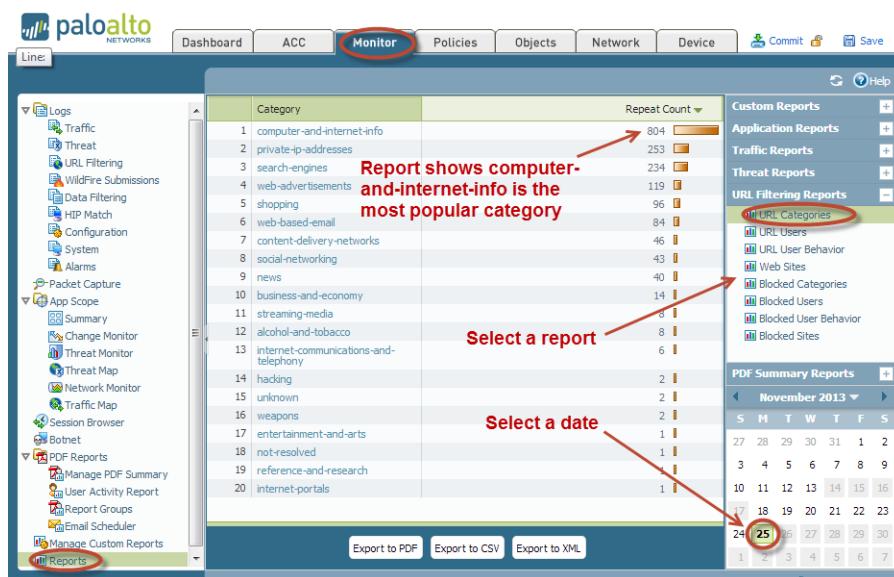
You can also add several other columns to your URL Filtering log view, such as: to and from zone, content type, and whether or not a packet capture was performed. To modify what columns to display, click the down arrow in any column and select the attribute to display.

The screenshot shows a table of logs with columns for Destin... Country, Application, Action, and Decrypted. A context menu is open over the 'Action' column, titled 'Columns'. The menu lists various log attributes with checkboxes: Receive Time (checked), Category (checked), Content Type (unchecked), URL (checked), From Zone (unchecked), To Zone (unchecked), Source (checked), Source Country (unchecked), NAT Source IP (unchecked), Destination (checked), Destination User (unchecked), Destination Country (checked), NAT Dest IP (unchecked), From Port (unchecked), NAT Source Port (unchecked), To Port (unchecked), and NAT Destination Port (unchecked). The 'Category' checkbox is checked and circled in red. The 'Columns' button at the bottom of the menu is also circled in red.

To view the complete log details and/or request a category change for the given URL that was accessed, click the log details icon in the first column of the log.

The screenshot shows the 'Log Details' page for session ID 35278. It includes sections for General, Source, Destination, URL Details, and Flags. In the URL Details section, the URL <http://www.facebook.com/> is listed with a 'Request Categorization Change' link, which is circled in red. The General section shows the session ID, action (alert), application (facebook-base), rule (Rule1), and various system details. The Source and Destination sections show network information. The Flags section includes checkboxes for Captive Portal, Proxy Transaction, Decrypted (checked), Packet Capture, Client to Server, and Server to Client.

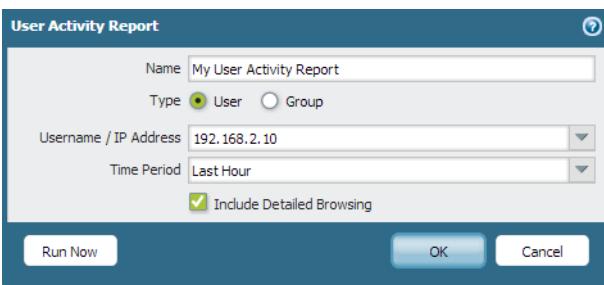
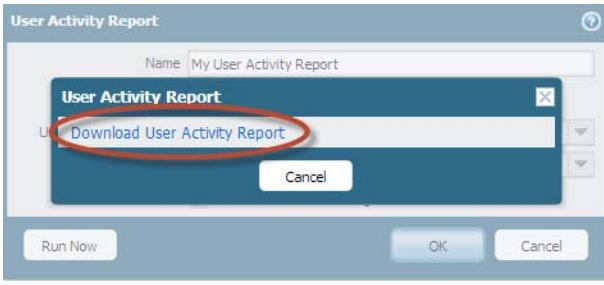
To generate a predefined URL filtering reports on URL categories, URL users, Websites accessed, Blocked categories, and more, select **Monitor > Reports** and under the **URL Filtering Reports** section, select one of the reports. The reports are based on a 24-hour period and the day is selected by choosing a day in the calendar section. You can also export the report to PDF, CSV, or XML.



## View the User Activity Report

This report provides a quick method of viewing user or group activity and also provides an option to view browse time activity.

### Generate a User Activity Report

<p><b>Step 1</b> Configure a User Activity Report</p>	<ol style="list-style-type: none"> <li>1. Select <b>Monitor &gt; PDF Reports &gt; User Activity Report</b>.</li> <li>2. Enter a report <b>Name</b> and select the report type. Select <b>User</b> to generate a report for one person, or select <b>Group</b> for a group of users.</li> </ol> <p> You must <b>Enable User-ID</b> in order to be able to select user or group names. If User-ID is not configured, you can select the type <b>User</b> and enter the IP address of the user's computer.</p> <ol style="list-style-type: none"> <li>3. Enter the Username/IP address for a user report or enter the group name for a user group report.</li> <li>4. Select the time period. You can select an existing time period, or select <b>Custom</b>.</li> <li>5. Select the <b>Include Detailed Browsing</b> check box, so browsing information is included in the report.</li> </ol> 
<p><b>Step 2</b> Run the user activity report and then download the report.</p>	<ol style="list-style-type: none"> <li>1. Click <b>Run Now</b>.</li> <li>2. After the report is generated, click the <b>Download User Activity Report</b> link.</li> </ol>  <ol style="list-style-type: none"> <li>3. After the report is downloaded, click <b>Cancel</b> and then click <b>OK</b> to save the report.</li> </ol>

**Generate a User Activity Report (Continued)**

- Step 3** View the user activity report by opening the PDF file that was downloaded. The top of the report will contain a table of contents similar to the following:

User Activity Report for 192.168.2.10  
Tuesday, December 31, 2013 09:35:47 - 10:35:46

<a href="#">Application Usage</a>	2
<a href="#">Traffic Summary by URL Category</a>	3
<a href="#">Browsing Summary by URL Category</a>	4
<a href="#">Browsing Summary by Website</a>	5
<a href="#">Blocked Browsing Summary by Website</a>	6
<a href="#">Detailed Web Browsing Activity</a>	7

- Step 4** Click an item in the table of contents to view details. For example, click *Traffic Summary by URL Category* to view statistics for the selected user or group.

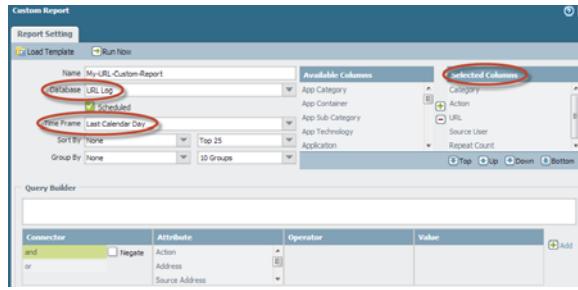
 **Traffic Summary by URL Category**

Category	Count	Bytes
web-advertisements	49	426.8k
business-and-economy	36	693.6k
computer-and-internet-info	35	224.7k
news	24	499.4k
content-delivery-networks	20	6.2M
private-ip-addresses	11	206.2k
search-engines	6	62.2k
web-based-email	2	26.0k
social-networking	1	685

## Configure Custom URL Filtering Reports

To generate a detailed report that can also be scheduled, you can configure a custom report and select from a list of all available URL filtering log fields.

### Configure a Custom URL Filtering Report

<b>Step 1</b> Add a new custom report.	<ol style="list-style-type: none"> <li>Select <b>Monitor &gt; Manage Custom Reports</b> and click <b>Add</b>.</li> <li>Enter a report <b>Name</b>, for example, My-URL-Custom-Report.</li> <li>From the <b>Database</b> drop-down, select <b>URL Log</b>.</li> </ol>
<b>Step 2</b> Configure report options.	<ol style="list-style-type: none"> <li>Select the <b>Time Frame</b> drop-down and select a range.</li> <li>(Optional) To customize how the report is sorted and grouped, select <b>Sort By</b> and chose the number of items to display (top 25 for example) and then select <b>Group By</b> and select an option such as <b>Category</b>, and then select how many groups will be defined.</li> <li>In the <b>Available Columns</b> list, select the fields to include the report. The following columns are typically used for a URL report:           <ul style="list-style-type: none"> <li>Action</li> <li>Category</li> <li>Destination Country</li> <li>Source User</li> <li>URL</li> </ul> </li> </ol> 
<b>Step 3</b> Run the report to check the results. If the results are satisfactory, set a schedule to run the report automatically.	<ol style="list-style-type: none"> <li>Click the <b>Run Now</b> icon to immediately generate the report that will appear in a new tab.</li> <li>(Optional) Click the <b>Schedule</b> check box to run the report once per day. This will generate a daily report that details web activity over the last 24 hours. To access the report, select <b>Monitor &gt; Report</b> and then expand <b>Custom Reports</b> on the right column and select the report.</li> </ol>
<b>Step 4</b> Save the configuration.	Click <b>Commit</b> .

## Configure URL Filtering

After you [Determine URL Filtering Policy Requirements](#), you should have a basic understanding of what types of websites and website categories your users are accessing. With this information, you are now ready to create custom URL filtering profiles and attach them to the security policy rule(s) that allow web access.

<b>Configure Website Controls</b>	
<b>Step 1</b> Create a URL Filtering profile or select an existing one.	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>. Select the default profile and then click <b>Clone</b>. The new profile will be named default-1.</li> <li>2. Select the new profile and rename it.</li> </ol> <p> Because the default URL filtering profile blocks risky and threat-prone content, it is a best practice to clone this profile rather than creating a new profile to preserve these default settings.</p>
<b>Step 2</b> Define how to control access to web content.	<p>In the <b>Categories</b> tab, for each category that you want visibility into or control over, select a value from the <b>Action</b> column as follows:</p> <ul style="list-style-type: none"> <li>• If you do not care about traffic to a particular category (that is you neither want to block it nor log it), select <b>allow</b>.</li> <li>• For visibility into traffic to sites in a category, select <b>alert</b>.</li> <li>• To deny access to traffic that matches the category and to enable logging of the blocked traffic, select <b>block</b>.</li> <li>• To require users to click <b>Continue</b> to proceed to a questionable site, select <b>continue</b>.</li> <li>• To only allow access if users provide a configured password, select <b>override</b>. For more details on this setting, see <a href="#">Configure URL Admin Override</a>.</li> </ul>
<b>Step 3</b> Define websites that should always be blocked or allowed.	<ol style="list-style-type: none"> <li>1. In the URL filtering profile, enter URLs or IP addresses in the <b>Block List</b> and select an action:               <ul style="list-style-type: none"> <li>• <b>block</b>—Block the URL.</li> <li>• <b>continue</b>—Prompt users click <b>Continue</b> to proceed to the web page.</li> <li>• <b>override</b>—The user will be prompted for a password to continue to the website.</li> <li>• <b>alert</b>—Allow the user to access the website and add an alert log entry in the URL log.</li> </ul> </li> <li>2. For the <b>Allow</b> list, enter IP addresses or URLs that should always be allowed. Each row must be separated by a new line.</li> <li>3. (Optional) <a href="#">Enable Safe Search Enforcement</a>.</li> </ol>

Configure Website Controls	
Step 4	Modify the setting to log Container Pages only.
Step 5	Enable <a href="#">HTTP Header Logging</a> for one or more of the supported HTTP header fields.
Step 6	Save the URL filtering profile.

The **Log container page only** option is enabled by default so that only the main page that matches the category is logged, not subsequent pages/categories that may be loaded within the container page. To enable logging for all pages/categories, clear the **Log container page only** check box.

To log an HTTP header field, select one or more of the following fields to log:

- **User-Agent**
- **Referer**
- **X-Forwarded-For**

1. Click **OK**.



Optionally, you can [Customize the URL Filtering Response Pages](#).

2. Click **Commit**.



To test the URL filtering configuration, simply access a website in a category that is set to block or continue to see if the appropriate action is performed.

## Customize the URL Filtering Response Pages

The firewall provides three predefined [URL Filtering Response Pages](#) that display by default when a user attempts to browse to a site in a category that is configured with one of the block actions in the [URL Filtering Profile](#) (block, continue, or override) or when [Safe Search Enforcement](#) blocks a search attempt. However, you can create your own custom response pages with your corporate branding, acceptable use policies, links to your internal resources as follows:

Customize the URL Filtering Response Pages	
Step 1 Export the default response page(s).	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Response Pages</b>.</li> <li>Select the link for the URL filtering response page you want to modify.</li> <li>Click the response page (predefined or shared) and then click the <b>Export</b> link and save the file to your desktop.</li> </ol>
Step 2 Edit the exported page.	<ol style="list-style-type: none"> <li>Using the HTML text editor of your choice, edit the page:           <ul style="list-style-type: none"> <li>If you want the response page to display custom information about the specific user, URL, or category that was blocked, add one or more of the supported <a href="#">URL Filtering Response Page Variables</a>.</li> <li>If you want to include custom images (such as your corporate logo), a sound, or style sheet, or link to another URL, for example to a document detailing your acceptable web use policy, include one or more of the supported <a href="#">Response Page References</a>.</li> </ul> </li> <li>Save the edited page with a new filename. Make sure that the page retains its UTF-8 encoding. For example, in Notepad you would select <b>UTF-8</b> from the <b>Encoding</b> drop-down in the Save As dialog.</li> </ol>
Step 3 Import the customized response page.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Response Pages</b>.</li> <li>Select the link that corresponds to the URL Filtering response page you edited.</li> <li>Click <b>Import</b> and then enter the path and filename in the <b>Import File</b> field or <b>Browse</b> to locate the file.</li> <li>(Optional) Select the virtual system on which this login page will be used from the <b>Destination</b> drop-down or select <b>shared</b> to make it available to all virtual systems.</li> <li>Click <b>OK</b> to import the file.</li> </ol>
Step 4 Save the new response page(s).	<b>Commit</b> the changes.
Step 5 Verify that the new response page displays.	From a browser, go to the URL that will trigger the response page. For example, to see a modified URL Filtering and Category Match response page, browse to URL that your URL filtering policy is set to block.

## Configure URL Admin Override

In some cases there may be URL categories that you want to block, but allow certain individuals to browse to on occasion. In this case, you would set the category action to **override** and define a URL admin override password in the firewall Content-ID configuration. When users attempt to browse to the category, they will be required to provide the override password before they are allowed access to the site. Use the following procedure to configure URL admin override:

### Configure URL Admin Override

<p><b>Step 1</b> Set the URL admin override password.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Content ID</b>.</li><li>2. In the <b>URL Admin Override</b> section, click <b>Add</b>.</li><li>3. In the <b>Location</b> field, select the virtual system to which this password applies.</li><li>4. Enter the <b>Password</b> and <b>Confirm Password</b>.</li><li>5. Select an <b>SSL/TLS Service Profile</b>. The profile specifies the certificate that the firewall presents to the user if the site with the override is an HTTPS site. For details, see <a href="#">Configure an SSL/TLS Service Profile</a>.</li><li>6. Select the <b>Mode</b> for prompting the user for the password:<ul style="list-style-type: none"><li>• <b>Transparent</b>—The firewall intercepts the browser traffic destined for site in a URL category you have set to override and impersonates the original destination URL, issuing an HTTP 401 to prompt for the password. Note that the client browser will display certificate errors if it does not trust the certificate.</li><li>• <b>Redirect</b>—The firewall intercepts HTTP or HTTPS traffic to a URL category set to override and redirects the request to a Layer 3 interface on the firewall using an HTTP 302 redirect in order to prompt for the override password. If you select this option, you must provide the <b>Address</b> (IP address or DNS hostname) to which to redirect the traffic.</li></ul></li><li>7. Click <b>OK</b>.</li></ol>
<p><b>Step 2</b> (Optional) Set a custom override period.</p>	<ol style="list-style-type: none"><li>1. Edit the URL Filtering section.</li><li>2. To change the amount of time users can browse to a site in a category for which they have successfully entered the override password, enter a new value in the <b>URL Admin Override Timeout</b> field. By default, users can access sites within the category for 15 minutes without re-entering the password.</li><li>3. To change the amount of time users are blocked from accessing a site set to override after three failed attempts to enter the override password, enter a new value in the <b>URL Admin Lockout Timeout</b> field. By default, users are blocked for 30 minutes.</li><li>4. Click <b>OK</b>.</li></ol>

<b>Configure URL Admin Override (Continued)</b>	
<b>Step 3</b> (Redirect mode only) Create a Layer 3 interface to which to redirect web requests to sites in a category configured for override.	<ol style="list-style-type: none"> <li>1. Create a management profile to enable the interface to display the URL Filtering Continue and Override Page response page:             <ol style="list-style-type: none"> <li>a. Select <b>Network &gt; Interface Mgmt</b> and click <b>Add</b>.</li> <li>b. Enter a <b>Name</b> for the profile, select <b>Response Pages</b>, and then click <b>OK</b>.</li> </ol> </li> <li>2. Create the Layer 3 interface. Be sure to attach the management profile you just created (on the <b>Advanced &gt; Other Info</b> tab of the Ethernet Interface dialog).</li> </ol>
<b>Step 4</b> (Redirect mode only) To transparently redirect users without displaying certificate errors, install a certificate that matches the IP address of the interface to which you are redirecting web requests to a site in a URL category configured for override. You can either generate a self-signed certificate or import a certificate that is signed by an external CA.	<p>To use a self-signed certificate, you must first create a root CA certificate and then use that CA to sign the certificate you will use for URL admin override as follows:</p> <ol style="list-style-type: none"> <li>1. To create a root CA certificate, select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and then click <b>Generate</b>. Enter a <b>Certificate Name</b>, such as RootCA. Do not select a value in the <b>Signed By</b> field (this is what indicates that it is self-signed). Make sure you select the <b>Certificate Authority</b> check box and then click <b>Generate</b> the certificate.</li> <li>2. To create the certificate to use for URL admin override, click <b>Generate</b>. Enter a <b>Certificate Name</b> and enter the DNS hostname or IP address of the interface as the <b>Common Name</b>. In the <b>Signed By</b> field, select the CA you created in the previous step. Add an IP address attribute and specify the IP address of the Layer 3 interface to which you will be redirecting web requests to URL categories that have the override action.</li> <li>3. <b>Generate</b> the certificate.</li> <li>4. To configure clients to trust the certificate, select the CA certificate on the <b>Device Certificates</b> tab and click <b>Export</b>. You must then import the certificate as a trusted root CA into all client browsers, either by manually configuring the browser or by adding the certificate to the trusted roots in an Active Directory Group Policy Object (GPO).</li> </ol>
<b>Step 5</b> Specify which URL categories require an override password to enable access.	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; URL Filtering</b> and either select an existing URL filtering profile or <b>Add</b> a new one.</li> <li>2. On the <b>Categories</b> tab, set the Action to <b>override</b> for each category that requires a password.</li> <li>3. Complete any remaining sections on the URL filtering profile and then click <b>OK</b> to save the profile.</li> </ol>
<b>Step 6</b> Apply the URL Filtering profile to the security policy rule(s) that allows access to the sites requiring password override for access.	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b> and select the appropriate security policy to modify it.</li> <li>2. Select the <b>Actions</b> tab and in the <b>Profile Setting</b> section, click the drop-down for <b>URL Filtering</b> and select the profile.</li> <li>3. Click <b>OK</b> to save.</li> </ol>
<b>Step 7</b> Save the configuration.	Click <b>Commit</b> .

## Enable Safe Search Enforcement

Many search engines have a safe search setting that filters out adult images and videos for search query return traffic. You can configure [Safe Search Enforcement](#) the Palo Alto Networks next-generation firewall to prevent search requests that do not have the strictest safe search settings enabled.



The [Safe Search Enforcement for Google and YouTube Searches using a Virtual IP Address](#) is not compatible with Safe Search Enforcement on the firewall.

There are two ways to enforce Safe Search on the firewall:

- ▲ [Block Search Results that are not Using Strict Safe Search Settings](#)
- ▲ [Enable Transparent Safe Search Enforcement](#)

### Block Search Results that are not Using Strict Safe Search Settings

By default, when you enable safe search enforcement, when a user attempts to perform a search without using the strictest safe search settings, the firewall will block the search query results and display the URL Filtering Safe Search Block Page. This page provides a link to the search settings page for the corresponding search provider so that the end user can enable the safe search settings. If you plan to use this default method for enforcing safe search, you should communicate the policy to your end users prior to deploying the policy. See [Table: Search Provider Safe Search Settings](#) for details on how each search provider implements safe search. The default URL Filtering Safe Search Block Page provides a link to the search settings for the corresponding search provider. You can optionally [Customize the URL Filtering Response Pages](#).

Alternatively, to enable safe search enforcement so that it is transparent to your end users, configure the firewall to [Enable Transparent Safe Search Enforcement](#).

<b>Enable Safe Search Enforcement</b>	
<b>Step 1</b> Enable Safe Search Enforcement in the URL Filtering profile.	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li> <li>2. Select an existing profile to modify, or clone the default profile to create a new profile.</li> <li>3. On the <b>Settings</b> tab, select the <b>Safe Search Enforcement</b> check box to enable it.</li> <li>4. (Optional) Restrict users to specific search engines:             <ol style="list-style-type: none"> <li>a. On the <b>Categories</b> tab, set the <b>search-engines</b> category to <b>block</b>.</li> <li>b. For each search engine that you want end users to be able to access, enter the web address in the <b>Allow List</b> text box. For example, to allow users access to Google and Bing searches only, you would enter the following:  <code>www.google.com</code>  <code>www.bing.com</code> </li> </ol> </li> <li>5. Configure other settings as necessary to:             <ul style="list-style-type: none"> <li>• Define how to control access to web content.</li> <li>• Define websites that should always be blocked or allowed.</li> </ul> </li> <li>6. Click <b>OK</b> to save the profile.</li> </ol>
<b>Step 2</b> Add the URL Filtering profile to the security policy rule that allows traffic from clients in the trust zone to the Internet.	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b> and select a rule to which to apply the URL filtering profile that you just enabled for Safe Search Enforcement.</li> <li>2. On the <b>Actions</b> tab, select the <b>URL Filtering</b> profile.</li> <li>3. Click <b>OK</b> to save the security policy rule.</li> </ol>
<b>Step 3</b> Enable SSL Forward Proxy decryption.  Because most search engines encrypt their search results, you must enable SSL forward proxy decryption so that the firewall can inspect the search traffic and detect the safe search settings.	<ol style="list-style-type: none"> <li>1. Add a custom URL category for the search sites:             <ol style="list-style-type: none"> <li>a. Select <b>Objects &gt; Custom Objects &gt; URL Category</b> and <b>Add</b> a custom category.</li> <li>b. Enter a <b>Name</b> for the category, such as <code>SearchEngineDecryption</code>.</li> <li>c. <b>Add</b> the following to the Sites list:  <code>www.bing.*</code>  <code>www.google.*</code>  <code>search.yahoo.*</code> </li> <li>d. Click <b>OK</b> to save the custom URL category object.</li> </ol> </li> <li>2. Follow the steps to <a href="#">Configure SSL Forward Proxy</a>.</li> <li>3. On the <b>Service/URL Category</b> tab in the Decryption policy rule, <b>Add</b> the custom URL category you just created and then click <b>OK</b>.</li> </ol>

**Enable Safe Search Enforcement (Continued)**

<p><b>Step 4</b> (Optional, but recommended) Block Bing search traffic running over SSL.</p> <p>Because the Bing SSL search engine does not adhere to the safe search settings, for full safe search enforcement, you must deny all Bing sessions that run over SSL.</p>	<ol style="list-style-type: none"><li>1. Add a custom URL category for Bing:<ol style="list-style-type: none"><li>a. Select <b>Objects &gt; Custom Objects &gt; URL Category</b> and <b>Add</b> a custom category.</li><li>b. Enter a <b>Name</b> for the category, such as EnableBingSafeSearch.</li><li>c. <b>Add</b> the following to the Sites list: <code>www.bing.com/images/*</code> <code>www.bing.com/videos/*</code></li><li>d. Click <b>OK</b> to save the custom URL category object.</li></ol></li><li>2. Create another URL filtering profile to block the custom category you just created:<ol style="list-style-type: none"><li>a. Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li><li>b. <b>Add</b> a new profile and give it a descriptive <b>Name</b>.</li><li>c. Locate the custom category in the Category list and set it to <b>block</b>.</li><li>d. Click <b>OK</b> to save the URL filtering profile.</li></ol></li><li>3. Add a security policy rule to block Bing SSL traffic:<ol style="list-style-type: none"><li>a. Select <b>Policies &gt; Security</b> and <b>Add</b> a policy rule that allows traffic from your trust zone to the Internet.</li><li>b. On the <b>Actions</b> tab, attach the URL filtering profile you just created to block the custom Bing category.</li><li>c. On the <b>Service/URL Category</b> tab <b>Add a New Service</b> and give it a descriptive <b>Name</b>, such as bingssl.</li><li>d. Select <b>TCP</b> as the <b>Protocol</b> and set the <b>Destination Port</b> to <b>443</b>.</li><li>e. Click <b>OK</b> to save the rule.</li><li>f. Use the <b>Move</b> options to ensure that this rule is below the rule that has the URL filtering profile with safe search enforcement enabled.</li></ol></li></ol>
<p><b>Step 5</b> Save the configuration.</p>	<p>Click <b>Commit</b>.</p>

**Enable Safe Search Enforcement (Continued)**

- Step 6** Verify the Safe Search Enforcement configuration.



This verification step only works if you are using block pages to enforce safe search. If you are using transparent safe search enforcement, the firewall block page will invoke a URL rewrite with the safe search parameters in the query string.

- From a computer that is behind the firewall, disable the strict search settings for one of the supported search providers. For example, on bing.com, click the **Preferences** icon on the Bing menu bar.



- Set the **SafeSearch** option to **Moderate** or **Off** and click **Save**.
- Perform a Bing search and verify that the URL Filtering Safe Search Block page displays instead of the search results:

**Search Blocked**

User: 192.168.2.10

Your search results have been blocked because your search settings are not in accordance with company policy. In order to continue, please update your search settings so that Safe Search is set to the strictest setting, and try your search again.

For more information, please refer to: <http://www.bing.com/account/general>

Please contact your system administrator if you believe this message is in error.

- Use the link in the block page to go to the search settings for the search provider and set the safe search setting back to the strictest setting (**Strict** in the case of Bing) and then click **Save**.
- Perform a search again from Bing and verify that the filtered search results display instead of the block page.

## Enable Transparent Safe Search Enforcement

If you want to enforce filtering of search query results with the strictest safe search filters, but you don't want your end users to have to manually configure the settings, you can enable transparent safe search enforcement as follows. This functionality is supported on Google, Yahoo, and Bing search engines only and requires Content Release version 475 or later.

<b>Enable Transparent Safe Search Enforcement</b>	
<b>Step 1</b>	<p>Make sure the firewall is running Content Release version 475 or later.</p> <ol style="list-style-type: none"> <li>Select <b>Device &gt; Dynamic Updates</b>.</li> <li>Check the <b>Applications and Threats</b> section to determine what update is currently running.</li> <li>If the firewall is not running the required update or later, click <b>Check Now</b> to retrieve a list of available updates.</li> <li>Locate the required update and click <b>Download</b>.</li> <li>After the download completes, click <b>Install</b>.</li> </ol>
<b>Step 1</b>	<p>Enable Safe Search Enforcement in the URL Filtering profile.</p> <ol style="list-style-type: none"> <li>Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li> <li>Select an existing profile to modify, or clone the default profile to create a new one.</li> <li>On the <b>Settings</b> tab, select the <b>Safe Search Enforcement</b> check box to enable it.</li> <li>(Optional) Allow access to specific search engines only:             <ol style="list-style-type: none"> <li>On the <b>Categories</b> tab, set the <b>search-engines</b> category to <b>block</b>.</li> <li>For each search engine that you want end users to be able to access, enter the web address in the <b>Allow List</b> text box. For example, to allow users access to Google and Bing searches only, you would enter the following:  <b>www.google.com</b>  <b>www.bing.com</b> </li> </ol> </li> <li>Configure other settings as necessary to:             <ul style="list-style-type: none"> <li><a href="#">Define how to control access to web content</a>.</li> <li><a href="#">Define websites that should always be blocked or allowed</a>.</li> </ul> </li> <li>Click <b>OK</b> to save the profile.</li> </ol>
<b>Step 2</b>	<p>Add the URL Filtering profile to the security policy rule that allows traffic from clients in the trust zone to the Internet.</p> <ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and select a rule to which to apply the URL filtering profile that you just enabled for Safe Search Enforcement.</li> <li>On the <b>Actions</b> tab, select the <b>URL Filtering</b> profile.</li> <li>Click <b>OK</b> to save the security policy rule.</li> </ol>

### Enable Transparent Safe Search Enforcement (Continued)

<p><b>Step 3</b> (Optional, but recommended) Block Bing search traffic running over SSL.</p> <p>Because the Bing SSL search engine does not adhere to the safe search settings, for full safe search enforcement, you must deny all Bing sessions that run over SSL.</p>	<ol style="list-style-type: none"> <li>1. Add a custom URL category for Bing:             <ol style="list-style-type: none"> <li>a. Select <b>Objects &gt; Custom Objects &gt; URL Category</b> and <b>Add</b> a custom category.</li> <li>b. Enter a <b>Name</b> for the category, such as <code>EnableBingSafeSearch</code>.</li> <li>c. <b>Add</b> the following to the Sites list:                 <pre>www.bing.com/images/* www.bing.com/videos/*</pre> </li> <li>d. Click <b>OK</b> to save the custom URL category object.</li> </ol> </li> <li>2. Create another URL filtering profile to block the custom category you just created:             <ol style="list-style-type: none"> <li>a. Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li> <li>b. <b>Add</b> a new profile and give it a descriptive <b>Name</b>.</li> <li>c. Locate the custom category you just created in the Category list and set it to <b>block</b>.</li> <li>d. Click <b>OK</b> to save the URL filtering profile.</li> </ol> </li> <li>3. <b>Add</b> a security policy rule to block Bing SSL traffic:             <ol style="list-style-type: none"> <li>a. Select <b>Policies &gt; Security</b> and <b>Add</b> a policy rule that allows traffic from your trust zone to the Internet.</li> <li>b. On the <b>Actions</b> tab, attach the URL filtering profile you just created to block the custom Bing category.</li> <li>c. On the <b>Service/URL Category</b> tab <b>Add a New Service</b> and give it a descriptive <b>Name</b>, such as <code>bingssl</code>.</li> <li>d. Select <b>TCP</b> as the <b>Protocol</b>, set the <b>Destination Port</b> to <code>443</code>.</li> <li>e. Click <b>OK</b> to save the rule.</li> <li>f. Use the <b>Move</b> options to ensure that this rule is below the rule that has the URL filtering profile with safe search enforcement enabled.</li> </ol> </li> </ol>
<p><b>Step 4</b> Edit the URL Filtering Safe Search Block Page, replacing the existing code with the Javascript for rewriting search query URLs to enforce safe search transparently.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Response Pages &gt; URL Filtering Safe Search Block Page</b>.</li> <li>2. Select <b>Predefined</b> and then click <b>Export</b> to save the file locally.</li> <li>3. Use an HTML editor and replace all of the existing block page text with this <b>script</b>.</li> </ol> <div style="display: flex; align-items: center;">  Copy the script and paste it into the HTML editor, replacing the entire block page.         </div>

### Enable Transparent Safe Search Enforcement (Continued)

<p><b>Step 5</b> Import the edited URL Filtering Safe Search Block page onto the firewall.</p>	<ol style="list-style-type: none"> <li>1. To import the edited block page, select <b>Device &gt; Response Pages &gt; URL Filtering Safe Search Block Page</b>.</li> <li>2. Click <b>Import</b> and then enter the path and filename in the <b>Import File</b> field or <b>Browse</b> to locate the file.</li> <li>3. (Optional) Select the virtual system on which this login page will be used from the <b>Destination</b> drop-down or select <b>shared</b> to make it available to all virtual systems.</li> <li>4. Click <b>OK</b> to import the file.</li> </ol>
<p><b>Step 6</b> Enable SSL Forward Proxy decryption.</p> <p>Because most search engines encrypt their search results, you must enable SSL forward proxy decryption so that the firewall can inspect the search traffic and detect the safe search settings.</p>	<ol style="list-style-type: none"> <li>1. Add a custom URL category for the search sites:             <ol style="list-style-type: none"> <li>a. Select <b>Objects &gt; Custom Objects &gt; URL Category</b> and <b>Add</b> a custom category.</li> <li>b. Enter a <b>Name</b> for the category, such as <code>SearchEngineDecryption</code>.</li> <li>c. <b>Add</b> the following to the Sites list:                     <pre>www.bing.* www.google.* search.yahoo.*</pre> </li> <li>d. Click <b>OK</b> to save the custom URL category object.</li> </ol> </li> <li>2. Follow the steps to <a href="#">Configure SSL Forward Proxy</a>.</li> <li>3. On the <b>Service/URL Category</b> tab in the Decryption policy rule, <b>Add</b> the custom URL category you just created and then click <b>OK</b>.</li> </ol>
<p><b>Step 7</b> Save the configuration.</p>	Click <b>Commit</b> .

## Set Up the PAN-DB Private Cloud

Complete the following tasks to deploy one or more M-500 appliances as a PAN-DB private cloud within your network or data center:

- ▲ [Set Up a PAN-DB Private Cloud](#)
- ▲ [Configure the Firewalls to Access the PAN-DB Private Cloud](#)

## Set Up a PAN-DB Private Cloud

Set up the PAN-DB Private Cloud	
Step 1	Rack mount the M-500 appliance.
Step 2	Register the M-500 appliance.
Step 3	<p>Perform Initial Configuration of the M-500 Appliance.</p>  <p>The M-500 appliance in PAN-DB mode uses two ports- MGT (Eth0) and Eth1; Eth2 is not used in PAN-DB mode. The management port is used for administrative access to the appliance and for obtaining the latest content updates from the PAN-DB public cloud. For communication between the appliance (PAN-DB server) and the firewalls on the network, you can use the MGT port or Eth1.</p> <p><b>1.</b> Connect to the M-500 appliance in one of the following ways:</p> <ul style="list-style-type: none"> <li>Attach a serial cable from a computer to the Console port on the M-500 appliance and connect using a terminal emulation software (9600-8-N-1).</li> <li>Attach an RJ-45 Ethernet cable from a computer to the MGT port on the M-500 appliance. From a browser, go to <a href="https://192.168.1.1">https://192.168.1.1</a>. Enabling access to this URL might require changing the IP address on the computer to an address in the 192.168.1.0 network (for example, 192.168.1.2).</li> </ul> <p><b>2.</b> When prompted, log in to the appliance. Log in using the default username and password (admin/admin). The appliance will begin to initialize.</p> <p><b>3.</b> Configure an network access settings including the IP address for the MGT interface:</p> <pre>set deviceconfig system ip-address &lt;server-IP&gt; netmask &lt;netmask&gt; default-gateway &lt;gateway-IP&gt; dns-setting servers primary &lt;DNS-IP&gt;</pre> <p>where &lt;server-IP&gt; is the IP address you want to assign to the management interface of the server, &lt;netmask&gt; is the subnet mask, &lt;gateway-IP&gt; is the IP address of the network gateway, and &lt;DNS-IP&gt; is the IP address of the primary DNS server.</p> <p><b>4.</b> Configure an network access settings including the IP address for the Eth1 interface:</p> <pre>set deviceconfig system eth1 ip-address &lt;server-IP&gt; netmask &lt;netmask&gt; default-gateway &lt;gateway-IP&gt; dns-setting servers primary &lt;DNS-IP&gt;</pre> <p>where &lt;server-IP&gt; is the IP address you want to assign to the data interface of the server, &lt;netmask&gt; is the subnet mask, &lt;gateway-IP&gt; is the IP address of the network gateway, and &lt;DNS-IP&gt; is the IP address of the DNS server.</p> <p><b>5.</b> Save your changes to the PAN-DB server.</p> <pre>commit</pre>

**Set up the PAN-DB Private Cloud (Continued)**

**Step 4** Switch to PAN-DB private cloud mode.

1. To switch to PAN-DB mode, use the CLI command:

```
request system system-mode pan-url-db
```



You can switch from Panorama mode to PAN-DB mode and back; and from [Panorama mode to Log Collector mode](#) and back. Switching directly from PAN-DB mode to Log Collector mode or vice versa is not supported. When switching operational mode, a data reset is triggered. With the exception of management access settings, all existing configuration and logs will be deleted on restart.

2. Use the following command to verify that the mode is changed:

```
show pan-url-cloud-status
```

```
hostname: M-500
ip-address: 1.2.3.4
netmask: 255.255.255.0
default-gateway: 1.2.3.1
ipv6-address: unknown
ipv6-link-local-address: fe80:00/64
ipv6-default-gateway:
mac-address: 00:56:90:e7:f6:8e
time: Mon Apr 27 13:43:59 2015
uptime: 10 days, 1:51:28
family: m
model: M-500
serial: 0073010000xxx
sw-version: 7.0.0
app-version: 492-2638
app-release-date: 2015/03/19 20:05:33
av-version: 0
av-release-date: unknown
wf-private-version: 0
wf-private-release-date: unknown
logdb-version: 7.0.9
platform-family: m
pan-url-db: 20150417-220
system-mode: Pan-URL-DB
operational-mode: normal
```

3. Use the following command to check the version of the cloud database on the M-500 appliance:

```
show pan-url-cloud-status
```

```
Cloud status: Up
URL database version: 20150417-220
```

**Set up the PAN-DB Private Cloud (Continued)**

<b>Step 5</b>	Install content and database updates.	Pick one of the following methods of installing the content and database updates: <ul style="list-style-type: none"><li>• If the PAN-DB server has direct Internet access use the following commands:<ol style="list-style-type: none"><li>a. To check whether a new version is published use: <code>request pan-url-db upgrade check</code></li><li>b. To check the version that is currently installed on your server use: <code>request pan-url-db upgrade info</code></li><li>c. To download and install the latest version: <code>- request pan-url-db upgrade download latest</code> <code>- request pan-url-db upgrade install &lt;version latest   file&gt;</code></li><li>d. To schedule the M-500 appliance to automatically check for updates: <code>set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week &lt;day of week&gt; at &lt;hr:min&gt;</code></li></ol></li><li>• If the PAN-DB server is offline, access the Palo Alto Networks Support portal to download and save the content updates to an SCP server on your network. You can then import and install the updates using the following commands:<ul style="list-style-type: none"><li>• <code>scp import pan-url-db remote-port &lt;port-number&gt; from username@host:path</code></li><li>• <code>request pan-url-db upgrade install file &lt;filename&gt;</code></li></ul></li></ul>
---------------	---------------------------------------	---

### Set up the PAN-DB Private Cloud (Continued)

- Step 6** Set up administrative access to the PAN-DB private cloud.



The appliance has a default admin account. Any additional administrative users that you create can either be superusers (with full access) or superusers with read-only access.

PAN-DB private cloud does not support the use of RADIUS VSAs. If the VSAs used on the firewall or Panorama are used for enabling access to the PAN-DB private cloud, an authentication failure will occur.

- To set up a local administrative user on the PAN-DB server:

- configure**
- set mgt-config users <username> permissions role-based <superreader | superuser> yes**
- set mgt-config users <username> password**

Enter password:**xxxxx**

Confirm password:**xxxxx**

- commit**

- To set up an administrative user with RADIUS authentication:

- Create RADIUS server profile.

```
set shared server-profile radius
<server_profile_name> server <server_name>
ip-address <ip_address> port <port_no> secret
<shared_password>
```

- Create authentication-profile.

```
set shared authentication-profile
<auth_profile_name> user-domain
<domain_name_for_authentication> allow-list <all>
method radius server-profile <server_profile_name>
```

- Attach the authentication-profile to the user.

```
set mgt-config users <username>
authentication-profile <auth_profile_name>
```

- Commit the changes.

```
commit
```

- To view the list of users:

```
show mgt-config users
users {
    admin {
        phash fnRL/G5lXVMug;
        permissions {
            role-based {
                superuser yes;
            }
        }
    }
    admin_user_2 {
        permissions {
            role-based {
                superreader yes;
            }
        }
    }
}
authentication-profile RADIUS;
```

- Step 7** Configure the Firewalls to Access the PAN-DB Private Cloud.

## Configure the Firewalls to Access the PAN-DB Private Cloud

When using the PAN-DB public cloud, each firewall accesses the PAN-DB servers in the AWS cloud to download the list of eligible servers to which it can connect for URL lookups. With the PAN-DB private cloud, you must configure the firewalls with a (static) list of your PAN-DB private cloud servers that will be used for URL lookups. The list can contain up to 20 entries; IPv4 addresses, IPv6 addresses, and FQDNs are supported. Each entry on the list—IP address or FQDN—must be assigned to the management port and/or eth1 of the PAN-DB server.

### Configure the Firewalls to Access the PAN-DB Private Cloud.

**Step 1** Pick one of the following options based on the PAN-OS version on the firewall.

- a. For firewalls running PAN-OS 7.0, [Access the PAN-OS CLI](#) or the web interface on the firewall.
  - Use the following CLI command to configure access to the private cloud:  
`set deviceconfig setting pan-url-db cloud-static-list <IP addresses> enable`
  - Or, in the web interface for each firewall,
    1. Select **Device > Setup >Content-ID**, edit the URL Filtering section.
    2. Enter the **PAN-DB Server** IP address(es) or FQDN(s). The list must be comma separated.
- b. For firewalls running PAN-OS 5.0, 6.0, or 6.1, use the following CLI command to configure access to the private cloud:

```
debug device-server pan-url-db cloud-static-list-enable <IP addresses> enable
```



To delete the entries for the private PAN-DB servers, and allow the firewalls to connect to the PAN-DB public cloud, use the command:

```
set deviceconfig setting pan-url-db cloud-static-list <IP addresses> disable
```

When you delete the list of private PAN-DB servers, a re-election process is triggered on the firewall. The firewall first checks for the list of PAN-DB private cloud servers and when it cannot find one, the firewall accesses the PAN-DB servers in the AWS cloud to download the list of eligible servers to which it can connect.

**Step 2** **Commit** your changes.

**Step 3** To verify that the change is effective, use the following CLI command on the firewall:

- `show url-cloud status`  
Cloud status: Up  
URL database version: 20150417-220

## URL Filtering Use Case Examples

The following use cases show how to use App-ID to control a specific set of web-based applications and how to use URL categories as match criteria in a policy. When working with App-ID, it is important to understand that each App-ID signature may have dependencies that are required to fully control an application. For example, with Facebook applications, the App-ID facebook-base is required to access the Facebook website and to control other Facebook applications. For example, to configure the firewall to control Facebook email, you would have to allow the App-IDs facebook-base and facebook-mail. As another example, if you search [Applipedia](#) (the App-ID database) for LinkedIn, you will see that in order to control LinkedIn mail, you need to apply the same action to both App-IDs: linkedin-base and linkedin-mail. To determine application dependencies for App-ID signatures, visit [Applipedia](#), search for the given application, and then click the application for details.



The [User-ID](#) feature is required to implement policies based on users and groups and a [Decryption](#) policy is required to identify and control websites that are encrypted using SSL/TLS.

This section includes two uses cases:

- ▲ [Use Case: Control Web Access](#)
- ▲ [Use Case: Use URL Categories for Policy Matching](#)

## Use Case: Control Web Access

When using URL filtering to control user website access, there may be instances where granular control is required for a given website. In this use case, a URL filtering profile is applied to the security policy that allows web access for your users and the *social-networking* URL category is set to block, but the allow list in the URL profile is configured to allow the social networking site Facebook. To further control Facebook, the company policy also states that only marketing has full access to Facebook and all other users within the company can only read Facebook posts and cannot use any other Facebook applications, such as email, posting, chat, and file sharing. To accomplish this requirement, App-ID must be used to provide granular control over Facebook.

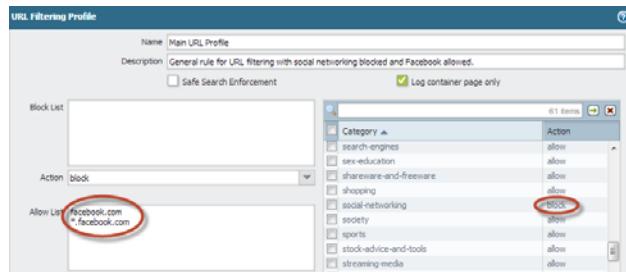
The first security rule will allow marketing to access the Facebook website as well as all Facebook applications. Because this allow rule will also allow access to the Internet, threat prevention profiles are applied to the rule, so traffic that matches the policy will be scanned for threats. This is important because the allow rule is terminal and will not continue to check other rules if there is a traffic match.

Control Web Access	
Step 1	Confirm that URL filtering is licensed.  1. Select <b>Device &gt; Licenses</b> and confirm that a valid date appears for the URL filtering database that will be used. This will either be PAN-DB or BrightCloud.  2. If a valid license is not installed, see <a href="#">Enable PAN-DB URL Filtering</a> .
Step 2	Confirm that User-ID is working. User-ID is required to create policies based on users and groups.  1. To check <b>Group Mapping</b> from the CLI, enter the following command:  <code>show user group-mapping statistics</code> 2. To check <b>User Mapping</b> from the CLI, enter the following command:  <code>show user ip-user-mapping-mp all</code> 3. If statistics do not appear and/or IP address to user mapping information is not displayed, see <a href="#">User-ID</a> .
Step 3	Set up a URL filtering profile by cloning the default profile.  1. Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b> and select the <b>default</b> profile. 2. Click the <b>Clone</b> icon. A new profile should appear named <b>default-1</b> . 3. Select the new profile and rename it.

### Control Web Access (Continued)

**Step 4** Configure the URL filtering profile to block social-networking and allow Facebook.

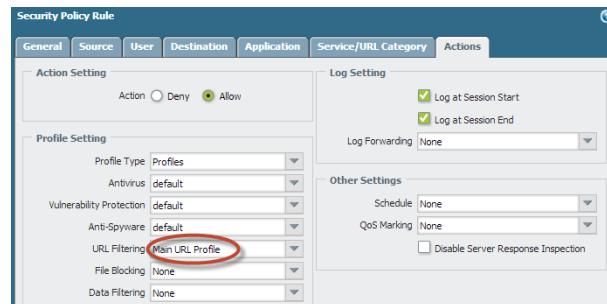
1. Modify the new URL filtering profile and in the **Category** list scroll to **social-networking** and in the **Action** column click on **allow** and change the action to **block**.
2. In the **Allow List**, enter `facebook.com`, press enter to start a new line and then type `*.facebook.com`. Both of these formats are required, so all URL variants a user may use will be identified, such as `facebook.com`, `www.facebook.com`, and `https://facebook.com`.



3. Click **OK** to save the profile.

**Step 5** Apply the new URL filtering profile to the security policy rule that allows web access from the user network to the Internet.

1. Select **Policies > Security** and click on the policy rule that allows web access.
2. On the **Actions** tab, select the URL profile you just created from the **URL Filtering** drop-down.



3. Click **OK** to save.

### Control Web Access (Continued)

**Step 6** Create the security policy rule that will allow marketing access the Facebook website and all Facebook applications.

This rule must precede other rules because:

- It is a specific rule. More specific rules must precede other rules.
- Allow rule will terminate when a traffic match occurs.

1. Select **Policies > Security** and click **Add**.
2. Enter a **Name** and optionally a **Description** and **Tag(s)**.
3. On the **Source** tab add the zone where the users are connected.
4. On the **User** tab in the **Source User** section click **Add**.
5. Select the directory group that contains your *marketing* users.
6. On the **Destination** tab, select the zone that is connected to the Internet.
7. On the **Applications** tab, click **Add** and add the *facebook* App-ID signature.
8. On the **Actions** tab, add the default profiles for **Antivirus**, **Vulnerability Protection**, and **Anti-Spyware**.

Name	Zone	Source		Destination		Service	Action	Profile
		Address	User	Zone	Address			
Marketing Facebook Allow	p2;1-vlan-trust	any	Marketing	any	p2;1-untrust	any	facebook	

9. Click **OK** to save the security profile.

The *facebook* App-ID signature used in this policy rule encompasses all Facebook applications, such as *facebook-base*, *facebook-chat*, and *facebook-mail*, so this is the only App-ID signature required in this rule.

With this rule in place, when a marketing employee attempts to access the Facebook website or any Facebook application, the rule matches based on the user being part of the marketing group. For traffic from any user outside of marketing, the rule will be skipped because there would not be a traffic match and rule processing would continue.

### Control Web Access (Continued)

**Step 7** Configure the security policy to block all other users from using any Facebook applications other than simple web browsing. The easiest way to do this is to clone the marketing allow policy and then modify it.

1. From **Policies > Security** click the marketing Facebook allow policy you created earlier to highlight it and then click the **Clone** icon.
2. Enter a **Name** and optionally enter a **Description** and **Tag(s)**.
3. On the **User** tab highlight the marketing group and delete it and in the drop-down select **any**.
4. On the **Applications** tab, click the *facebook* App-ID signature and delete it.
5. Click **Add** and add the following App-ID signatures:
  - facebook-apps
  - facebook-chat
  - facebook-file-sharing
  - facebook-mail
  - facebook-posting
  - facebook-social-plugin
6. On the **Actions** tab in the **Action Setting** section, select **Deny**. The profile settings should already be correct because this rule was cloned.



7. Click **OK** to save the security profile.
8. Ensure that this new deny rule is listed after the marketing allow rule, to ensure that rule processing occurs in the correct order to allow marketing users and then to deny/limit all other users.
9. Click **Commit** to save the configuration.

With these security policy rules in place, any user who is part of the marketing group will have full access to all Facebook applications and any user that is not part of the marketing group will only have read-only access to the Facebook website and will not be able to use Facebook applications such as post, chat, email, and file sharing.

## Use Case: Use URL Categories for Policy Matching

URL categories can also be used as match criteria in the following policy types: Captive Portal, Decryption, Security, and QoS. In this use case, URL categories will be used in Decryption policy rules to control which web categories should be decrypted or not decrypted. The first rule is a no-decrypt rule that will not decrypt user traffic if the website category is *financial-services* or *health-and-medicine* and the second rule will decrypt all other traffic. The decryption policy type is *ssl-forward-proxy*, which is used for controlling decryption for all outbound connections performed by users.

### Configure a Decryption Policy Based on URL Category

- |   |   |
|---|---|
| <b>Step 1</b> Create the no-decrypt rule that will be listed first in the decryption policies list. This will prevent any website that is in the <i>financial-services</i> or <i>health-and-medicine</i> URL categories from being decrypted. | <ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Decryption</b> and click <b>Add</b>.</li> <li>2. Enter a <b>Name</b> and optionally enter a <b>Description</b> and <b>Tag(s)</b>.</li> <li>3. On the <b>Source</b> tab, add the zone where the users are connected.</li> <li>4. On the <b>Destination</b> tab, enter the zone that is connected to the Internet.</li> <li>5. On the <b>URL Category</b> tab, click <b>Add</b> and select the <i>financial-services</i> and <i>health-and-medicine</i> URL categories.</li> <li>6. On the <b>Options</b> tab, set the action to <b>No Decrypt</b>.</li> <li>7. (Optional) Although the firewall does not decrypt and inspect the traffic for the session, you can attach a <b>Decryption profile</b> if you want to enforce the server certificates used during the session. The decryption profile allows you to configure the firewall to terminate the SSL connection either when the server certificates are expired or when the server certificates are issued by an untrusted issuer.</li> </ol> |
|---|---|

Name	Tags	Zone	Address	User	Zone	Address	URL Category	Action	Type
2 No-Decrypt-Finance-Health	No-Decrypt	13-vlan-trust	any	any	13-untrust	any	financial-services health-and-medicine	no-decrypt	ssl-forward-proxy

8. Click **OK** to save the policy rule.

### Configure a Decryption Policy Based on URL Category (Continued)

**Step 2** Create the decryption policy rule that will decrypt all other traffic.

1. Select the no-decrypt policy you created previously and then click **Clone**.
2. Enter a **Name** and optionally enter a **Description** and **Tag(s)**.
3. On the **URL Category** tab, select *financial-services* and *health-and-medicine* and then click the **Delete** icon.
4. On the **Options** tab, set the action to **Decrypt** and the **Type** to **SSL Forward Proxy**.
5. (Optional) Attach a **Decryption profile** to specify the server



certificate verification, unsupported mode checks and failure checks for the SSL traffic. See [Configure SSL Forward Proxy](#) for more details.

6. Ensure that this new decryption rule is listed after the no-decrypt rule to ensure that rule processing occurs in the correct order, so websites in the *financial-services* and *health-and-medicine* are not decrypted
7. Click **OK** to save the policy rule.

**Step 3** (BrightCloud only) Enable cloud lookups for dynamically categorizing a URL when the category is not available on the local database on the firewall.

1. Access the CLI on the firewall.
2. Enter the following commands to enable Dynamic URL Filtering:
  - a. **configure**
  - b. **set deviceconfig setting url dynamic-url yes**
  - c. **commit**

**Step 4** Save the configuration.

Click **Commit**.

With these two decrypt policies in place, any traffic destined for the *financial-services* or *health-and-medicine* URL categories will not be decrypted. All other traffic will be decrypted.

Now that you have a basic understanding of the powerful features of URL filtering, App-ID, and User-ID, you can apply similar policies to your firewall to control any application in the Palo Alto Networks App-ID signature database and control any website contained in the URL filtering database.

For help in troubleshooting URL filtering issues, see [Troubleshoot URL Filtering](#).

# Troubleshoot URL Filtering

The following topics provide troubleshooting guidelines for diagnosing and resolving common URL filtering problems.

- ▲ [Problems Activating PAN-DB](#)
- ▲ [PAN-DB Cloud Connectivity Issues](#)
- ▲ [URLs Classified as Not-Resolved](#)
- ▲ [Incorrect Categorization](#)
- ▲ [URL Database Out of Date](#)

## Problems Activating PAN-DB

The following table describes procedures that you can use to resolve issues with activating PAN-DB.

Troubleshoot PAN-DB Activation Issues
<p>1. <a href="#">Access the PAN-OS CLI.</a></p>
<p>2. Verify whether PAN-DB has been activated by running the following command: <code>admin@PA-200&gt; show system setting url-database</code> If the response is <code>paloaltonetworks</code>, then PAN-DB is the active vendor.</p>
<p>3. Verify that the firewall has a valid PAN-DB license by running the following command: <code>admin@PA-200&gt; request license info</code> You should see the license entry Feature: PAN_DB URL Filtering. If the license is not installed, you will need to obtain and install a license. See <a href="#">Configure URL Filtering</a>.</p>
<p>4. After the license is installed, download a new PAN-DB seed database by running the following command: <code>admin@PA-200&gt; request url-filtering download paloaltonetworks region &lt;region&gt;</code></p>
<p>5. Check the download status by running the following command: <code>admin@PA-200&gt; request url-filtering download status vendor paloaltonetworks</code><ul style="list-style-type: none"><li>• If the message is different from <code>PAN-DB download: Finished successfully</code>, stop here; there may be a problem connecting to the cloud. Attempt to solve the connectivity issue by performing basic network troubleshooting between the firewall and the Internet. For more information, see <a href="#">PAN-DB Cloud Connectivity Issues</a>.</li><li>• If the message is <code>PAN-DB download: Finished successfully</code>, the firewall successfully downloaded the URL seed database. Try to enable PAN-DB again by running the following command: <code>admin@PA-200&gt; set system setting url-database paloaltonetworks</code></li></ul></p>
<p>6. If the problems persists, contact Palo Alto Networks support.</p>

## PAN-DB Cloud Connectivity Issues

To check cloud connectivity, run the following command:

```
admin@pa-200> show url-cloud status
```

If the cloud is accessible, the expected response is similar to the following:

```
admin@PA-200> show url-cloud status
PAN-DB URL Filtering
License : valid
Current cloud server : s0000.urlcloud.paloaltonetworks.com
Cloud connection : connected
URL database version - device : 2013.11.18.000
URL database version - cloud : 2013.11.18.000 ( last update time
2013/11/19
13:20:51 )
URL database status : good
URL protocol version - device : pan/0.0.2
URL protocol version - cloud : pan/0.0.2
Protocol compatibility status : compatible
```

If the cloud is not accessible, the expected response is similar to the following:

```
admin@PA-200> show url-cloud status
PAN-DB URL Filtering
License : valid
Cloud connection : not connected
URL database version - device : 2013.11.18.000
URL database version - cloud : 2013.11.18.000 ( last update time
2013/11/19
13:20:51 )
URL database status : good
URL protocol version - device : pan/0.0.2
URL protocol version - cloud : pan/0.0.2
Protocol compatibility status : compatible
```

The following table describes procedures that you can use to resolve issues based on the output of the `show url-cloud status` command, how to ping the URL cloud servers, and what to check if the firewall is in a High Availability (HA) configuration.

### Troubleshoot Cloud Connectivity Issues

- PAN-DB URL Filtering license field shows invalid—Obtain and install a valid PAN-DB license.
- URL database status is out of date—Download a new seed database by running the following command:

```
admin@pa-200> request url-filtering download paloaltonetworks region <region>
```

- URL protocol version shows not compatible—Upgrade PAN-OS to the latest version.

- Attempt to ping the PAN-DB cloud server from the firewall by running the following command:

```
admin@pa-200> ping source <ip-address> host s0000.urlcloud.paloaltonetworks.com
```

For example, if your management interface IP address is 10.1.1.5, run the following command:

```
admin@pa-200> ping source 10.1.1.5 host s0000.urlcloud.paloaltonetworks.com
```

- If the firewall is in an HA configuration, verify that the HA state of the devices supports connectivity to the cloud systems. You can determine the HA state by running the following command:

```
admin@pa-200> show high-availability state
```

Connection to the cloud will be blocked if the firewall is not in one of the following states:

- active
- active-primary
- active-secondary

If the problem persists, contact Palo Alto Networks support.

## URLs Classified as Not-Resolved

The following table describes procedures you can use to resolve issues where some or all of the URLs being identified by PAN-DB are classified as *Not-resolved*.

### Troubleshoot URLs Classified as Not-Resolved

1. Check the PAN-DB cloud connection by running the following command:

```
admin@PA-200> show url-cloud status
```

The Cloud connection: field should show *connected*. If you see anything other than *connected*, any URL that do not exist in the management plane cache will be categorized as *not-resolved*. To resolve this issue, see [PAN-DB Cloud Connectivity Issues](#).

2. If the cloud connection status shows *connected*, check the current utilization of the firewall. If the firewall's performance is spiking, URL requests may be dropped (may not reach the management plane), and will be categorized as *not-resolved*.

To view system resources, run the following command and view the %CPU and %MEM columns:

```
admin@PA-200> show system resources
```

You can also view system resources from the firewall's web interfaces by clicking the **Dashboard** tab and viewing the **System Resources** section.

3. If the problem persist, contact Palo Alto Networks support.

## Incorrect Categorization

The following steps describe the procedures you can use if you identify a URL that does not have the correct categorization. For example, if the URL `paloaltonetworks.com` was categorized as `alcohol-and-tobacco`, the categorization is not correct; the category should be `computer-and-internet-info`.

### Troubleshoot Incorrect Categorization Issues

1. Verify the category in the dataplane by running the following command:

```
admin@PA-200> show running url <URL>
```

For example, to view the category for the Palo Alto Networks website, run the following command:

```
admin@PA-200> show running url paloaltonetworks.com
```

If the URL stored in the dataplane cache has the correct category (`computer-and-internet-info` in this example), then the categorization is correct and no further action is required. If the category is not correct, continue to the next step.

2. Verify if the category in the management plane by running the command:

```
admin@PA-200> test url-info-host <URL>
```

For example:

```
admin@PA-200> test url-info-host paloaltonetworks.com
```

If the URL stored in the management plane cache has the correct category, remove the URL from the dataplane cache by running the following command:

```
admin@PA-200> clear url-cache url <URL>
```

The next time the device requests the category for this URL, the request will be forwarded to the management plane. This will resolve the issue and no further action is required. If this does not solve the issue, go to the next step to check the URL category on the cloud systems.

3. Verify the category in the cloud by running the following command:

```
admin@PA-200> test url-info-cloud <URL>
```

4. If the URL stored in the cloud has the correct category, remove the URL from the dataplane and the management plane caches.

Run the following command to delete a URL from the dataplane cache:

```
admin@PA-200> clear url-cache url <URL>
```

Run the following command to delete a URL from the management plane cache:

```
admin@PA-200> delete url-database url <URL>
```

The next time the device queries for the category of the given URL, the request will be forwarded to the management plane and then to the cloud. This should resolve the category lookup issue. If problems persist, see the next step to submit a categorization change request.

5. To submit a change request from the web interface, go to the URL log and select the log entry for the URL you would like to have changed.

### Troubleshoot Incorrect Categorization Issues

6. Click the **Request Categorization** change link and follow instructions. You can also request a category change from the Palo Alto Networks Test A Site website by searching for the URL and then clicking the **Request Change** icon. To view a list of all available categories with descriptions of each category, refer to <https://urlfiltering.paloaltonetworks.com/CategoryList.aspx>.

If your change request is approved, you will receive an email notification. You then have two options to ensure that the URL category is updated on the firewall:

- Wait until the URL in the cache expires and the next time the URL is accessed by a user, the new categorization update will be put in the cache.
- Run the following command to force an update in the cache:

```
admin@PA-200> request url-filtering update url <URL>
```

### URL Database Out of Date

If you have observed through the syslog or the CLI that PAN-DB is out-of-date, it means that the connection from the firewall to the URL Cloud is blocked. This usually occurs when the URL database on the firewall is too old (version difference is more than three months) and the cloud cannot update the firewall automatically. In order to resolve this issue, you will need to re-download an initial seed database from the cloud (this operation is not blocked). This will result in an automatic re-activation of PAN-DB.

To manually update the database, perform one of the following steps:

- From the web interface, select **Device > Licenses** and in the **PAN-DB URL Filtering** section click the **Re-Download** link.
- From the CLI, run the following command:

```
admin@PA-200> request url-filtering download paloaltonetworks region <region_name>
```



When the seed database is re-download, the URL cache in the management plane and dataplane will be purged. The management plane cache will then be re-populated with the contents of the new seed database.



# Quality of Service

---

Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which traffic is handled, and the amount of bandwidth afforded to traffic.

Palo Alto Networks Application Quality of Service (QoS) provides basic QoS applied to networks and extends it to provide QoS to applications and users.

Use the following topics to learn about and configure Palo Alto Networks Application QoS:

- ▲ [QoS Overview](#)
- ▲ [QoS Concepts](#)
- ▲ [Configure QoS](#)
- ▲ [Configure QoS for a Virtual System](#)
- ▲ [Enforce QoS Based on DSCP Classification](#)
- ▲ [QoS Use Cases](#)



- Use the Palo Alto Networks [product comparison tool](#) to view the QoS features supported on your firewall platform. Select two or more product platforms and click **Compare Now** to view QoS feature support for each platform (for example, you can check if your firewall platform supports QoS on subinterfaces and if so, the maximum number of subinterfaces on which QoS can be enabled).
- QoS on Aggregate Ethernet (AE) interfaces is supported on PA-7000 Series, PA-5000 Series, PA-3000 Series, and PA-2000 Series firewalls running PAN-OS 7.0 or later release versions.

## QoS Overview

Use QoS to prioritize and adjust quality aspects of network traffic. You can assign the order in which packets are handled and allot bandwidth, ensuring preferred treatment and optimal levels of performance are afforded to selected traffic, applications, and users.

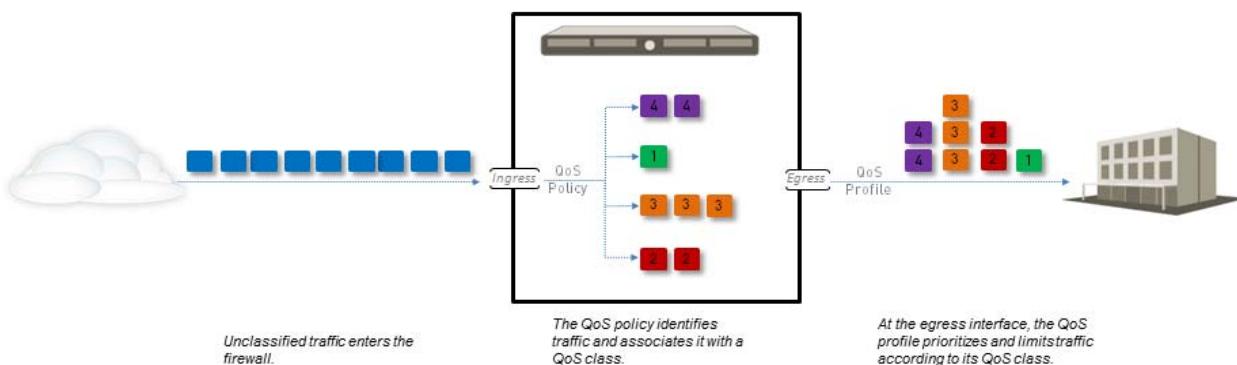
Service quality measurements subject to a QoS implementation are bandwidth (maximum rate of transfer), throughput (actual rate of transfer), latency (delay), and jitter (variance in latency). The capability to shape and control these service quality measurements makes QoS of particular importance to high-bandwidth, real-time traffic such as voice over IP (VoIP), video conferencing, and video-on-demand that has a high sensitivity to latency and jitter. Additionally, use QoS to achieve outcomes such as the following:

- Prioritize network and application traffic, guaranteeing high priority to important traffic or limiting non-essential traffic.
- Achieve equal bandwidth sharing among different subnets, classes, or users in a network.
- Allocate bandwidth externally or internally or both, applying QoS to both upload and download traffic or to only upload or download traffic.
- Ensure low latency for customer and revenue-generating traffic in an enterprise environment.
- Perform traffic profiling of applications to ensure bandwidth usage.

QoS implementation on a Palo Alto Networks firewall begins with three primary configuration components that support a full QoS solution: a [QoS Profile](#), a [QoS Policy](#), and setting up the [QoS Egress Interface](#). Each of these options in the QoS configuration task facilitate a broader process that optimizes and prioritizes the traffic flow and allocates and ensures bandwidth according to configurable parameters.

The figure [QoS Traffic Flow](#) shows traffic as it flows from the source, is shaped by the firewall with QoS enabled, and is ultimately prioritized and delivered to its destination.

### QoS Traffic Flow



The QoS configuration options allow you to control the traffic flow and define it at different points in the flow. The [QoS Traffic Flow](#) indicates where the configurable options define the traffic flow. Use the QoS Profile to define QoS classes and use the QoS Policy to associate QoS classes with selected traffic. Enable the QoS Profile on an interface to shape traffic according to the QoS configuration as it flows through the network.

You can configure a QoS Profile and QoS Policy individually or in any order, according to your preference. Each of the QoS configuration options has components that influence the definition of the other options and the QoS configuration options can be used to create a full and granular QoS policy or can be used sparingly with minimal administrator action.

Each firewall model supports a maximum number of ports that can be configured with QoS. Refer to the spec sheet for your [firewall model](#) or use the [product comparison tool](#) to view QoS feature support for two or more firewalls on a single page.

## QoS Concepts

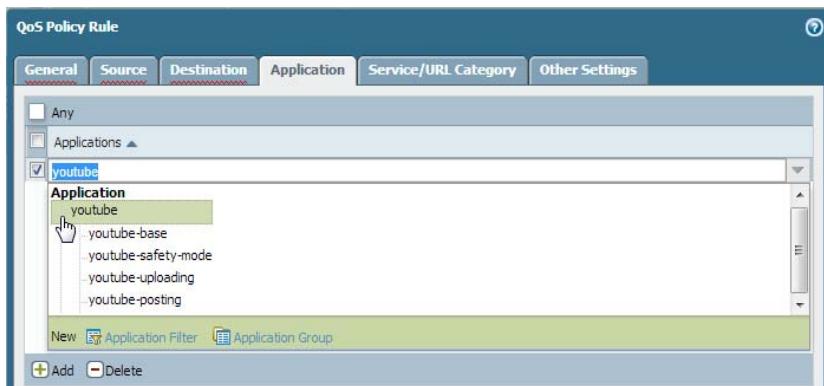
Use the following topics to learn about the different components and mechanisms of a QoS configuration on a Palo Alto Networks firewall:

- ▲ [QoS for Applications and Users](#)
- ▲ [QoS Profile](#)
- ▲ [QoS Classes](#)
- ▲ [QoS Policy](#)
- ▲ [QoS Egress Interface](#)
- ▲ [QoS Clear Text and Tunneled Traffic](#)

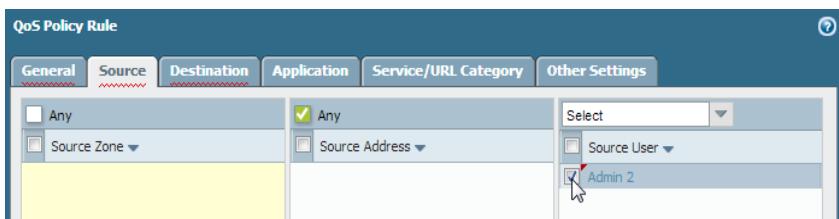
### QoS for Applications and Users

A Palo Alto Networks firewall provides basic QoS, controlling traffic leaving the firewall according to network or subnet, and extends the power of QoS to also classify and shape traffic according to application and user. The Palo Alto Networks firewall provides this capability by integrating the features App-ID and User-ID with the QoS configuration. App-ID and User-ID entries that exist to identify specific applications and users in your network are available in the QoS configuration so that you can easily specify applications and users to apply QoS to.

You can use a QoS Policy in the web interface (**Policies > QoS**) to apply QoS specifically to an application's traffic:



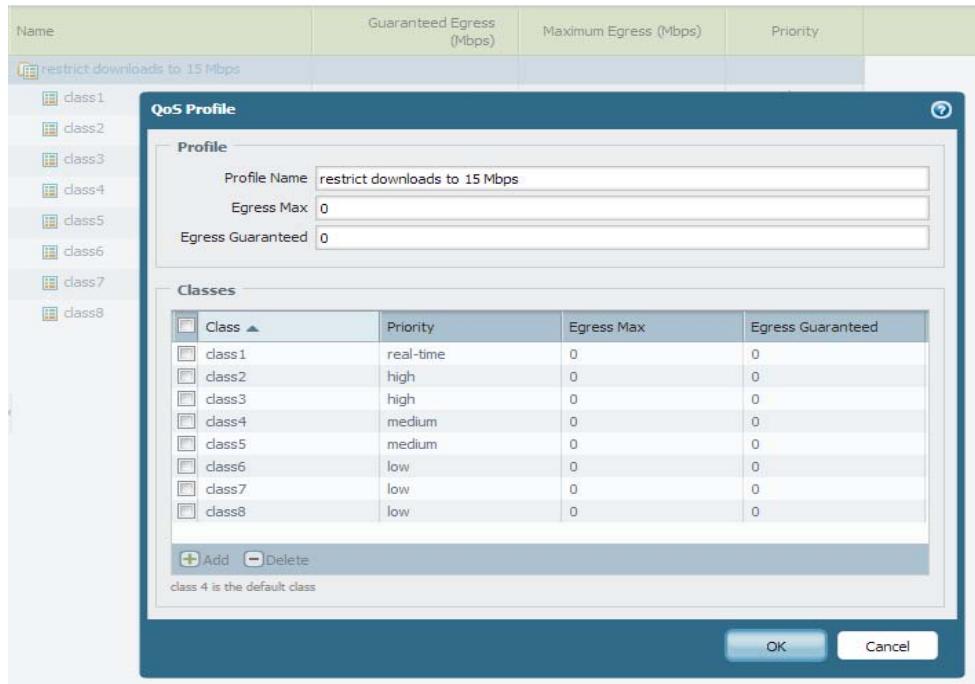
Or to a user's traffic:



See [App-ID](#) and [User-ID](#) for more information on these features.

## QoS Profile

Use a QoS profile to define values of up to eight QoS classes contained within that single profile (**Network > Network Profiles > QoS Profile**):



You enable QoS by applying a QoS profile to the egress interface for network, application, and user traffic, and for clear text or tunneled traffic. An interface configured with QoS shapes traffic according to the QoS profile class definitions and the traffic associated with those classes in the QoS policy.

A default QoS Profile is available on the firewall. The default profile and the classes defined in the profile do not have predefined maximum or guaranteed bandwidth limits.

You can set bandwidth limits for a QoS profile and/or set limits for individual QoS classes within the QoS profile. The total guaranteed bandwidth limits of all eight QoS classes in a QoS Profile cannot exceed the total bandwidth allocated to that QoS Profile. Enabling QoS on a physical interface includes setting the maximum bandwidth for traffic leaving the firewall through this interface. A QoS profile's guaranteed bandwidth (the **Egress Guaranteed** field) should not exceed the bandwidth allocated to the physical interface that QoS is enabled on.

For details, see [Add a QoS profile](#).

## QoS Classes

A QoS class determines the priority and bandwidth for traffic it is assigned to. In the web interface, use the QoS profile to define QoS classes (**Network > Network Profiles > QoS Profile**):

Class	Priority	Egress Max	Egress Guaranteed
class1	medium	0	0
class2	high	0	0
class3	high	0	0

Defining a QoS class includes setting the class's Priority, maximum bandwidth (Egress Max), and guaranteed bandwidth (Egress Guaranteed).



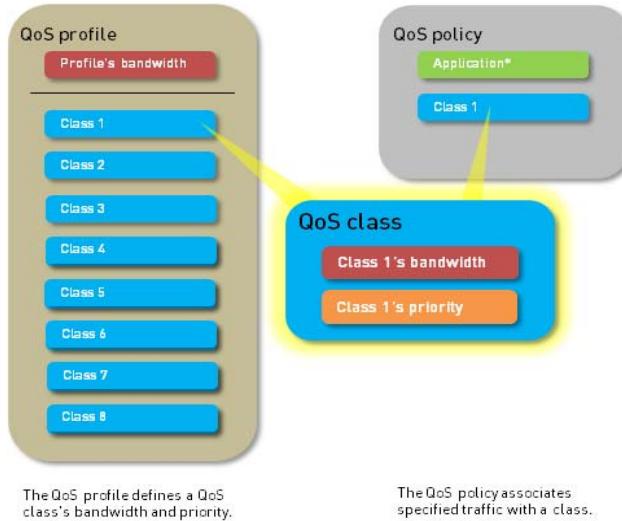
Real-time priority is typically used for applications that are particularly sensitive to latency, such as voice and video applications.

Use the QoS policy to assign a QoS class to specified traffic (**Policies > QoS**):

Class	1
Schedule	None

There are up to eight definable QoS classes in a single QoS profile. Unless otherwise configured, traffic that does not match a QoS class is assigned a class of 4.

QoS priority queuing and bandwidth management, the fundamental mechanisms of a QoS configuration, are configured within the QoS class definition (see [Step 3](#)). Queuing priority is determined by the priority set for a QoS class. Bandwidth management is determined according to the maximum and guaranteed bandwidths set for a QoS class.



The queuing and bandwidth management mechanisms determine the order of traffic and how traffic is handled upon entering or leaving a network:

- **QoS Priority:** One of four QoS priorities can be defined in a QoS class: real-time, high, medium, and low. When a QoS class is associated with specific traffic, the priority defined in that QoS class is assigned to the traffic. Packets in the traffic flow are then queued according to their priority until the network is ready to process them. This method of priority queuing provides the capability to ensure that important traffic, applications, or users takes precedence.
- **QoS Class Bandwidth Management:** QoS class bandwidth management provides the capability to control traffic flows on a network so that traffic does not exceed network capacity, resulting in network congestion, or to allocate specific bandwidth limits to traffic, applications, or users. You can set overall limits on bandwidth using the QoS profile or set limits for individual QoS classes. A QoS profile and QoS classes in the profile have guaranteed and maximum bandwidth limits. The guaranteed bandwidth limit (Egress Guaranteed) ensures that any amount of traffic up to that set bandwidth limit is processed. The maximum bandwidth limit (Egress Max) sets the total limit of bandwidth allocated to either the QoS Profile or QoS Class. Traffic in excess of the Maximum Bandwidth limit is dropped. The total bandwidth limits and guaranteed bandwidth limits of QoS classes in a QoS profile cannot exceed the bandwidth limit of the QoS profile.

## QoS Policy

Use a QoS policy rule to define traffic to receive QoS treatment (either preferential treatment or bandwidth-limiting) and assigns such traffic a QoS class of service.

Define a QoS policy rule to match to traffic based on:

- Applications and application groups.
- Source zones, source addresses, and source users.
- Destination zones and destination addresses.

- Services and service groups limited to specific TCP and/or UDP port numbers.
- URL categories, including custom URL categories.
- Differentiated Services Code Point (DSCP) and Type of Service (ToS) values, which are used to indicate the level of service requested for traffic, such as high priority or best effort delivery.

Set up multiple QoS policy rules (**Policies > QoS**) to associate different types of traffic with different **QoS Classes** of service.



## QoS Egress Interface

Enabling a QoS profile on the egress interface of the traffic identified for QoS treatment completes a QoS configuration. The ingress interface for QoS traffic is the interface on which the traffic enters the firewall. The egress interface for QoS traffic is the interface that traffic leaves the firewall from. QoS is always enabled and enforced on a traffic flow's egress interface. The egress interface in a QoS configuration can either be the external- or internal-facing interface of the firewall, depending on the flow of the traffic receiving QoS treatment.

For example, in an enterprise network, if you are limiting employees' download traffic from a specific website, the egress interface in the QoS configuration is the firewall's internal interface, as the traffic flow is from the Internet, through the firewall, and to your company network. Alternatively, when limiting employees' upload traffic to the same website, the egress interface in the QoS configuration is the firewall's external interface, as the traffic you are limiting flows from your company network, through the firewall, and then to the Internet.



See [Step 3](#) to learn how to Identify the egress interface for applications that you identified as needing QoS treatment.

## QoS Clear Text and Tunneled Traffic

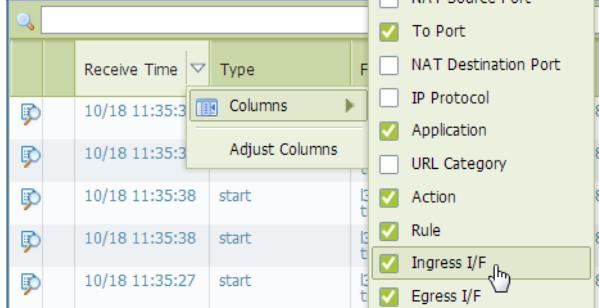
At the minimum, enabling a QoS interfaces requires you to select a default QoS profile to be used to shape all clear text traffic egressing the interface. However, when setting up or modifying a QoS interface, granular QoS settings can be applied to outgoing clear text traffic and tunneled traffic. QoS preferential treatment and bandwidth limiting can be enforced for individual tunnel interfaces and/or for clear text traffic originating from different source interfaces and source subnets.



On Palo Alto Networks firewalls, *tunneled traffic* refers to tunnel interface traffic, specifically IPSec traffic in tunnel mode.

# Configure QoS

Follow these steps to configure Quality of Service (QoS), which includes creating a QoS profile, creating a QoS policy, and enabling QoS on an interface.

Configure QoS	
<p><b>Step 1</b> Identify the traffic to which to apply QoS.</p> <p>This example shows how to use QoS to limit web browsing.</p>	<p>Select <b>ACC</b> to view the <b>Application Command Center</b> page. Use the settings and charts on the <b>ACC</b> page to view trends and traffic related to Applications, URL filtering, Threat Prevention, Data Filtering, and HIP Matches.</p> <p>Click any application name to display detailed application information.</p>
<p><b>Step 2</b> Identify the egress interface for applications that you identified as needing QoS treatment.</p> <p> The egress interface for traffic depends on the traffic flow. If you are shaping incoming traffic, the egress interface is the internal-facing interface. If you are shaping outgoing traffic, the egress interface is the external-facing interface.</p>	<p>Select <b>Monitor &gt; Logs &gt; Traffic</b> to view the device's traffic logs. To filter and only show logs for a specific application:</p> <ul style="list-style-type: none"> <li>If an entry is displayed for the application, click the underlined link in the Application column then click the Submit icon.</li> <li>If an entry is not displayed for the application, click the Add Log icon and search for the application.</li> </ul> <p>The <b>Egress I/F</b> in the traffic logs displays each application's egress interface. To display the <b>Egress I/F</b> column if it is not displayed by default:</p> <ul style="list-style-type: none"> <li>Click any column header to add a column to the log:</li> </ul>  <ul style="list-style-type: none"> <li>Click the spyglass icon to the left of any entry to display a detailed log that includes the application's egress interface listed in the Destination section:</li> </ul>  <p>In this example, the egress interface for web-browsing traffic is ethernet 1/1.</p>

### Configure QoS (Continued)

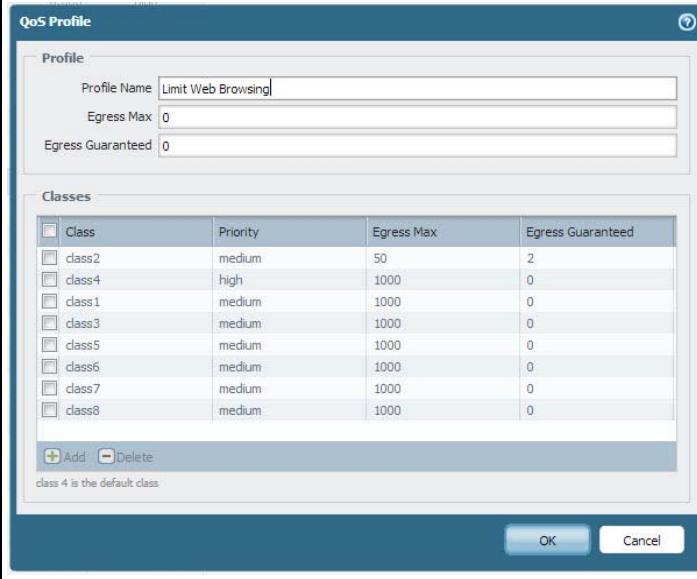
#### Step 3 Add a QoS profile.

A QoS profile allows you to define the eight classes of service that traffic can receive, including the priority and bandwidth for each class, as well as the total, combined bandwidth for all eight classes.

You can edit any existing QoS profile, including the default, by clicking the QoS profile name.

1. Select **Network > Network Profiles > QoS Profile** and click **Add** to open the **QoS Profile** dialog.
  2. Enter a descriptive **Profile Name**.
  3. Enter an **Egress Max** to set the overall bandwidth allocation for the QoS Profile.
  4. Enter an **Egress Guaranteed** to set the guaranteed bandwidth for the QoS Profile.
-  Any traffic that exceeds the **Egress Guaranteed** value is best effort and not guaranteed.
5. In the Classes section, specify how to treat up to eight individual QoS classes:
    - a. Click **Add** to add a class to the QoS Profile.
    - b. Select the **Priority** for the class.
    - c. Enter an **Egress Max** for a class to set the overall bandwidth limit for that individual class.
    - d. Enter an **Egress Guaranteed** for the class to set the guaranteed bandwidth for that individual class.
  6. Click **OK** to save the QoS Profile.

In the following example, the QoS Profile named Limit Web Browsing limits traffic identified as Class 2 traffic to maximum bandwidth of 50Mbps and a guaranteed bandwidth of 2Mbps. Any traffic that is associated with class 2 in a the QoS policy ([Step 4](#)) is subject to these limits.



The screenshot shows the 'QoS Profile' dialog box. The 'Profile' section contains fields for 'Profile Name' (set to 'Limit Web Browsing'), 'Egress Max' (set to 0), and 'Egress Guaranteed' (set to 0). The 'Classes' section displays a table with eight rows, each representing a QoS class. The table columns are 'Class', 'Priority', 'Egress Max', and 'Egress Guaranteed'. The data in the table is as follows:

Class	Priority	Egress Max	Egress Guaranteed
class2	medium	50	2
class4	high	1000	0
class1	medium	1000	0
class3	medium	1000	0
class5	medium	1000	0
class6	medium	1000	0
class7	medium	1000	0
class8	medium	1000	0

Below the table, there are 'Add' and 'Delete' buttons, and a note stating 'class 4 is the default class'. At the bottom right are 'OK' and 'Cancel' buttons.

## Configure QoS (Continued)

### Step 4 Add a QoS policy rule.

A QoS policy allows define traffic to receive QoS treatment, and to assign traffic matched to the policy rule a QoS class of service.

1. Select **Policies > QoS** and click **Add** to open the QoS Policy Rule dialog.
2. On the **General** tab, give the QoS Policy Rule a descriptive **Name**.
3. Specify the traffic to which the QoS Policy Rule will apply. Use the **Source**, **Destination**, **Application**, **Service/URL Category**, and **DSCP/ToS** tabs to define matching parameters for identifying traffic (use the **DSCP/ToS** tab to [Enforce QoS Based on DSCP Classification](#)).

For example, select the **Application** tab, click **Add**, and select web-browsing to apply the QoS Policy Rule to that application:



(Optional) Define additional parameters. For example, on the **Source** tab, click **Add** to limit web-browsing for a specific user, in this case, user1:



4. On the **Other Settings** tab, select a QoS Class to assign to the QoS Policy Rule. For example, assign Class 2 to the user1's web-browsing traffic:



5. Click **OK** to save the QoS Policy Rule.

## Configure QoS (Continued)

<p><b>Step 5</b> Enable the QoS Profile on a physical interface.</p> <p>You can configure settings to select clear text and tunneled traffic for unique QoS treatment, in addition to the QoS configuration on the physical interface:</p> <ul style="list-style-type: none"> <li>• To define QoS treatment for clear text traffic based on source interface and subnet, perform step 4.</li> <li>• To define QoS treatment for a specific tunnel interface(s), perform step 5.</li> </ul> <p>See <a href="#">QoS Clear Text and Tunneled Traffic</a> for details on enforcing QoS for clear text and tunneled traffic.</p> <p> Check if the platform you're using supports enabling QoS on a subinterface by reviewing a summary of the <a href="#">Product Specifications</a>.</p> <p> It is a best practice to always define the <b>Egress Max</b> value for a QoS interface.</p>
---

1. Select **Network > QoS** and click **Add** to open the QoS Interface dialog.
2. Enable QoS on the physical interface:
  - a. On the **Physical Interface** tab, select the **Interface Name** of the interface to which to enable QoS. In the example, Ethernet 1/1 is the egress interface for web-browsing traffic (see [Step 2](#)).
  - b. Select **Turn on QoS feature on this interface**.
3. On the **Physical Interface** tab, select a QoS profile to apply by default to all **Clear Text** traffic.
 

(Optional) Use the Tunnel Interface field to apply a QoS profile by default to all tunneled traffic.

For example, enable QoS on ethernet 1/1 and apply the QoS Profile named Limit Web Browsing as the default QoS Profile for clear text traffic.

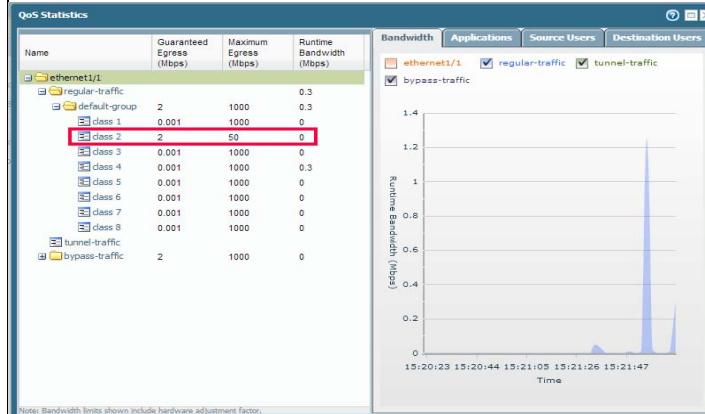

4. (Optional) Select **Clear Text Traffic** and configure more granular QoS settings for clear text traffic:
  - Set the **Egress Guaranteed** and **Egress Max** bandwidths for clear text traffic.
  - Click **Add** to further specify QoS treatment for clear text traffic, based on source interface and source subnet.
5. (Optional) Select **Tunneled Traffic** and configure more granular QoS settings for tunnel interfaces:
  - Set the **Egress Guaranteed** and **Egress Max** bandwidths for tunneled traffic.
  - Click **Add** and attach a QoS profile to a single tunnel interface.
6. Click **OK** and **Commit** the changes to enable QoS on the interface.

### Configure QoS (Continued)

**Step 6** Verify QoS configuration.

Select **Network > QoS** and then **Statistics** to view QoS bandwidth, active sessions of a selected QoS class, and active applications for the selected QoS class.

For example, see the statistics for ethernet 1/1 with QoS enabled:



Class 2 traffic limited to 2Mbps of guaranteed bandwidth and a maximum bandwidth of 50Mbps.

Continue to click the tabs to display further information regarding applications, source users, destination users, security rules and QoS rules.



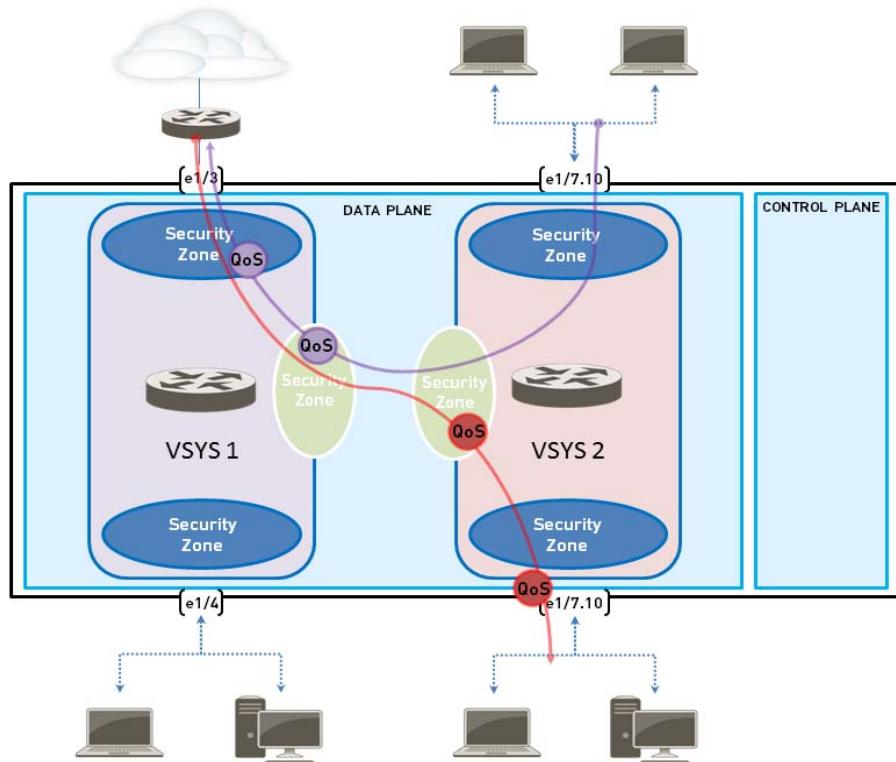
Bandwidth limits shown on the **QoS Statistics** window include a hardware adjustment factor.

## Configure QoS for a Virtual System

QoS can be configured for a single or several virtual systems configured on a Palo Alto Networks firewall. Because a virtual system is an independent firewall, QoS must be configured independently for a single virtual system.

Configuring QoS for a virtual system is similar to configuring QoS on a physical firewall, with the exception that configuring QoS for a virtual system requires specifying the source and destination of traffic. Because a virtual system exists without set physical boundaries and because traffic in a virtual environment spans more than one virtual system, specifying source and destination zones and interfaces for traffic is necessary to control and shape traffic for a single virtual system.

The example below shows two virtual systems configured on firewall. VSYS 1 (purple) and VSYS 2 (red) each have QoS configured to prioritize or limit two distinct traffic flows, indicated by their corresponding purple (VSYS 1) and red (VSYS 2) lines. The QoS nodes indicate the points at traffic is matched to a QoS policy and assigned a QoS class of service, and then later indicate the point at which traffic is shaped as it egresses the firewall.



Refer to the [Virtual Systems \(VSYS\) tech note](#) for information on Virtual Systems and how to configure them.

### Configure QoS in a Virtual System Environment

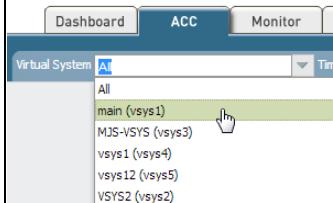
<p><b>Step 1</b> Confirm that the appropriate interfaces, virtual routers, and security zones are associated with each virtual system.</p>	<ul style="list-style-type: none"> <li>To view configured interfaces, select <b>Network &gt; Interface</b>.</li> <li>To view configured zones, select <b>Network &gt; Zones</b>.</li> <li>To view information on defined virtual routers, select <b>Network &gt; Virtual Routers</b>.</li> </ul>
--	--

**Configure QoS in a Virtual System Environment**

**Step 2** Identify traffic to apply QoS to.

Select **ACC** to view the **Application Command Center** page. Use the settings and charts on the **ACC** page to view trends and traffic related to Applications, URL filtering, Threat Prevention, Data Filtering, and HIP Matches.

To view information for a specific virtual system, select the virtual system from the **Virtual System** drop-down:



Click any application name to display detailed application information.

### Configure QoS in a Virtual System Environment

- Step 3** Identify the egress interface for applications that you identified as needing QoS treatment.

In a virtual system environment, QoS is applied to traffic on the traffic's egress point on the virtual system. Depending the configuration and QoS policy for a virtual system, the egress point of QoS traffic could be associated with a physical interface or could be a zone.

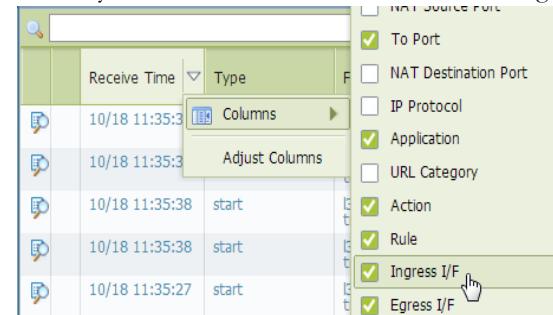
This example shows how to limit web-browsing traffic on vsys 1.

Select **Monitor > Logs > Traffic** to view traffic logs. Each entry has the option to display columns with information necessary to configure QoS in a virtual system environment:

- virtual system
- egress interface
- ingress interface
- source zone
- destination zone

To display a column if it is not displayed by default:

- Click any column header to add a column to the log:



- Click the spyglass icon to the left of any entry to display a detailed log that includes the application's egress interface, as well as source and destination zones, in the **Source** and **Destination** sections:

Source		Destination	
User	Address 10.22.2.68	User	Address 10.0.0.106
Country	10.0.0.0-10.255.255	Country	10.0.0.0-10.255.255
Port	61865	Port	80
Zone	trust	Zone	untrust
Interface	ethernet1/2	Interface	ethernet1/1

Session Counters		Flags	
Bytes	1980	Captive Portal	<input type="checkbox"/>
Bytes Received	858	Proxy Transaction	<input type="checkbox"/>
Bytes Sent	1122	Decrypted	<input type="checkbox"/>
Repeat Count	1	Packet Capture	<input type="checkbox"/>
Packets	12	Client to Server	<input type="checkbox"/>
Packets Received	4	Server to Client	<input type="checkbox"/>
Packets Sent	8	Symmetric Return	<input type="checkbox"/>
		Mirrored	<input type="checkbox"/>

For example, for web-browsing traffic from VSYS 1, the ingress interface is ethernet 1/2, the egress interface is ethernet 1/1, the source zone is *trust* and the destination zone is *untrust*.

## Configure QoS in a Virtual System Environment

### Step 4 Create a QoS Profile.

You can edit any existing QoS Profile, including the default, by clicking the profile name.

1. Select **Network > Network Profiles > QoS Profile** and click **Add** to open the QoS Profile dialog.
2. Enter a descriptive **Profile Name**.
3. Enter an **Egress Max** to set the overall bandwidth allocation for the QoS profile.
4. Enter an **Egress Guaranteed** to set the guaranteed bandwidth for the QoS profile.  
 Any traffic that exceeds the QoS profile's egress guaranteed limit is best effort but is not guaranteed.
5. In the Classes section of the **QoS Profile**, specify how to treat up to eight individual QoS classes:
  - a. Click **Add** to add a class to the QoS Profile.
  - b. Select the **Priority** for the class.
  - c. Enter an **Egress Max** for a class to set the overall bandwidth limit for that individual class.
  - d. Enter an **Egress Guaranteed** for the class to set the guaranteed bandwidth for that individual class.
6. Click **OK** to save the QoS profile.

## Configure QoS in a Virtual System Environment

### Step 5 Create a QoS policy.

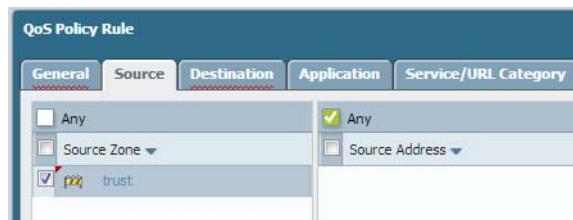
In an environment with multiple virtual systems, traffic spans more than one virtual system. Because of this, when you are enabling QoS for a virtual system, you must define traffic to receive QoS treatment based on source and destination zones. This ensures that the traffic is prioritized and shaped only for that virtual system (and not for other virtual systems through which the traffic might flow).

1. Select **Policies > QoS** and **Add** a QoS Policy Rule.
2. Select **General** and give the QoS Policy Rule a descriptive **Name**.
3. Specify the traffic to which the QoS policy rule will apply. Use the **Source, Destination, Application, and Service/URL Category** tabs to define matching parameters for identifying traffic.

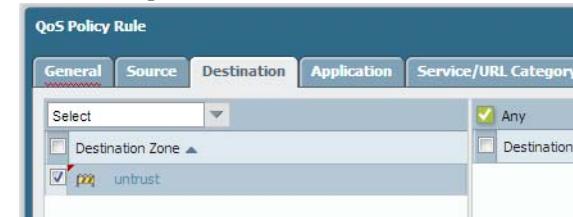
For example, select **Application** and **Add** web-browsing to apply the QoS policy rule to that application:



4. Select **Source** and **Add** the source zone of vsys 1 web-browsing traffic.



5. Select **Destination** and **Add** the destination zone of vsys 1 web-browsing traffic.



6. Select **Other Settings** and select a **QoS Class** to assign to the QoS policy rule. For example, assign Class 2 to web-browsing traffic on vsys 1:



7. Click **OK** to save the QoS policy rule.

## Configure QoS in a Virtual System Environment

- Step 6** Enable the QoS Profile on a physical interface.



It is a best practice to always define the **Egress Max** value for a QoS interface.

- Select **Network > QoS** and click **Add** to open the QoS Interface dialog.

- Enable QoS on the physical interface:

- On the **Physical Interface** tab, select the **Interface Name** of the interface to apply the QoS Profile to.

In this example, ethernet 1/1 is the egress interface for web-browsing traffic on vsys 1 (see [Step 2](#)).



- Select **Turn on QoS feature on this interface**.

- On the **Physical Interface** tab, select the default QoS profile to apply to all **Clear Text** traffic.

(Optional) Use the **Tunnel Interface** field to apply a default QoS profile to all tunneled traffic.

- (Optional) On the **Clear Text Traffic** tab, configure additional QoS settings for clear text traffic:

- Set the **Egress Guaranteed** and **Egress Max** bandwidths for clear text traffic.
- Click **Add** to apply a QoS Profile to selected clear text traffic, further selecting the traffic for QoS treatment according to source interface and source subnet (creating a QoS node).

- (Optional) On the **Tunneled Traffic** tab, configure additional QoS settings for tunnel interfaces:

- Set the **Egress Guaranteed** and **Egress Max** bandwidths for tunneled traffic.
- Click **Add** to associate a selected tunnel interface with a QoS Profile.

- Click **OK** to save changes.

- Commit** the changes.

**Configure QoS in a Virtual System Environment**

**Step 7** Verify QoS configuration.

- Select **Network > QoS** to view the QoS Policies page. The **QoS Policies** page verifies that QoS is enabled and includes a **Statistics** link. Click the Statistics link to view QoS bandwidth, active sessions of a selected QoS node or class, and active applications for the selected QoS node or class.
- In a multi-vsyst environment, sessions cannot span multiple systems. Multiple sessions are created for one traffic flow if the traffic passes through more than one virtual system. To browse sessions running on the firewall and view applied QoS Rules and QoS Classes, select **Monitor > Session Browser**.

## Enforce QoS Based on DSCP Classification

A Differentiated Services Code Point (DSCP) is a packet header value that can be used to indicate the level of service requested for traffic, such as high priority or best effort delivery. Session-Based DSCP Classification allows you to both honor the service class requested for traffic and to mark a session to receive continued QoS treatment. Session-based DSCP extends the power of Quality of Service (QoS), which polices traffic as it passes through the firewall, by allowing all network devices between the firewall and the client to also police traffic. All inbound and outbound traffic for a session can receive continuous QoS/DSCP treatment as it flows through your network. For example, inbound return traffic from an external server can now be treated with the same QoS/DSCP priority that the firewall initially enforced for the outbound flow. Network devices between the firewall and end user will also then enforce the same priority for the return traffic (and any other outbound or inbound traffic for the session).

Use the following steps to enable Session-Based DSCP Classification. Start by configuring QoS based on DSCP marking detected at the beginning of a session. You can then continue to enable the firewall to mark the return flow for a session with the same DSCP value used to enforce QoS for the initial outbound flow.

### Provide QoS Based on DSCP/ToS Marking

Before you set up or modify a QoS policy to control traffic based on DSCP/ToS code point values, make sure that you have performed the preliminary steps for configuring QoS.

The following steps are useful before setting up a QoS policy:

- Identify the traffic to which to apply QoS.
- Identify the egress interface for traffic to be enforced with QoS.

See [Configure QoS](#) for details on performing these steps.

### Provide QoS Based on DSCP/ToS Marking (Continued)

**Step 1** Apply QoS to traffic based on the DSCP value detected at the beginning of the session.

1. Select **Policies > QoS** and **Add** or modify an existing QoS rule and populate required fields.
2. **Add a DSCP/ToS rule** and give the rule a descriptive **Name**. You can choose to add multiple DSCP/ToS rules to a single QoS rule to enforce the same QoS priority for sessions with different DSCP values.
3. Select the **Type** of DSCP/ToS marking for the QoS rule to match to traffic:



It is a best practice to use a single DSCP type to manage and prioritize your network traffic.

- **Expedited Forwarding (EF):** Can be used to request low loss, low latency and guaranteed bandwidth for traffic. Packets with EF codepoints are typically guaranteed highest priority delivery.
- **Assured Forwarding (AF):** Can be used to provide reliable delivery for applications. Packets with AF codepoint indicate a request for the traffic to receive higher priority treatment than best effort service provides (though packets with an EF codepoint will continue to take precedence over those with an AF codepoint).
- **Class Selector (CS):** Can be used to provide backward compatibility with network devices that use the IP precedence field to mark priority traffic.
- **IP Precedence (ToS):** Can be used by legacy network devices to mark priority traffic (the IP Precedence header field was used to indicate the priority for a packet before the introduction of the DSCP classification).
- **Custom Codepoint:** Create a custom codepoint to match to traffic by entering a **Codepoint Name** and **Binary Value**.

For example, select the **Assured Forwarding (AF)** to ensure traffic marked with an **AF** codepoint value has higher priority for reliable delivery over applications marked to receive lower priority.

4. Match the QoS policy to traffic on a more granular scale by specifying the **Codepoint** value. For example, with Assured Forwarding (AF) selected as the **Type** of DSCP value for the policy to match, further specify an AF **Codepoint** value such as AF11.



When Expedited Forwarding (EF) is selected as the **Type** of DSCP marking, a granular **Codepoint** value cannot be specified. The QoS policy will match to traffic marked with any EF codepoint value.

5. Select **Other Settings** and a **QoS Class** to assign to traffic matched to the QoS rule. For example, assign Class 1 to sessions where a DSCP marking of AF11 is detected for the first packet in the session.
6. Click **OK** to save the QoS rule.

**Step 2** Define the QoS priority for traffic to receive when it is matched to a QoS rule based the DSCP marking detected at the beginning of a session.

1. Select **Network > Network Profiles > QoS Profile** and **Add** or modify an existing QoS profile. For details on profile options to set priority and bandwidth for traffic, see [QoS Concepts](#) and [Configure QoS](#).
2. **Add** or modify a profile class. For example, because **Step 1** showed steps to classify AF11 traffic as Class 1 traffic, you could add or modify a **class1** entry.
3. Select a **Priority** for the class of traffic, such as **high**.
4. Click **OK** to save the QoS Profile.

Provide QoS Based on DSCP/ToS Marking (Continued)	
Step 3 Enable QoS on an interface.	Select <b>Network &gt; QoS</b> and <b>Add</b> or modify an existing interface and <b>Turn on QoS feature on this interface</b> .  In this example, traffic with an AF11 DSCP marking is matched to the QoS rule and assigned Class 1. The QoS profile enabled on the interface enforces high priority treatment for Class 1 traffic as it egresses the firewall (the session <i>outbound</i> traffic).
Step 4 Enable DSCP Marking.  Mark return traffic with a DSCP value, enabling the inbound flow for a session to be marked with the same DSCP value detected for the outbound flow.	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b> and <b>Add</b> or modify a security policy.</li><li>2. Select <b>Actions</b> and in the <b>QoS Marking</b> drop-down, choose <b>Follow-Client-to-Server-Flow</b>.</li><li>3. Click <b>OK</b> to save your changes.</li></ol> Completing this step enables the firewall to mark traffic with the same DSCP value that was detected at the beginning of a session (in this example, the firewall would mark return traffic with the DSCP AF11 value). While configuring QoS allows you to shape traffic as it egresses the firewall, enabling this option in a security rule allows the other network devices intermediate to the firewall and the client to continue to enforce priority for DSCP marked traffic.
Step 5 Save the configuration.	<b>Commit</b> your changes.

## QoS Use Cases

The following use cases demonstrate how to use QoS in common scenarios:

- ▲ [Use Case: QoS for a Single User](#)
- ▲ [Use Case: QoS for Voice and Video Applications](#)

## Use Case: QoS for a Single User

A CEO finds that during periods of high network usage, she is unable to access enterprise applications to respond effectively to critical business communications. The IT admin wants to ensure that all traffic to and from the CEO receives preferential treatment over other employee traffic so that she is guaranteed not only access to, but high performance of, critical network resources.

### Apply QoS to a Single User

- Step 1** The admin creates the QoS profile *CEO\_traffic* to define how traffic originating from the CEO will be treated and shaped as it flows out of the company network:

The screenshot shows the 'QoS Profile' configuration window. In the 'Profile' section, the 'Profile Name' is set to 'CEO\_traffic', 'Egress Max' is set to '1000', and 'Egress Guaranteed' is set to '50'. In the 'Classes' section, there is a table with one row. The first column is labeled 'Class' and contains 'class1' with a checked checkbox. The second column is labeled 'Priority' and contains 'high'. The third column is labeled 'Egress Max' and contains '1000'. The fourth column is labeled 'Egress Guaranteed' and contains '50'.

The admin assigns a guaranteed bandwidth (**Egress Guaranteed**) of 50 Mbps to ensure that the CEO will have that amount of bandwidth guaranteed to her at all times (more than she would need to use), regardless of network congestion.

The admin continues by designating Class 1 traffic as high priority and sets the profile's maximum bandwidth usage (**Egress Max**) to 1000 Mbps, the same maximum bandwidth for the interface that the admin will enable QoS on. The admin is choosing to not restrict the CEO's bandwidth usage in any way.



It is a best practice to populate the **Egress Max** field for a QoS profile, even if the max bandwidth of the profile matches the max bandwidth of the interface. The QoS profile's max bandwidth should never exceed the max bandwidth of the interface you are planning to enable QoS on.

### Apply QoS to a Single User (Continued)

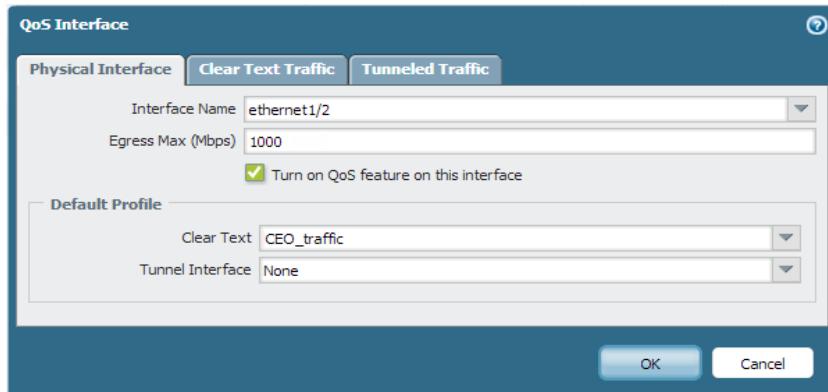
- Step 2** The admin creates a QoS policy to identify the CEO's traffic (**Policies > QoS**) and assigns it the class that he defined in the QoS profile (see [Step 1](#)). Because User-ID is configured, the admin uses the **Source** tab in the QoS policy to singularly identify the CEO's traffic by her company network username. (If User-ID is not configured, the administrator could **Add** the CEO's IP address under **Source Address**. See [User-ID](#)):



The admin associates the CEO's traffic with Class 1 (**Other Settings** tab) and then continues to populate the remaining required policy fields; the admin gives the policy a descriptive **Name** (**General** tab) and selects **Any** for the **Source Zone** (**Source** tab) and **Destination Zone** (**Destination** tab):

Name	Tags	Zone	Source		Destination		Application	Service	Class	Schedule
			Address	User	Zone	Address				
1 Video	none	any	any	any	any	any	google-video	any	1	none
2 HTTPS	none	any	any	companynetwork\JoeAdmin	any	any	http-video		2	none
3 FTP	none	any	any	any	any	any	youtube		4	none
4 Guarantee CEO bandwidth	none	any	any	companynetwork\CEO	any	any	web-browsing	any	1	none

- Step 3** Now that Class 1 is associated with the CEO's traffic, the admin enables QoS by checking **Turn on QoS feature on interface** and selecting the traffic flow's egress interface. The egress interface for the CEO's traffic flow is the external-facing interface, in this case, ethernet 1/2:



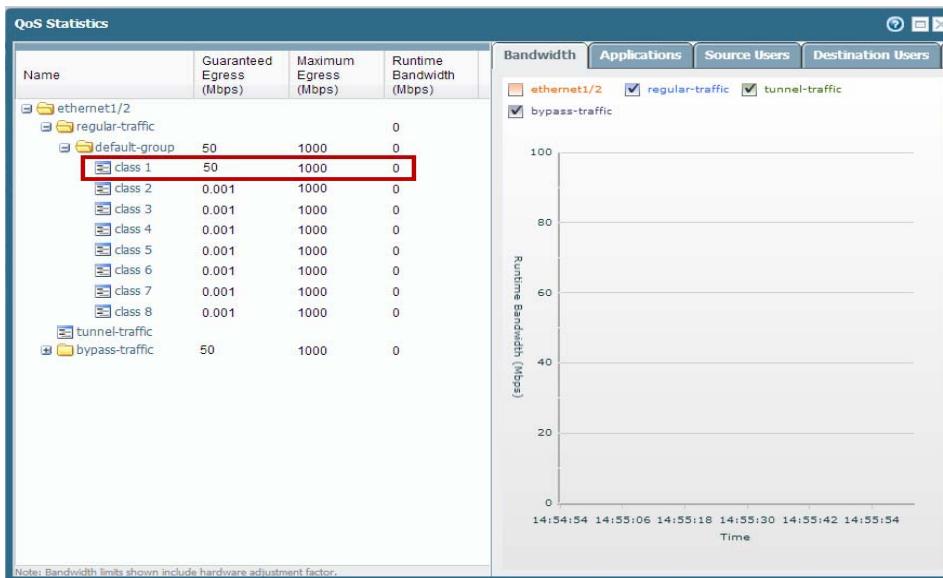
Because the admin wants to ensure that all traffic originating from the CEO is guaranteed by the QoS profile and associated QoS policy he created, he selects the *CEO\_traffic* to apply to **Clear Text** traffic flowing from ethernet 1/2.

### Apply QoS to a Single User (Continued)

- Step 4** After committing the QoS configuration, the admin navigates to the **Network > QoS** page to confirm that the QoS profile *CEO\_traffic* is enabled on the external-facing interface, ethernet 1/2:

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled	
ethernet1/2		1,000.000		<input checked="" type="checkbox"/>	Statistics
Tunneled Traffic	0.000	0.000			
Clear Text Traffic	50.000	0.000	CEO_traffic		
ethernet1/18		0.000		<input checked="" type="checkbox"/>	Statistics
Tunneled Traffic	0.000	0.000			
Clear Text Traffic	0.000	0.000	Limit Facebook apps		
Facebook Apps (ethernet1/19 - any)			Limit Facebook apps		

He clicks **Statistics** to view how traffic originating with the CEO (Class 1) is being shaped as it flows from ethernet 1/2:



 This case demonstrates how to apply QoS to traffic originating from a single source user. However, if you also wanted to guarantee or shape traffic to a destination user, you could configure a similar QoS setup. Instead of, or in addition to this work flow, create a QoS policy that specifies the user's IP address as the **Destination Address** on the **Policies > QoS** page (instead of specifying the user's source information, as shown in Step 2) and then enable QoS on the network's internal-facing interface on the **Network > QoS** page (instead of the external-facing interface, as shown in Step 3.)

## Use Case: QoS for Voice and Video Applications

Voice and video traffic is particularly sensitive to measurements that the QoS feature shapes and controls, especially latency and jitter. For voice and video transmissions to be audible and clear, voice and video packets cannot be dropped, delayed, or delivered inconsistently. A best practice for voice and video applications, in addition to guaranteeing bandwidth, is to guarantee priority to voice and video traffic.

In this example, employees at a company branch office are experiencing difficulties and unreliability in using video conferencing and Voice over IP (VoIP) technologies to conduct business communications with other branch offices, with partners, and with customers. An IT admin intends to implement QoS in order to address these issues and ensure effective and reliable business communication for the branch employees. Because the admin wants to guarantee QoS to both incoming and outgoing network traffic, he will enable QoS on both the firewall's internal- and external-facing interfaces.

### Ensure Quality for Voice and Video Applications

- Step 1** The admin creates a QoS profile, defining Class 2 so that any traffic associated with Class 2 receives real-time priority and on an interface with a maximum bandwidth of 1000 Mbps, is guaranteed a bandwidth of 250 Mbps at all times, including peak periods of network usage.

Real-time priority is typically recommended for applications affected by latency, and is particularly useful in guaranteeing performance and quality of voice and video applications.

On the **Network > Network Profiles > Qos Profile** page, the admin clicks **Add**, enters the **Profile Name** *ensure voip-video traffic* and defines Class 2 traffic.

The screenshot shows the 'QoS Profile' configuration screen. Under the 'Profile' section, the 'Profile Name' is set to 'ensure voip-video traffic', 'Egress Max' is 1000, and 'Egress Guaranteed' is 250. Under the 'Classes' section, there is a table with two rows. The first row has an empty checkbox under 'Class'. The second row has a checked checkbox under 'Class', which is labeled 'class2'. The 'Priority' column is set to 'real-time', and the 'Egress Max' and 'Egress Guaranteed' columns are both set to 1000.

Class	Priority	Egress Max	Egress Guaranteed
<input type="checkbox"/>	real-time	1000	250
<input checked="" type="checkbox"/> class2			

## Ensure Quality for Voice and Video Applications (Continued)

- Step 2** The admin creates a QoS policy to identify voice and video traffic. Because the company does not have one standard voice and video application, the admin wants to ensure QoS is applied to a few applications that are widely and regularly used by employees to communicate with other offices, with partners, and with customers. On the **Policies > QoS > QoS Policy Rule > Applications** tab, the admin clicks **Add** and opens the **Application Filter** window. The admin continues by selecting criteria to filter the applications he wants to apply QoS to, choosing the Subcategory *voip-video*, and narrowing that down by specifying only voip-video applications that are both low-risk and widely-used.

The application filter is a dynamic tool that, when used to filter applications in the QoS policy, allows QoS to be applied to all applications that meet the criteria of *voip-video*, *low risk*, and *widely used* at any given time.

Name	Category	Subcategory	Risk	Technology	Standard Ports
foonz	collaboration	voip-video	1	browser-based	80,tcp
fring	collaboration	voip-video	1	client-server	dynamic,tcp,udp
ms-lync (2 out	ms-lync-	voip-video	1	client-server	dynamic,udp
ms-lync-	collaboration	voip-video	1	client-server	dynamic,udp
naver-line	collaboration	voip-video	1	client-server	443,5223,5242,80

The admin names the **Application Filter** *voip-video-low-risk* and includes it in the QoS policy:

The admin names the QoS policy *Voice-Video* and associates the *voip-video-low-risk* application filter with Class 2 traffic (as he defined it in Step 1). He is going to use the *Voice-Video* QoS policy for both incoming and outgoing QoS traffic, so he sets **Source** and **Destination** information to **Any**:

2	HTTPS	none	any	any	companynet...	any	any	web-browsing	any	2	none
3	FTP	none	any	any	any	any	any	ftp	any	4	none
4	Voice-Video	none	any	any	any	any	any	voip-video-lo...	any	2	none

### Ensure Quality for Voice and Video Applications (Continued)

- Step 3** Because the admin wants to ensure QoS for both incoming and outgoing voice and video communications, he enables QoS on the network's external-facing interface (to apply QoS to outgoing communications) and to the internal-facing interface (to apply QoS to incoming communications).

The admin begins by enabling the QoS profile he created in [Step 1, ensure voice-video traffic](#) (Class 1 in this profile is associated with policy created in [Step 2, Voice-Video](#)) on the external-facing interface, in this case, ethernet 1/2.

He then enables the same QoS profile *ensure voip-video traffic* on the internal-facing interface, in this case, ethernet 1/1.

- Step 4** The admin confirms that QoS is enabled for both incoming and outgoing voice and video traffic:

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled	
ethernet1/1		1,000.000		<input checked="" type="checkbox"/>	Statistics
Tunneled Traffic	0.000	0.000			
Clear Text Traffic	250.000	0.000	ensure voice-video traffic		
ethernet1/2		1,000.000		<input checked="" type="checkbox"/>	Statistics
Tunneled Traffic	0.000	0.000			
Clear Text Traffic	250.000	0.000	ensure voice-video traffic		

The admin has successfully enabled QoS on both the network's internal- and external-facing interfaces. Real-time priority is now ensured for voice and video application traffic as it flows both into and out of the network, ensuring that these communications, which are particularly sensitive to latency and jitter, can be used reliably and effectively to perform both internal and external business communications.





# VPNs

---

Virtual private networks (VPNs) create tunnels that allow users/systems to connect securely over a public network, as if they were connecting over a local area network (LAN). To set up a VPN tunnel, you need a pair of devices that can authenticate each other and encrypt the flow of information between them. The devices can be a pair of Palo Alto Networks firewalls, or a Palo Alto Networks firewall along with a VPN-capable device from another vendor.

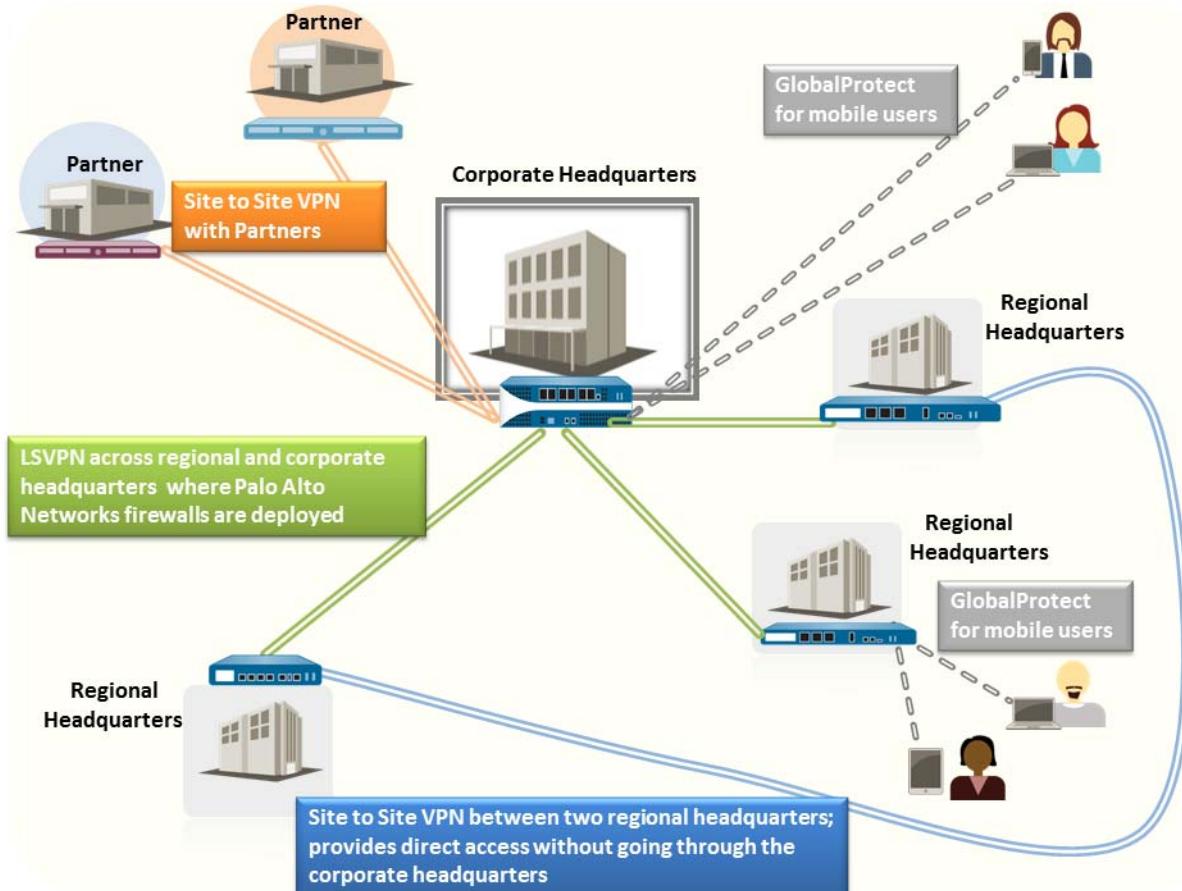
- ▲ [VPN Deployments](#)
- ▲ [Site-to-Site VPN Overview](#)
- ▲ [Site-to-Site VPN Concepts](#)
- ▲ [Set Up Site-to-Site VPN](#)
- ▲ [Site-to-Site VPN Quick Configs](#)

# VPN Deployments

The Palo Alto Networks firewall supports the following VPN deployments:

- **Site-to-Site VPN**—A simple VPN that connects a central site and a remote site, or a hub and spoke VPN that connects a central site with multiple remote sites. The firewall uses the IP Security (IPSec) set of protocols to set up a secure tunnel for the traffic between the two sites. See [Site-to-Site VPN Overview](#).
- **Remote User-to-Site VPN**—A solution that uses the GlobalProtect agent to allow a remote user to establish a secure connection through the firewall. This solution uses SSL and IPSec to establish a secure connection between the user and the site. Refer to the [GlobalProtect Administrator's Guide](#).
- **Large Scale VPN**—The Palo Alto Networks GlobalProtect Large Scale VPN (LSVPN) provides a simplified mechanism to roll out a scalable hub and spoke VPN with up to 1024 satellite offices. The solution requires Palo Alto Networks firewalls to be deployed at the hub and at every spoke. It uses certificates for device authentication, SSL for securing communication between all components, and IPSec to secure data. See [Large Scale VPN \(LSVPN\)](#).

**Figure: VPN Deployments**



## Site-to-Site VPN Overview

A VPN connection that allows you to connect two Local Area Networks (LANs) is called a site-to-site VPN. You can configure route-based VPNs to connect Palo Alto Networks firewalls located at two sites or to connect a Palo Alto Networks firewall with a third-party security device at another location. The firewall can also interoperate with third-party policy-based VPN devices; the Palo Alto Networks firewall supports route-based VPN.

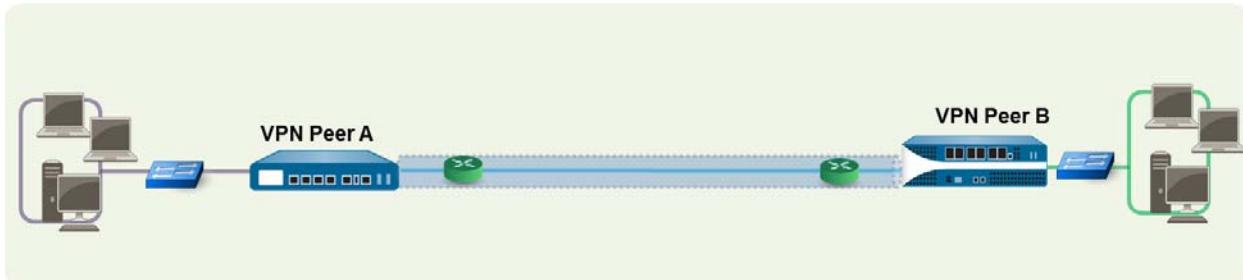
The Palo Alto Networks firewall sets up a route-based VPN, where the firewall makes a routing decision based on the destination IP address. If traffic is routed to a specific destination through a VPN tunnel, then it is handled as VPN traffic.

The IP Security (IPSec) set of protocols is used to set up a secure tunnel for the VPN traffic, and the information in the TCP/IP packet is secured (and encrypted if the tunnel type is ESP). The IP packet (header and payload) is embedded in another IP payload, and a new header is applied and then sent through the IPSec tunnel. The source IP address in the new header is that of the local VPN peer and the destination IP address is that of the VPN peer on the far end of the tunnel. When the packet reaches the remote VPN peer (the firewall at the far end of the tunnel), the outer header is removed and the original packet is sent to its destination.

In order to set up the VPN tunnel, first the peers need to be authenticated. After successful authentication, the peers negotiate the encryption mechanism and algorithms to secure the communication. The Internet Key Exchange (IKE) process is used to authenticate the VPN peers, and IPSec Security Associations (SAs) are defined at each end of the tunnel to secure the VPN communication. IKE uses digital certificates or preshared keys, and the Diffie Hellman keys to set up the SAs for the IPSec tunnel. The SAs specify all of the parameters that are required for secure transmission—including the security parameter index (SPI), security protocol, cryptographic keys, and the destination IP address—encryption, data authentication, data integrity, and endpoint authentication.

The following figure shows a VPN tunnel between two sites. When a client that is secured by VPN Peer A needs content from a server located at the other site, VPN Peer A initiates a connection request to VPN Peer B. If the security policy permits the connection, VPN Peer A uses the IKE Crypto profile parameters (IKE phase 1) to establish a secure connection and authenticate VPN Peer B. Then, VPN Peer A establishes the VPN tunnel using the IPSec Crypto profile, which defines the IKE phase 2 parameters to allow the secure transfer of data between the two sites.

**Figure: Site-to-Site VPN**



## Site-to-Site VPN Concepts

A VPN connection provides secure access to information between two or more sites. In order to provide secure access to resources and reliable connectivity, a VPN connection needs the following components:

- ▲ IKE Gateway
- ▲ Tunnel Interface
- ▲ Tunnel Monitoring
- ▲ Internet Key Exchange (IKE) for VPN
- ▲ IKEv2

### IKE Gateway

The Palo Alto Networks firewalls or a firewall and another security device that initiate and terminate VPN connections across the two networks are called the IKE Gateways. To set up the VPN tunnel and send traffic between the IKE Gateways, each peer must have an IP address—static or dynamic—or FQDN. The VPN peers use preshared keys or certificates to mutually authenticate each other.

The peers must also negotiate the mode—main or aggressive—for setting up the VPN tunnel and the SA lifetime in IKE Phase 1. Main mode protects the identity of the peers and is more secure because more packets are exchanged when setting up the tunnel. Main mode is the recommended mode for IKE negotiation if both peers support it. Aggressive mode uses fewer packets to set up the VPN tunnel and is hence faster but a less secure option for setting up the VPN tunnel.

See [Set Up an IKE Gateway](#) for configuration details.

### Tunnel Interface

To set up a VPN tunnel, the Layer 3 interface at each end must have a logical *tunnel* interface for the firewall to connect to and establish a VPN tunnel. A tunnel interface is a logical (virtual) interface that is used to deliver traffic between two endpoints. If you configure any proxy IDs, the proxy ID is counted toward any IPSec tunnel capacity.

The tunnel interface must belong to a security zone to apply policy and it must be assigned to a virtual router in order to use the existing routing infrastructure. Ensure that the tunnel interface and the physical interface are assigned to the same virtual router so that the firewall can perform a route lookup and determine the appropriate tunnel to use.

Typically, the Layer 3 interface that the tunnel interface is attached to belongs to an external zone, for example the untrust zone. While the tunnel interface can be in the same security zone as the physical interface, for added security and better visibility, you can create a separate zone for the tunnel interface. If you create a separate zone for the tunnel interface, say a VPN zone, you will need to create security policies to enable traffic to flow between the VPN zone and the trust zone.

To route traffic between the sites, a tunnel interface does not require an IP address. An IP address is only required if you want to enable tunnel monitoring or if you are using a dynamic routing protocol to route traffic across the tunnel. With dynamic routing, the tunnel IP address serves as the next hop IP address for routing traffic to the VPN tunnel.

If you are configuring the Palo Alto Networks firewall with a VPN peer that performs policy-based VPN, you must configure a local and remote Proxy ID when setting up the IPSec tunnel. Each peer compares the Proxy-IDs configured on it with what is actually received in the packet in order to allow a successful IKE phase 2 negotiation. If multiple tunnels are required, configure unique Proxy IDs for each tunnel interface; a tunnel interface can have a maximum of 250 Proxy IDs. Each Proxy ID counts towards the IPSec VPN tunnel capacity of the firewall, and the tunnel capacity varies by the firewall model.

See [Set Up an IPSec Tunnel](#) for configuration details.

## Tunnel Monitoring

For a VPN tunnel, you can check connectivity to a destination IP address across the tunnel. The network monitoring profile on the firewall allows you to verify connectivity (using ICMP) to a destination IP address or a next hop at a specified polling interval, and to specify an action on failure to access the monitored IP address.

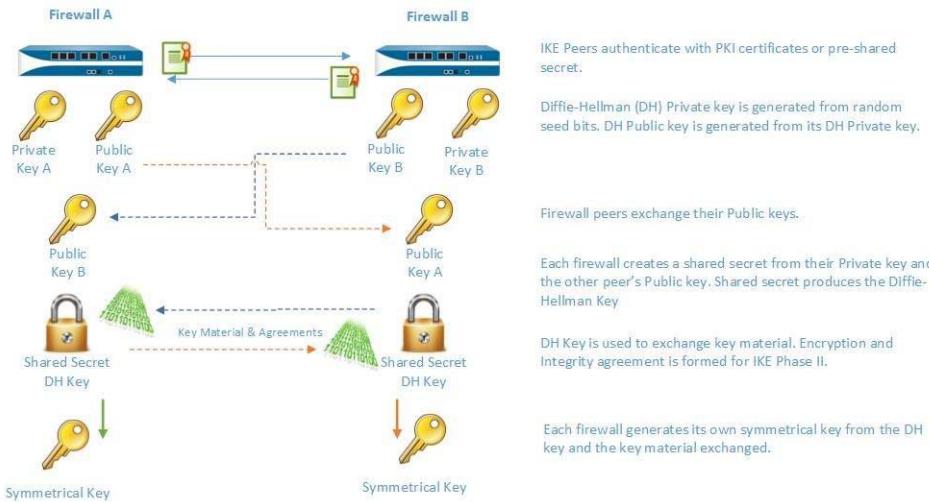
If the destination IP is unreachable, you either configure the firewall to wait for the tunnel to recover or configure automatic failover to another tunnel. In either case, the firewall generates a system log that alerts you to a tunnel failure and renegotiates the IPSec keys to accelerate recovery.

The default monitoring profile is configured to wait for the tunnel to recover; the polling interval is 3 seconds and the failure threshold is 5.

See [Set Up Tunnel Monitoring](#) for configuration details.

## Internet Key Exchange (IKE) for VPN

The IKE process allows the VPN peers at both ends of the tunnel to encrypt and decrypt packets using mutually agreed-upon keys or certificate and method of encryption. The IKE process occurs in two phases: [IKE Phase 1](#) and [IKE Phase 2](#). Each of these phases use keys and encryption algorithms that are defined using cryptographic profiles—IKE crypto profile and IPSec crypto profile—and the result of the IKE negotiation is a Security Association (SA). An SA is a set of mutually agreed-upon keys and algorithms that are used by both VPN peers to allow the flow of data across the VPN tunnel. The following illustration depicts the key exchange process for setting up the VPN tunnel:



## IKE Phase 1

In this phase, the firewalls use the parameters defined in the IKE Gateway configuration and the IKE Crypto profile to authenticate each other and set up a secure control channel. IKE Phase supports the use of preshared keys or digital certificates (which use public key infrastructure, PKI) for mutual authentication of the VPN peers. Preshared keys are a simple solution for securing smaller networks because they do not require the support of a PKI infrastructure. Digital certificates can be more convenient for larger networks or implementations that require stronger authentication security.

When using certificates, make sure that the CA issuing the certificate is trusted by both gateway peers and that the maximum length of certificates in the certificate chain is 5 or less. With IKE fragmentation enabled, the firewall can reassemble IKE messages with up to 5 certificates in the certificate chain and successfully establish a VPN tunnel.

The IKE Crypto profile defines the following options that are used in the IKE SA negotiation:

- Diffie-Hellman (DH) group for generating symmetrical keys for IKE.  
The Diffie-Hellman algorithm uses the private key of one party and the public key of the other to create a shared secret, which is an encrypted key that both VPN tunnel peers share. The DH groups supported on the firewall are: Group 1—768 bits, Group 2—1024 bits (default), Group 5—1536 bits, Group 14—2048 bits, Group 19—256-bit elliptic curve group, and Group 20—384-bit elliptic curve group.
- Authentication algorithms—sha1, sha 256, sha 384, sha 512, or md5
- Encryption algorithms—3des, aes-128-cbc, aes-192-cbc, or aes-256-cbc

## IKE Phase 2

After the tunnel is secured and authenticated, in Phase 2 the channel is further secured for the transfer of data between the networks. IKE Phase 2 uses the keys that were established in Phase 1 of the process and the IPSec Crypto profile, which defines the IPSec protocols and keys used for the SA in IKE Phase 2.

The IPSEC uses the following protocols to enable secure communication:

- Encapsulating Security Payload (ESP)—Allows you to encrypt the entire IP packet, and authenticate the source and verify integrity of the data. While ESP requires that you encrypt and authenticate the packet, you can choose to only encrypt or only authenticate by setting the encryption option to Null; using encryption without authentication is discouraged.
- Authentication Header (AH)—Authenticates the source of the packet and verifies data integrity. AH does not encrypt the data payload and is unsuited for deployments where data privacy is important. AH is commonly used when the main concern is to verify the legitimacy of the peer, and data privacy is not required.

**Table: Algorithms Supported for IPSEC Authentication and Encryption**

ESP	AH
Diffie Hellman (DH) exchange options supported	
<ul style="list-style-type: none"> <li>• Group 1—768 bits</li> <li>• Group 2—1024 bits (the default)</li> <li>• Group 5—1536 bits</li> <li>• Group 14—2048 bits.</li> <li>• Group 19— 256-bit elliptic curve group</li> <li>• Group 20—384-bit elliptic curve group</li> <li>• no-pfs—By default, perfect forward secrecy (PFS) is enabled, which means a new DH key is generated in IKE phase 2 using one of the groups listed above. This key is independent of the keys exchanged in IKE phase1 and provides better data transfer security. If you select no-pfs, the DH key created at phase 1 is not renewed and a single key is used for the IPsec SA negotiations. Both VPN peers must be enabled or disabled for PFS.</li> </ul>	
Encryption algorithms supported	
• 3des	Triple Data Encryption Standard (3DES) with a security strength of 112 bits
• aes-128-cbc	Advanced Encryption Standard (AES) using cipher block chaining (CBC) with a security strength of 128 bits
• aes-192-cbc	AES using CBC with a security strength of 192 bits
• aes-256-cbc	AES using CBC with a security strength of 256 bits
• aes-128-ccm	AES using Counter with CBC-MAC (CCM) with a security strength of 128 bits
• aes-128-gcm	AES using Galois/Counter Mode (GCM) with a security strength of 128 bits
• aes-256-gcm	AES using GCM with a security strength of 256 bits
Authentication algorithms supported	
• md5	• md5

ESP	AH
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• sha512	• sha 512

## Methods of Securing IPSec VPN Tunnels (IKE Phase 2)

IPSec VPN tunnels can be secured using manual keys or auto keys. In addition, IPSec configuration options include Diffie-Hellman Group for key agreement, and/or an encryption algorithm and a hash for message authentication.

- **Manual Key**—Manual key is typically used if the Palo Alto Networks firewall is establishing a VPN tunnel with a legacy device, or if you want to reduce the overhead of generating session keys. If using manual keys, the same key must be configured on both peers.  
Manual keys are not recommended for establishing a VPN tunnel because the session keys can be compromised when relaying the key information between the peers; if the keys are compromised, the data transfer is no longer secure.
- **Auto Key**— Auto Key allows you to automatically generate keys for setting up and maintaining the IPSec tunnel based on the algorithms defined in the IPSec Crypto profile.

## IKEv2

An IPSec VPN gateway uses IKEv1 or [IKEv2](#) to negotiate the IKE security association (SA) and IPSec tunnel. IKEv2 is defined in [RFC 5996](#).

Unlike IKEv1, which uses Phase 1 SA and Phase 2 SA, IKEv2 uses a child SA for Encapsulating Security Payload (ESP) or Authentication Header (AH), which is set up with an IKE SA.

NAT traversal (NAT-T) must be enabled on both gateways if you have NAT occurring on a device that sits between the two gateways. A gateway can see only the public (globally routable) IP address of the NAT device.

IKEv2 provides the following benefits over IKEv1:

- Tunnel endpoints exchange fewer messages to establish a tunnel. IKEv2 uses four messages; IKEv1 uses either nine messages (in main mode) or six messages (in aggressive mode).
- Built-in NAT-T functionality improves compatibility between vendors.
- Built-in health check automatically re-establishes a tunnel if it goes down. The liveness check replaces the Dead Peer Detection used in IKEv1.
- Supports traffic selectors (one per exchange). The traffic selectors are used in IKE negotiations to control what traffic can access the tunnel.

- Supports Hash and URL certificate exchange to reduce fragmentation.
- Resiliency against DoS attacks with improved peer validation. An excessive number of half-open SAs can trigger cookie validation.

Before configuring IKEv2, you should be familiar with the following concepts:

- ▲ [Liveness Check](#)
- ▲ [Cookie Activation Threshold and Strict Cookie Validation](#)
- ▲ [Traffic Selectors](#)
- ▲ [Hash and URL Certificate Exchange](#)
- ▲ [SA Key Lifetime and Re-Authentication Interval](#)

After you [Set Up an IKE Gateway](#), if you chose IKEv2, perform the following optional tasks related to IKEv2 as required by your environment:

- ▲ [Export a Certificate for a Peer to Access Using Hash and URL](#)
- ▲ [Import a Certificate for IKEv2 Gateway Authentication](#)
- ▲ [Change the Key Lifetime or Authentication Interval for IKEv2](#)
- ▲ [Change the Cookie Activation Threshold for IKEv2](#)
- ▲ [Configure IKEv2 Traffic Selectors](#)

## Liveness Check

The liveness check for IKEv2 is similar to Dead Peer Detection (DPD), which IKEv1 uses as the way to determine whether a peer is still available.

In IKEv2, the liveness check is achieved by any IKEv2 packet transmission or an empty informational message that the gateway sends to the peer at a configurable interval, five seconds by default. If necessary, the sender attempts the retransmission up to ten times. If it doesn't get a response, the sender closes and deletes the IKE\_SA and corresponding CHILD\_SAs. The sender will start over by sending out another IKE\_SA\_INIT message.

## Cookie Activation Threshold and Strict Cookie Validation

Cookie validation is always enabled for IKEv2; it helps protect against half-SA DoS attacks. You can configure the global threshold number of half-open SAs that will trigger cookie validation. You can also configure individual IKE gateways to enforce cookie validation for every new IKEv2 SA.

- The **Cookie Activation Threshold** is a global VPN session setting that limits the number of simultaneous half-opened IKE SAs (default is 500). When the number of half-opened IKE SAs exceeds the **Cookie Activation Threshold**, the Responder will request a cookie, and the Initiator must respond with an IKE\_SA\_INIT containing a cookie to validate the connection. If the cookie validation is successful, another SA can be initiated. A value of 0 means that cookie validation is always on.

The Responder does not maintain a state of the Initiator, nor does it perform a Diffie-Hellman key exchange, until the Initiator returns the cookie. IKEv2 cookie validation mitigates a DoS attack that would try to leave numerous connections half open.

The **Cookie Activation Threshold** must be lower than the **Maximum Half Opened SA** setting. If you [Change the Cookie Activation Threshold for IKEv2](#) to a very high number (for example, 65534) and the **Maximum Half Opened SA** setting remained at the default value of 65535, cookie validation is essentially disabled.

- You can enable **Strict Cookie Validation** if you want cookie validation performed for every new IKEv2 SA a gateway receives, regardless of the global threshold. **Strict Cookie Validation** affects only the IKE gateway being configured and is disabled by default. If **Strict Cookie Validation** is disabled, the system uses the **Cookie Activation Threshold** to determine whether a cookie is needed or not.

## Traffic Selectors

In IKEv1, a firewall that has a route-based VPN needs to use a local and remote Proxy ID in order to set up an IPSec tunnel. Each peer compares its Proxy IDs with what it received in the packet in order to successfully negotiate IKE Phase 2. IKE Phase 2 is about negotiating the SAs to set up an IPSec tunnel. (For more information on Proxy IDs, see [Tunnel Interface](#).)

In IKEv2, you can [Configure IKEv2 Traffic Selectors](#), which are components of network traffic that are used during IKE negotiation. Traffic selectors are used during the CHILD\_SA (tunnel creation) Phase 2 to set up the tunnel and to determine what traffic is allowed through the tunnel. The two IKE gateway peers must negotiate and agree on their traffic selectors; otherwise, one side narrows its address range to reach agreement. One IKE connection can have multiple tunnels; for example, you can assign different tunnels to each department to isolate their traffic. Separation of traffic also allows features such as QoS to be implemented.

The IPv4 and IPv6 traffic selectors are:

- **Source IP address**—A network prefix, address range, specific host, or wildcard.
- **Destination IP address**—A network prefix, address range, specific host, or wildcard.
- **Protocol**—A transport protocol, such as TCP or UDP.
- **Source port**—The port where the packet originated.
- **Destination port**—The port the packet is destined for.

During IKE negotiation, there can be multiple traffic selectors for different networks and protocols. For example, the Initiator might indicate that it wants to send TCP packets from 172.168.0.0/16 through the tunnel to its peer, destined for 198.5.0.0/16. It also wants to send UDP packets from 172.17.0.0/16 through the same tunnel to the same gateway, destined for 0.0.0.0 (any network). The peer gateway must agree to these traffic selectors so that it knows what to expect.

It is possible that one gateway will start negotiation using a traffic selector that is a more specific IP address than the IP address of the other gateway.

- For example, gateway A offers a source IP address of 172.16.0.0/16 and a destination IP address of 192.16.0.0/16. But gateway B is configured with 0.0.0.0 (any source) as the source IP address and 0.0.0.0 (any destination) as the destination IP address. Therefore, gateway B narrows down its source IP address to 192.16.0.0/16 and its destination address to 172.16.0.0/16. Thus, the narrowing down accommodates the addresses of gateway A and the traffic selectors of the two gateways are in agreement.
- If gateway B (configured with source IP address 0.0.0.0) is the Initiator instead of the Responder, gateway A will respond with its more specific IP addresses, and gateway B will narrow down its addresses to reach agreement.

## Hash and URL Certificate Exchange

IKEv2 supports Hash and URL Certificate Exchange, which is used during an IKEv2 negotiation of an SA. You store the certificate on an HTTP server, which is specified by a URL. The peer fetches the certificate from the server based on receiving the URL to the server. The hash is used to check whether the content of the certificate is valid or not. Thus, the two peers exchange certificates with the HTTP CA rather than with each other.

The hash part of Hash and URL reduces the message size and thus Hash and URL is a way to reduce the likelihood of packet fragmentation during IKE negotiation. The peer receives the certificate and hash that it expects, and thus IKE Phase 1 has validated the peer. Reducing fragmentation occurrences helps protect against DoS attacks.

You can enable the Hash and URL certificate exchange when configuring an IKE gateway by selecting **HTTP Certificate Exchange** and entering the **Certificate URL**. The peer must also use Hash and URL certificate exchange in order for the exchange to be successful. If the peer cannot use Hash and URL, X.509 certificates are exchanged similarly to how they are exchanged in IKEv1.

If you enable the Hash and URL certificate exchange, you must export your certificate to the certificate server if it is not already there. When you export the certificate, the file format should be **Binary Encoded Certificate (DER)**. See [Export a Certificate for a Peer to Access Using Hash and URL](#).

## SA Key Lifetime and Re-Authentication Interval

In IKEv2, two IKE crypto profile values, **Key Lifetime** and **IKEv2 Authentication Multiple**, control the establishment of IKEv2 IKE SAs. The key lifetime is the length of time that a negotiated IKE SA key is effective. Before the key lifetime expires, the SA must be re-keyed; otherwise, upon expiration, the SA must begin a new IKEv2 IKE SA re-key. The default value is 8 hours.

The re-authentication interval is derived by multiplying the **Key Lifetime** by the **IKEv2 Authentication Multiple**. The authentication multiple defaults to 0, which disables the re-authentication feature.

The range of the authentication multiple is 0-50. So, if you were to configure an authentication multiple of 20, for example, the system would perform re-authentication every 20 re-keys, which is every 160 hours. That means the gateway could perform Child SA creation for 160 hours before the gateway must re-authenticate with IKE to recreate the IKE SA from scratch.

In IKEv2, the Initiator and Responder gateways have their own key lifetime value, and the gateway with the shorter key lifetime is the one that will request that the SA be re-keyed.

## Set Up Site-to-Site VPN

To set up site-to-site VPN:

- Make sure that your Ethernet interfaces, virtual routers, and zones are configured properly. For more information, see [Configure Interfaces and Zones](#).
- Create your tunnel interfaces. Ideally, put the tunnel interfaces in a separate zone, so that tunneled traffic can use different policies.
- Set up static routes or assign routing protocols to redirect traffic to the VPN tunnels. To support dynamic routing (OSPF, BGP, RIP are supported), you must assign an IP address to the tunnel interface.
- Define IKE gateways for establishing communication between the peers across each end of the VPN tunnel; also define the cryptographic profile that specifies the protocols and algorithms for identification, authentication, and encryption to be used for setting up VPN tunnels in IKEv1 Phase 1. See [Set Up an IKE Gateway](#) and [Define IKE Crypto Profiles](#).
- Configure the parameters that are needed to establish the IPSec connection for transfer of data across the VPN tunnel; See [Set Up an IPSec Tunnel](#). For IKEv1 Phase-2, see [Define IPSec Crypto Profiles](#).
- (Optional) Specify how the firewall will monitor the IPSec tunnels. See [Set Up Tunnel Monitoring](#).
- Define security policies to filter and inspect the traffic.



If there is a deny rule at the end of the security rulebase, intra-zone traffic is blocked unless otherwise allowed. Rules to allow IKE and IPSec applications must be explicitly included above the deny rule.

When these tasks are complete, the tunnel is ready for use. Traffic destined for the zones/addresses defined in policy is automatically routed properly based on the destination route in the routing table, and handled as VPN traffic. For a few examples on site-to-site VPN, see [Site-to-Site VPN Quick Configs](#).

For troubleshooting purposes, you can [Enable/Disable, Refresh or Restart an IKE Gateway or IPSec Tunnel](#).

## Set Up an IKE Gateway

To set up a VPN tunnel, the VPN peers or gateways must authenticate each other using preshared keys or digital certificates and establish a secure channel in which to negotiate the IPSec security association (SA) that will be used to secure traffic between the hosts on each side.

<b>Set Up an IKE Gateway</b>	
Step 1 Define the IKE Gateway.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Network Profiles &gt; IKE Gateways</b>, click <b>Add</b>, and on the <b>General</b> tab, enter the <b>Name</b> of the gateway.</li><li>2. For <b>Version</b>, select <b>IKEv1 only mode</b>, <b>IKEv2 only mode</b>, or <b>IKEv2 preferred mode</b>. The IKE gateway begins its negotiation with its peer in the mode specified here. If you select <b>IKEv2 preferred mode</b>, the two peers will use IKEv2 if the remote peer supports it; otherwise they will use IKEv1. (The <b>Version</b> selection also determines which options are available on the <b>Advanced Options</b> tab.)</li></ol>
Step 2 Establish the local endpoint of the tunnel (gateway).	<ol style="list-style-type: none"><li>1. For <b>Address Type</b>, click <b>IPv4</b> or <b>IPv6</b>.</li><li>2. Select the physical, outgoing <b>Interface</b> on the firewall where the local gateway resides.</li><li>3. From the <b>Local IP Address</b> drop-down, select the IP address that will be used as the endpoint for the VPN connection. This is the external-facing interface with a publicly routable IP address on the firewall.</li></ol>
Step 3 Establish the peer at the far end of the tunnel (gateway).	<ol style="list-style-type: none"><li>1. Select the <b>Peer IP Type</b> to be a <b>Static</b> or <b>Dynamic</b> address assignment.</li><li>2. If the <b>Peer IP Address</b> is static, enter the IP address of the peer.</li></ol>
Step 4 Specify how the peer is authenticated.	Select the <b>Authentication</b> method: <b>Pre-Shared Key</b> or <b>Certificate</b> . If you choose Pre-Shared Key, proceed to <a href="#">Step 5</a> . If you choose Certificate, proceed to <a href="#">Step 6</a> .

## Set Up an IKE Gateway

<p><b>Step 5</b> Configure a pre-shared key.</p>	<ol style="list-style-type: none"><li>1. Enter a <b>Pre-shared Key</b>, which is the security key to use for authentication across the tunnel. Re-enter the value to <b>Confirm Pre-shared Key</b>.  Generate a key that is difficult to crack with dictionary attacks; use a pre-shared key generator, if necessary.</li><li>2. For <b>Local Identification</b>, choose from the following types and enter a value that you determine: <b>FQDN (hostname)</b>, <b>IP address</b>, <b>KEYID (binary format ID string in HEX)</b>, <b>User FQDN (email address)</b>. Local identification defines the format and identification of the local gateway. If no value is specified, the local IP address will be used as the local identification value.</li><li>3. For <b>Peer Identification</b>, choose from the following types and enter the value: <b>FQDN (hostname)</b>, <b>IP address</b>, <b>KEYID (binary format ID string in HEX)</b>, <b>User FQDN (email address)</b>. Peer identification defines the format and identification of the peer gateway. If no value is specified, the peer IP address will be used as the peer identification value.</li><li>4. Proceed to <a href="#">Step 7</a> and continue from there.</li></ol>
--	--

## Set Up an IKE Gateway

<p><b>Step 6</b> Configure certificate-based authentication. Perform the remaining steps in this procedure if you selected <b>Certificate</b> as the method of authenticating the peer gateway at the opposite end of the tunnel.</p>	<ol style="list-style-type: none"><li>1. Select a <b>Local Certificate</b> that is already on the firewall from the drop-down, or <b>Import</b> a certificate, or <b>Generate</b> to create a new certificate.<ul style="list-style-type: none"><li>• If you want to <b>Import</b> a certificate, <a href="#">Import a Certificate for IKEv2 Gateway Authentication</a> and then return to this task.</li><li>• If you want to <b>Generate</b> a new certificate, <a href="#">Generate a Certificate on the Device</a> and then return to this task.</li></ul></li><li>2. Click the <b>HTTP Certificate Exchange</b> check box if you want to configure Hash and URL (IKEv2 only). For an HTTP certificate exchange, enter the <b>Certificate URL</b>. For more information, see <a href="#">Hash and URL Certificate Exchange</a>.</li><li>3. Select the <b>Local Identification</b> type from the following: <b>Distinguished Name (Subject)</b>, <b>FQDN (hostname)</b>, <b>IP address</b>, <b>User FQDN (email address)</b>, and enter the value. Local identification defines the format and identification of the local gateway.</li><li>4. Select the <b>Peer Identification</b> type from the following: <b>Distinguished Name (Subject)</b>, <b>FQDN (hostname)</b>, <b>IP address</b>, <b>User FQDN (email address)</b>, and enter the value. Peer identification defines the format and identification of the peer gateway.</li><li>5. Select one type of <b>Peer ID Check</b>:<ul style="list-style-type: none"><li>• <b>Exact</b>—Check this to ensure that the local setting and peer IKE ID payload match exactly.</li><li>• <b>Wildcard</b>—Check this to allow the peer identification to match as long as every character before the wildcard (*) matches. The characters after the wildcard need not match.</li></ul></li><li>6. Click <b>Permit peer identification and certificate payload identification mismatch</b> if you want to allow a successful IKE SA even when the peer identification does not match the peer identification in the certificate.</li><li>7. Choose a <b>Certificate Profile</b> from the drop-down. A certificate profile contains information about how to authenticate the peer gateway.</li><li>8. Click <b>Enable strict validation of peer's extended key use</b> if you want to strictly control how the key can be used.</li></ol>
---	--

## Set Up an IKE Gateway

<p><b>Step 7</b> Configure advanced options for the gateway.</p>	<ol style="list-style-type: none"><li>1. Select the <b>Advanced Options</b> tab.</li><li>2. In the Common Options section, <b>Enable Passive Mode</b> if you want the firewall to only respond to IKE connection requests and never initiate them.</li><li>3. <b>Enable NAT Traversal</b> if you have a device performing NAT between the gateways, to have UDP encapsulation used on IKE and UDP protocols, enabling them to pass through intermediate NAT devices.</li><li>4. If you chose <b>IKEv1 only mode</b> earlier, on the IKEv1 tab:<ul style="list-style-type: none"><li>• Choose <b>auto</b>, <b>aggressive</b>, or <b>main</b> for the <b>Exchange Mode</b>. When a device is set to use <b>auto</b> exchange mode, it can accept both <b>main</b> mode and <b>aggressive</b> mode negotiation requests; however, whenever possible, it initiates negotiation and allows exchanges in <b>main</b> mode.  If the exchange mode is not set to <b>auto</b>, you must configure both peers with the same exchange mode to allow each peer to accept negotiation requests.</li><li>• Select an existing profile or keep the default profile from <b>IKE Crypto Profile</b> drop-down. For details on defining an IKE Crypto profile, see <a href="#">Define IKE Crypto Profiles</a>.</li><li>• (Only if using certificate-based authentication and the exchange mode is not set to <b>aggressive</b> mode) Click <b>Enable Fragmentation</b> to enable the firewall to operate with IKE Fragmentation.</li><li>• Click <b>Dead Peer Detection</b> and enter an <b>Interval</b> (range is 2-100 seconds). For <b>Retry</b>, define the time to delay (range is 2-100 seconds) before attempting to re-check availability. Dead peer detection identifies inactive or unavailable IKE peers by sending an IKE phase 1 notification payload to the peer and waiting for an acknowledgment.</li></ul></li><li>5. If you chose <b>IKEv2 only mode</b> or <b>IKEv2 preferred mode</b> in <a href="#">Step 1</a>, on the IKEv2 tab:<ul style="list-style-type: none"><li>• Select an <b>IKE Crypto Profile</b> from the drop-down, which configures IKE Phase 1 options such as the DH group, hash algorithm, and ESP authentication. For information about IKE crypto profiles, see <a href="#">IKE Phase 1</a>.</li><li>• Enable <b>Strict Cookie Validation</b> if you want to always enforce cookie validation on IKEv2 SAs for this gateway. See <a href="#">Cookie Activation Threshold and Strict Cookie Validation</a>.</li><li>• <b>Enable Liveness Check</b> and enter an <b>Interval (sec)</b> (default is 5) if you want to have the gateway send a message request to its gateway peer, requesting a response. If necessary, the Initiator attempts the liveness check up to 10 times. If it doesn't get a response, the Initiator closes and deletes the IKE_SA and CHILD_SA. The Initiator will start over by sending out another IKE_SA_INIT.</li></ul></li></ol>
--	---

**Set Up an IKE Gateway****Step 8** Save the changes.Click **OK** and **Commit**.**Export a Certificate for a Peer to Access Using Hash and URL**

IKEv2 supports [Hash and URL Certificate Exchange](#) as a method of having the peer at the remote end of the tunnel fetch the certificate from a server where you have exported the certificate. Perform this task to export your certificate to that server.

- You must have already created a certificate using **Device > Certificate Management**.

**Export a Certificate for Hash and URL**

Export a certificate for a peer to access using Hash and URL certificate exchange.

1. Select **Device > Certificates**, and if your platform supports multiple virtual systems, for **Location**, select the appropriate virtual system.
2. On the **Device Certificates** tab, select the certificate to **Export** to the server.  
 The status of the certificate should be valid, not expired. The firewall will not stop you from exporting an invalid certificate.
3. For **File Format**, select **Binary Encoded Certificate (DER)**.
4. Leave **Export private key** clear. Exporting the private key is unnecessary for Hash and URL.
5. Click **OK**.

**Import a Certificate for IKEv2 Gateway Authentication**

Perform this task if you are authenticating a peer for an IKEv2 gateway and you did not use a local certificate already on the firewall; you want to import a certificate from elsewhere.

This task presumes that you selected **Network > IKE Gateways**, added a gateway, and for **Local Certificate**, you clicked **Import**.

### Import a Certificate for IKEv2 Gateway Authentication

<p><b>Step 1</b> Import a certificate.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; IKE Gateways</b>, <b>Add</b> a gateway, and on the <b>General</b> tab, for <b>Authentication</b>, select <b>Certificate</b>. For <b>Local Certificate</b>, click <b>Import</b>.</li> <li>2. In the Import Certificate window, enter a <b>Certificate Name</b> for the certificate you are importing.</li> <li>3. Select <b>Shared</b> if this certificate is to be shared among multiple virtual systems.</li> <li>4. For <b>Certificate File</b>, <b>Browse</b> to the certificate file. Click on the file name and click <b>Open</b>, which populates the <b>Certificate File</b> field.</li> <li>5. For <b>File Format</b>, select one of the following: <ul style="list-style-type: none"> <li>• <b>Base64 Encoded Certificate (PEM)</b>—Contains the certificate, but not the key. It is cleartext.</li> <li>• <b>Encrypted Private Key and Certificate (PKCS12)</b>—Contains both the certificate and the key.</li> </ul> </li> <li>6. Select <b>Import private key</b> if the key is in a different file from the certificate file. The key is optional, with the following exception: <ul style="list-style-type: none"> <li>• You must import a key if you set the <b>File Format</b> to <b>PEM</b>. Enter a <b>Key file</b> by clicking <b>Browse</b> and navigating to the key file to import.</li> <li>• Enter a <b>Passphrase</b> and <b>Confirm Passphrase</b>.</li> </ul> </li> <li>7. Click <b>OK</b>.</li> </ol>
<p><b>Step 2</b> After you perform this task, return to Configure an IKEv2 Gateway and resume <a href="#">Step 6</a>.</p>	

### Change the Key Lifetime or Authentication Interval for IKEv2

This task is optional; the default setting of the IKEv2 IKE SA re-key lifetime is 8 hours. The default setting of the IKEv2 Authentication Multiple is 0, meaning the re-authentication feature is disabled. For more information, see [SA Key Lifetime and Re-Authentication Interval](#).

To change the default values, perform the following task. A prerequisite is that an IKE crypto profile already exists.

### Change the SA Key Lifetime or Authentication Interval

Step 1	Change the SA key lifetime or authentication interval for an IKE Crypto profile.	<ol style="list-style-type: none"><li>Select <b>Network &gt; Network Profiles &gt; IKE Crypto</b> and select the IKE Crypto profile that applies to the local gateway.</li><li>For the <b>Key Lifetime</b>, select a unit (<b>Seconds</b>, <b>Minutes</b>, <b>Hours</b>, or <b>Days</b>) and enter a value. The minimum is three minutes.</li><li>For <b>IKE Authentication Multiple</b>, enter a value, which is multiplied by the lifetime to determine the re-authentication interval.</li></ol>
Step 2	Save the configuration.	Click <b>OK</b> and <b>Commit</b> .

### Change the Cookie Activation Threshold for IKEv2

Perform the following task if you want a firewall to have a threshold different from the default setting of 500 half-opened SA sessions before cookie validation is required. For more information about cookie validation, see [Cookie Activation Threshold and Strict Cookie Validation](#).

### Change the Cookie Activation Threshold

Step 1	Change the Cookie Activation Threshold.	<ol style="list-style-type: none"><li>Select <b>Device &gt; Setup &gt; Session</b> and edit the VPN Session Settings. For <b>Cookie Activation Threshold</b>, enter the maximum number of half-opened SAs that are allowed before the responder requests a cookie from the initiator (range is 0-65535; default: is 500).</li><li>Click <b>OK</b>.</li></ol>
Step 2	Save the configuration	Click <b>OK</b> and <b>Commit</b> .

### Configure IKEv2 Traffic Selectors

#### Configure Traffic Selectors for IKEv2

Step 1	Configure Traffic Selectors.	<ol style="list-style-type: none"><li>Select <b>Network &gt; IPSec Tunnels &gt; Proxy IDs</b>.</li><li>Select the <b>IPv4</b> or <b>IPv6</b> tab.</li><li>Click <b>Add</b> and enter the <b>Name</b> in the <b>Proxy ID</b> field.</li><li>In the <b>Local</b> field, enter the <b>Source IP Address</b>.</li><li>In the <b>Remote</b> field, enter the <b>Destination IP Address</b>.</li><li>In the <b>Protocol</b> field, select the transport protocol (<b>TCP</b> or <b>UDP</b>) from the drop-down.</li><li>Click <b>OK</b>.</li></ol>
--------	------------------------------	--

## Define Cryptographic Profiles

A cryptographic profile specifies the ciphers used for authentication and/or encryption between two IKE peers, and the lifetime of the key. The time period between each renegotiation is known as the lifetime; when the specified time expires, the firewall renegotiates a new set of keys.

For securing communication across the VPN tunnel, the firewall requires IKE and IPSec cryptographic profiles for completing IKE phase 1 and phase 2 negotiations, respectively. The firewall includes a default IKE crypto profile and a default IPSec crypto profile that is ready for use.

- ▲ [Define IKE Crypto Profiles](#)
- ▲ [Define IPSec Crypto Profiles](#)

### Define IKE Crypto Profiles

The IKE crypto profile is used to set up the encryption and authentication algorithms used for the key exchange process in [IKE Phase 1](#), and lifetime of the keys, which specifies how long the keys are valid. To invoke the profile, you must attach it to the IKE Gateway configuration.



All IKE gateways configured on the same interface or local IP address must use the same crypto profile.

#### Define an IKE Crypto Profile

<b>Step 1</b> Create a new IKE profile.	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Network Profiles &gt; IKE Crypto</b> and select <b>Add</b>.</li> <li>2. Enter a <b>Name</b> for the new profile.</li> </ol>
<b>Step 2</b> Specify the DH Group (Diffie–Hellman group) for key exchange, and the Authentication and Encryption algorithms.	<p>Click <b>Add</b> in the corresponding sections (DH Group, Authentication, and Encryption) and select from the drop-downs. If you are not certain of what the VPN peers support, add multiple groups or algorithms in the order of most-to-least secure as follows; the peers negotiate the strongest supported group or algorithm to establish the tunnel:</p> <ul style="list-style-type: none"> <li>• DH Group—<b>group20, group19, group14, group5, group2, and group1</b>.</li> <li>• Authentication—<b>sha512, sha384, sha256, sha1, md5</b>.</li> <li>• Encryption—<b>aes-256-cbc, aes-192-cbc, aes-128-cbc, 3des</b>.</li> </ul>
<b>Step 3</b> Specify the duration for which the key is valid and the re-authentication interval.  For details, see <a href="#">SA Key Lifetime and Re-Authentication Interval</a> .	<ol style="list-style-type: none"> <li>1. In the <b>Key Lifetime</b> fields, specify the period (in seconds, minutes, hours, or days) for which the key is valid. (Range is 3 minutes to 365 days; default is 8 hours.) When the key expires, the firewall renegotiates a new key. A lifetime is the period between each renegotiation.</li> <li>2. For the <b>IKEv2 Authentication Multiple</b>, specify a value (range is 0-50) that is multiplied by the <b>Key Lifetime</b> to determine the authentication count. The default value of 0 disables the re-authentication feature.</li> </ol>

### Define an IKE Crypto Profile

Step 4	Save your IKE Crypto profile.	Click <b>OK</b> and click <b>Commit</b> .
Step 5	Attach the IKE Crypto profile to the IKE Gateway configuration.	See Step 7 in <a href="#">Set Up an IKE Gateway</a> .

### Define IPSec Crypto Profiles

The IPSec crypto profile is invoked in [IKE Phase 2](#). It specifies how the data is secured within the tunnel when Auto Key IKE is used to automatically generate keys for the IKE SAs.

### Define the IPSec Crypto Profile

Step 1	<p>Create a new IPSec profile.</p> <ol style="list-style-type: none"> <li>Select <b>Network &gt; Network Profiles &gt; IPSec Crypto</b> and select <b>Add</b>.</li> <li>Enter a <b>Name</b> for the new profile.</li> <li>Select the <b>IPSec Protocol</b>—ESP or AH—that you want to apply to secure the data as it traverses across the tunnel.</li> <li>Click <b>Add</b> and select the <b>Authentication</b> and <b>Encryption</b> algorithms for ESP, and <b>Authentication</b> algorithms for AH, so that the IKE peers can negotiate the keys for the secure transfer of data across the tunnel.</li> </ol> <p>If you are not certain of what the IKE peers support, add multiple algorithms in the order of most-to-least secure as follows; the peers negotiate the strongest supported algorithm to establish the tunnel:</p> <ul style="list-style-type: none"> <li>Encryption—<b>aes-256-gcm, aes-256-cbc, aes-192-cbc, aes-128-gcm, aes-128-ccm</b> (the VM-Series firewall doesn't support this option), <b>aes-128-cbc, 3des</b>.</li> <li>Authentication—<b>sha512, sha384, sha256, sha1, md5</b>.</li> </ul>
Step 2	<p>Select the DH Group to use for the IPSec SA negotiations in IKE phase 2.</p> <p>Select the key strength that you want to use from the <b>DH Group</b> drop-down.</p> <p>If you are not certain of what the VPN peers support, add multiple groups in the order of most-to-least secure as follows; the peers negotiate the strongest supported group to establish the tunnel: <b>group20, group19, group14, group5, group2, and group1</b>.</p> <p>Select <b>no-pfs</b> if you do not want to renew the key that was created at phase 1; the current key is reused for the IPSEC SA negotiations.</p>

Define the IPSec Crypto Profile	
Step 3	Specify the duration of the key—time and volume of traffic.
	<p>Using a combination of time and traffic volume allows you to ensure safety of data.</p> <p>Select the <b>Lifetime</b> or time period for which the key is valid in seconds, minutes, hours, or days (range is 3 minutes to 365 days). When the specified time expires, the firewall will renegotiate a new set of keys.</p> <p>Select the <b>Lifesize</b> or volume of data after which the keys must be renegotiated.</p>
Step 4	Save your IPSec profile.
Step 5	Attach the IPSec Profile to an IPSec tunnel configuration.

## Set Up an IPSec Tunnel

The IPSec tunnel configuration allows you to authenticate and/or encrypt the data (IP packet) as it traverses across the tunnel.

If you are setting up the Palo Alto Networks firewall to work with a peer that supports policy-based VPN, you must define Proxy IDs. Devices that support policy-based VPN use specific security rules/policies or access-lists (source addresses, destination addresses and ports) for permitting interesting traffic through an IPSec tunnel. These rules are referenced during quick mode/IKE phase 2 negotiation, and are exchanged as Proxy-IDs in the first or the second message of the process. So, if you are configuring the Palo Alto Networks firewall to work with a policy-based VPN peer, for a successful phase 2 negotiation you must define the Proxy-ID so that the setting on both peers is identical. If the Proxy-ID is not configured, because the Palo Alto Networks firewall supports route-based VPN, the default values used as Proxy-ID are source ip: 0.0.0.0/0, destination ip: 0.0.0.0/0 and application: any; and when these values are exchanged with the peer, it results in a failure to set up the VPN connection.

### Set Up an IPSec Tunnel

**Step 1** Select **Network > IPSec Tunnels > General** and enter a **Name** for the new tunnel.

**Step 2** Select the **Tunnel interface** that will be used to set up the IPSec tunnel.

To create a new tunnel interface:

1. Select **Network > Interfaces > Tunnel** and click **Add**.
2. In the **Interface Name** field, specify a numeric suffix, such as **.2**.
3. On the **Config** tab, expand the **Security Zone** drop-down to define the zone as follows:
  - To use your trust zone as the termination point for the tunnel, select the zone from the drop-down. Associating the tunnel interface with the same zone (and virtual router) as the external-facing interface on which the packets enter the firewall, mitigates the need to create inter-zone routing.
  - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for new zone (for example **vpn-corp**), and click **OK**.
4. In the **Virtual Router** drop-down, select **default**.
5. (Optional) If you want to assign an IPv4 address to the tunnel interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example **10.31.32.1/32**.
6. If you want to assign an IPv6 address to the tunnel interface, see [Step 3](#).
7. To save the interface configuration, click **OK**.

Set Up an IPSec Tunnel	
Step 3 (Optional) Enable IPv6 on the tunnel interface.	<ol style="list-style-type: none"><li>1. Select the IPv6 tab on <b>Network &gt; Interfaces &gt; Tunnel &gt; IPv6</b>.</li><li>2. Select the check box to <b>Enable IPv6 on the interface</b>. This option allows you to route IPv6 traffic over an IPv4 IPSec tunnel and will provide confidentiality between IPv6 networks. The IPv6 traffic is encapsulated by IPv4 and then ESP. To route IPv6 traffic to the tunnel, you can use a static route to the tunnel, or use OSPFv3, or use a Policy-Based Forwarding (PBF) rule to direct traffic to the tunnel.</li><li>3. Enter the 64-bit extended unique <b>Interface ID</b> in hexadecimal format, for example, 00:26:08:FF:FE:DE:4E:29. By default, the firewall will use the EUI-64 generated from the physical interface's MAC address.</li><li>4. To enter an IPv6 <b>Address</b>, click <b>Add</b> and enter an IPv6 address and prefix length, for example 2001:400:f00::1/64. If <b>Prefix</b> is not selected, the IPv6 address assigned to the interface will be wholly specified in the address text box.<ol style="list-style-type: none"><li>a. Select <b>Use interface ID as host portion</b> to assign an IPv6 address to the interface that will use the interface ID as the host portion of the address.</li><li>b. Select <b>Anycast</b> to include routing through the nearest node.</li></ol></li></ol>
Step 4 Select the type of key that will be used to secure the IPSec tunnel.	Continue to one of the following steps, depending on what type of key exchange you are using: <ul style="list-style-type: none"><li>• Set up Auto Key exchange.</li><li>• Set up a Manual Key exchange.</li></ul>
• Set up Auto Key exchange.	<ol style="list-style-type: none"><li>1. Select the IKE Gateway. To set up an IKE gateway, see <a href="#">Set Up an IKE Gateway</a>.</li><li>2. (Optional) Select the default IPSec Crypto Profile. To create a new IPSec Profile, see <a href="#">Define IPSec Crypto Profiles</a>.</li></ol>

Set Up an IPSec Tunnel	
<ul style="list-style-type: none"> <li>• Set up a Manual Key exchange.</li> </ul>	<ol style="list-style-type: none"> <li>1. Set up the parameters for the local firewall:             <ol style="list-style-type: none"> <li>a. Specify the <b>SPI</b> for the local firewall. SPI is a 32-bit hexadecimal index that is added to the header for IPSec tunneling to assist in differentiating between IPSec traffic flows; it is used to create the SA required for establishing a VPN tunnel.</li> <li>b. Select the <b>Interface</b> that will be the tunnel endpoint, and optionally select the IP address for the local interface that is the endpoint of the tunnel.</li> <li>c. Select the protocol to be used—<b>AH</b> or <b>ESP</b>.</li> <li>d. For AH, select the <b>Authentication</b> method from the drop-down and enter a <b>Key</b> and then <b>Confirm Key</b>.</li> <li>e. For ESP, select the <b>Authentication</b> method from the drop-down and enter a <b>Key</b> and then <b>Confirm Key</b>. Then, select the <b>Encryption</b> method and enter a <b>Key</b> and then <b>Confirm Key</b>, if needed.</li> </ol> </li> <li>2. Set up the parameters that pertain to the remote VPN peer.             <ol style="list-style-type: none"> <li>a. Specify the <b>SPI</b> for the remote peer.</li> <li>b. Enter the <b>Remote Address</b>, the IP address of the remote peer.</li> </ol> </li> </ol>
<p><b>Step 5</b> Protect against a replay attack.</p> <p>A replay attack occurs when a packet is maliciously intercepted and retransmitted by the interceptor.</p>	Select the <b>Show Advanced Options</b> check box, select <b>Enable Replay Protection</b> to detect and neutralize against replay attacks.
<p><b>Step 6</b> Preserve the Type of Service header for the priority or treatment of IP packets.</p>	In the <b>Show Advanced Options</b> section, select <b>Copy TOS Header</b> . This copies the Type of Service (TOS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information.
<p><b>Step 7</b> Enable Tunnel Monitoring.</p> <p> You need to assign an IP address to the tunnel interface for monitoring.</p>	<p>To alert the device administrator to tunnel failures and to provide automatic failover to another tunnel interface:</p> <ol style="list-style-type: none"> <li>1. Specify a <b>Destination IP</b> address on the other side of the tunnel to determine if the tunnel is working properly.</li> <li>2. Select a <b>Profile</b> to determine the action on tunnel failure. To create a new profile, see <a href="#">Define a Tunnel Monitoring Profile</a>.</li> </ol>

Set Up an IPSec Tunnel	
Step 8 (Required only if the VPN peer uses policy-based VPN). Create a Proxy ID to identify the VPN peers.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; IPSec Tunnels</b> and click <b>Add</b>.</li><li>2. Select the <b>Proxy IDs</b> tab.</li><li>3. Select the <b>IPv4</b> or <b>IPv6</b> tab.</li><li>4. Click <b>Add</b> and enter the <b>Proxy ID</b> name.</li><li>5. Enter the <b>Local</b> IP address or subnet for the VPN gateway.</li><li>6. Enter the <b>Remote</b> address for the VPN gateway.</li><li>7. Select the <b>Protocol</b> from the drop-down:<ul style="list-style-type: none"><li>• <b>Number</b>—Specify the protocol number (used for interoperability with third-party devices).</li><li>• <b>Any</b>—Allows TCP and/or UDP traffic.</li><li>• <b>TCP</b>—Specify the Local Port and Remote Port numbers.</li><li>• <b>UDP</b>—Specify the Local Port and Remote Port numbers.</li></ul></li><li>8. Click <b>OK</b>.</li></ol>
Step 9 Save your changes.	Click <b>OK</b> and <b>Commit</b> .

## Set Up Tunnel Monitoring

To provide uninterrupted VPN service, you can use the Dead Peer Detection capability along with the tunnel monitoring capability on the firewall. You can also monitor the status of the tunnel. These monitoring tasks are described in the following sections:

- ▲ [Define a Tunnel Monitoring Profile](#)
- ▲ [View the Status of the Tunnels](#)

### Define a Tunnel Monitoring Profile

A tunnel monitoring profile allows you to verify connectivity between the VPN peers; you can configure the tunnel interface to ping a destination IP address at a specified interval and specify the action if the communication across the tunnel is broken.

#### Define a Tunnel Monitoring Profile

1. Select **Network > Network Profiles > Monitor**. A default tunnel monitoring profile is available for use.
2. Click **Add**, and enter a **Name** for the profile.
3. Select the **Action** if the destination IP address is unreachable.
  - **Wait Recover**—the firewall waits for the tunnel to recover. It continues to use the tunnel interface in routing decisions as if the tunnel were still active.
  - **Fail Over**—forces traffic to a back-up path if one is available. The firewall disables the tunnel interface, and thereby disables any routes in the routing table that use the interface.In either case, the firewall attempts to accelerate the recovery by negotiating new IPSec keys.
4. Specify the **Interval** and **Threshold** to trigger the specified action.  
The threshold specifies the number of heartbeats to wait before taking the specified action. The range is 2-100 and the default is 5.  
The Interval measures the time between heartbeats. The range is 2-10 and the default is 3 seconds.
5. Attach the monitoring profile to the IPsec Tunnel configuration. See [Enable Tunnel Monitoring](#).

### View the Status of the Tunnels

The status of the tunnel informs you about whether or not valid IKE phase-1 and phase-2 SAs have been established, and whether the tunnel interface is up and available for passing traffic.

Because the tunnel interface is a logical interface, it cannot indicate a physical link status. Therefore, you must enable tunnel monitoring so that the tunnel interface can verify connectivity to an IP address and determine if the path is still usable. If the IP address is unreachable, the firewall will either wait for the tunnel to recover or failover. When a failover occurs, the existing tunnel is torn down and routing changes are triggered to set up a new tunnel and redirect traffic.

**View Tunnel Status**

1. Select **Network > IPSec Tunnels**.
2. View the **Tunnel Status**.
  - Green indicates a valid IPSec SA tunnel.
  - Red indicates that IPSec SA is not available or has expired.
3. View the **IKE Gateway Status**.
  - Green indicates a valid IKE phase-1 SA.
  - Red indicates that IKE phase-1 SA is not available or has expired.
4. View the **Tunnel Interface Status**.
  - Green indicates that the tunnel interface is up.
  - Red indicates that the tunnel interface is down, because tunnel monitoring is enabled and the status is down.

To troubleshoot a VPN tunnel that is not yet up, see [Interpret VPN Error Messages](#).

**Enable/Disable, Refresh or Restart an IKE Gateway or IPSec Tunnel**

You can enable, disable, refresh or restart an IKE gateway or VPN tunnel to make troubleshooting easier.

**Enable or Disable an IKE Gateway or Tunnel**

Enable or disable an IKE gateway.	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Network Profiles &gt; IKE Gateways</b> and select the gateway you want to enable or disable.</li> <li>2. At the bottom of the screen, click <b>Enable or Disable</b>.</li> </ol>
Enable or disable an IPSec tunnel.	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; IPSec Tunnels</b> and select the tunnel you want to enable or disable.</li> <li>2. At the bottom of the screen, click <b>Enable or Disable</b>.</li> </ol>

The refresh and restart behaviors for an IKE gateway and IPSec tunnel are as follows:

	<b>Refresh</b>	<b>Restart</b>
IKE Gateway (IKE Phase 1)	Updates the onscreen statistics for the selected IKE gateway. Equivalent to issuing a second <code>show</code> command in the CLI (after an initial <code>show</code> command).	Restarts the selected IKE gateway. <b>IKEv2:</b> Also restarts any associated child IPSec security associations (SAs). <b>IKEv1:</b> Does not restart the associated IPSec SAs. A restart is disruptive to all existing sessions. Equivalent to issuing a <code>clear</code> , <code>test</code> , <code>show</code> command sequence in the CLI.

	<b>Refresh</b>	<b>Restart</b>
IPSec Tunnel (IKE Phase 2)	<p>Updates the onscreen statistics for the selected IPSec tunnel.</p> <p>Equivalent to issuing a second <code>show</code> command in the CLI (after an initial <code>show</code> command).</p>	<p>Restarts the IPSec tunnel.</p> <p>A restart is disruptive to all existing sessions.</p> <p>Equivalent to issuing a <code>clear, test, show</code> command sequence in the CLI.</p>

As the table above indicates, restarting an IKEv2 gateway has a result different from restarting an IKEv1 gateway.

#### Refresh or Restart an IKE Gateway or IPSec Tunnel

Refresh or restart an IKE gateway.	<ol style="list-style-type: none"> <li>Select <b>Network &gt; IPSec Tunnels</b> and select the tunnel for the gateway you want to refresh or restart.</li> <li>In the row for that tunnel, under the Status column, click <b>IKE Info</b>.</li> <li>At the bottom of the IKE Info screen, click the action you want: <ul style="list-style-type: none"> <li><b>Refresh</b>—Updates the statistics on the screen.</li> <li><b>Restart</b>—Clears the SAs, so traffic is dropped until the IKE negotiation starts over and the tunnel is recreated.</li> </ul> </li> </ol>
Refresh or restart an IPSec tunnel.  You might determine that the tunnel needs to be refreshed or restarted because you use the tunnel monitor to monitor the tunnel status, or you use an external network monitor to monitor network connectivity through the IPSec tunnel	<ol style="list-style-type: none"> <li>Select <b>Network &gt; IPSec Tunnels</b> and select the tunnel you want to refresh or restart.</li> <li>In the row for that tunnel, under the Status column, click <b>Tunnel Info</b>.</li> <li>At the bottom of the Tunnel Info screen, click the action you want: <ul style="list-style-type: none"> <li><b>Refresh</b>—Updates the onscreen statistics.</li> <li><b>Restart</b>—Clears the SAs, so traffic is dropped until the IKE negotiation starts over and the tunnel is recreated.</li> </ul> </li> </ol>

## Test VPN Connectivity

### Test Connectivity

- Initiate IKE phase 1 by either pinging a host across the tunnel or using the following CLI command:

```
test vpn ike-sa gateway gateway_name
```

- Then enter the following command to test if IKE phase 1 is set up:

```
show vpn ike-sa gateway gateway_name
```

In the output, check if the Security Association displays. If it does not, review the system log messages to interpret the reason for failure.

- Initiate IKE phase 2 by either pinging a host from across the tunnel or using the following CLI command:

```
test vpn ipsec-sa tunnel tunnel_name
```

- Then enter the following command to test if IKE phase 1 is set up:

```
show vpn ipsec-sa tunnel tunnel_name
```

In the output, check if the Security Association displays. If it does not, review the system log messages to interpret the reason for failure.

- To view the VPN traffic flow information, use the following command:

```
show vpn-flow
admin@PA-500> show vpn flow
total tunnels configured: 1
filter - type IPSec, state any

total IPSec tunnel configured: 1
total IPSec tunnel shown: 1

name      id      state    local-ip      peer-ip      tunnel-i/f
-----+-----+-----+-----+-----+-----+
vpn-to-siteB  5  active  100.1.1.1  200.1.1.1  tunnel.41
```

## Interpret VPN Error Messages

The following table lists some of the common VPN error messages that are logged in the system log.

**Table: Syslog Error Messages for VPN Issues**

If error is this:	Try this:
<p>IKE phase-1 negotiation is failed as initiator, main mode. Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9 :0000000000000000 due to timeout. or IKE phase 1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]</p>	<ul style="list-style-type: none"> <li>Verify that the public IP address for each VPN peer is accurate in the IKE Gateway configuration.</li> <li>Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.</li> </ul>
<p>Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored... or IKE phase-1 negotiation is failed. Unable to process peer's SA payload.</p>	Check the IKE Crypto profile configuration to verify that the proposals on both sides have a common encryption, authentication, and DH Group proposal.
<p>pfs group mismatched:my:2peer: 0 or IKE phase-2 negotiation failed when processing SA payload. No suitable proposal found in peer's SA payload.</p>	<p>Check the IPSec Crypto profile configuration to verify that:</p> <ul style="list-style-type: none"> <li>pfs is either enabled or disabled on both VPN peers</li> <li>the DH Groups proposed by each peer has at least one DH Group in common</li> </ul>
<p>IKE phase-2 negotiation failed when processing Proxy ID. Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.</p>	The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto Networks firewall. See <a href="#">Step 8</a> .

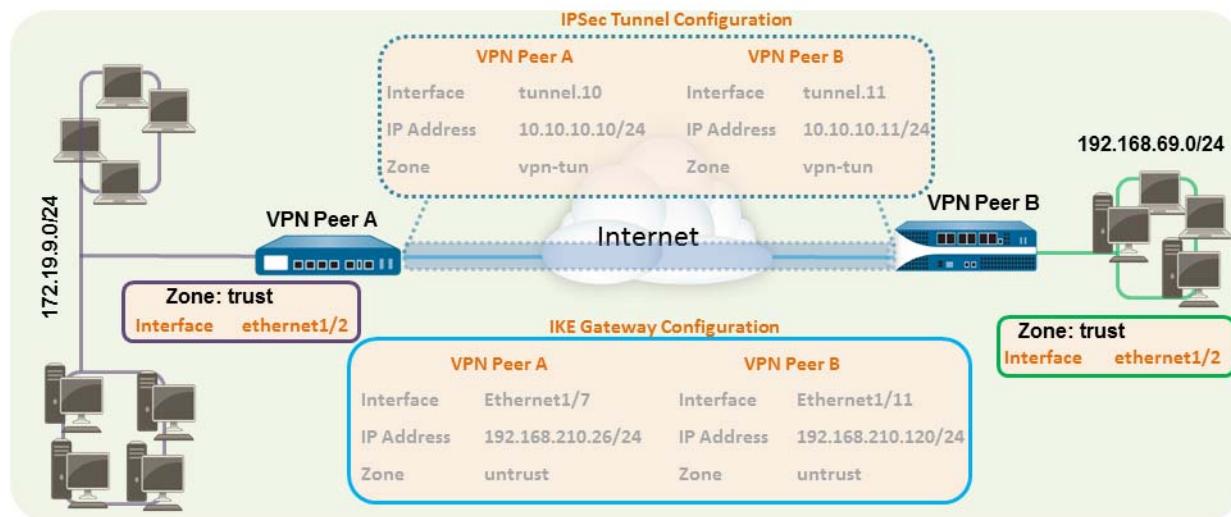
## Site-to-Site VPN Quick Configs

The following sections provide instructions for configuring some common VPN deployments:

- ▲ [Site-to-Site VPN with Static Routing](#)
- ▲ [Site-to-Site VPN with OSPF](#)
- ▲ [Site-to-Site VPN with Static and Dynamic Routing](#)

## Site-to-Site VPN with Static Routing

The following example shows a VPN connection between two sites that use static routes. Without dynamic routing, the tunnel interfaces on VPN Peer A and VPN Peer B do not require an IP address because the firewall automatically uses the tunnel interface as the next hop for routing traffic across the sites. However, to enable tunnel monitoring, a static IP address has been assigned to each tunnel interface.



**Quick Config: Site-to-Site VPN with Static Routing**

<p><b>Step 1</b> Configure a Layer 3 interface. This interface is used for the IKE phase-1 tunnel.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and then select the interface you want to configure for VPN.</li><li>2. Select <b>Layer3</b> from the <b>Interface Type</b> drop-down.</li><li>3. On the <b>Config</b> tab, select the <b>Security Zone</b> to which the interface belongs:<ul style="list-style-type: none"><li>• The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.</li><li>• If you have not yet created the zone, select <b>New Zone</b> from the <b>Security Zone</b> drop-down, define a <b>Name</b> for the new zone and then click <b>OK</b>.</li></ul></li><li>4. Select the <b>Virtual Router</b> to use.</li><li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.210.26/24.</li><li>6. To save the interface configuration, click <b>OK</b>.</li></ol> <p>In this example, the configuration for VPN Peer A is:</p> <ul style="list-style-type: none"><li>• <b>Interface</b>—ethernet1/7</li><li>• <b>Security Zone</b>—untrust</li><li>• <b>Virtual Router</b>—default</li><li>• <b>IPv4</b>—192.168.210.26/24</li></ul> <p>The configuration for VPN Peer B is:</p> <ul style="list-style-type: none"><li>• <b>Interface</b>—ethernet1/11</li><li>• <b>Security Zone</b>—untrust</li><li>• <b>Virtual Router</b>—default</li><li>• <b>IPv4</b>—192.168.210.120/24</li></ul>
--	--

### Quick Config: Site-to-Site VPN with Static Routing

- Step 2** Create a tunnel interface and attach it to a virtual router and security zone.

Interface	Management Profile	IP Address	Virtual Router	Security Zone
tunnel	none	none	none	none
tunnel.11		172.19.9.2	default	vpn_tun

- Select **Network > Interfaces > Tunnel** and click **Add**.
- In the **Interface Name** field, specify a numeric suffix, such as **.1**.
- On the **Config** tab, expand the **Security Zone** drop-down to define the zone as follows:
  - To use your trust zone as the termination point for the tunnel, select the zone from the drop-down.
  - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for new zone (for example *vpn\_tun*), and then click **OK**.
- Select the **Virtual Router**.
- (Optional) Assign an IP address to the tunnel interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface.

With static routes, the tunnel interface does not require an IP address. For traffic that is destined to a specified subnet/IP address, the tunnel interface will automatically become the next hop. Consider adding an IP address if you want to enable tunnel monitoring.

- To save the interface configuration, click **OK**.

In this example, the configuration for VPN Peer A is:

- Interface**—tunnel.11
- Security Zone**—vpn\_tun
- Virtual Router**—default
- IPv4**—172.19.9.2/24

The configuration for VPN Peer B is:

- Interface**—tunnel.12
- Security Zone**—vpn\_tun
- Virtual Router**—default
- IPv4**—192.168.69.2/24

- Step 3** Configure a static route, on the virtual router, to the destination subnet.

Virtual Router - default						
General		IPv4				
Static Routes		Destination	Interface	Type	Value	Admin Distance
traffic to 192.168.69.0		192.168.69.0	tunnel.11			default

- Select **Network > Virtual Router** and click the router you defined in the prior step.
- Select **Static Route**, click **Add**, and enter a new route to access the subnet that is at the other end of the tunnel.

In this example, the configuration for VPN Peer A is:

- Destination**—192.168.69.0/24
- Interface**—tunnel.11

The configuration for VPN Peer B is:

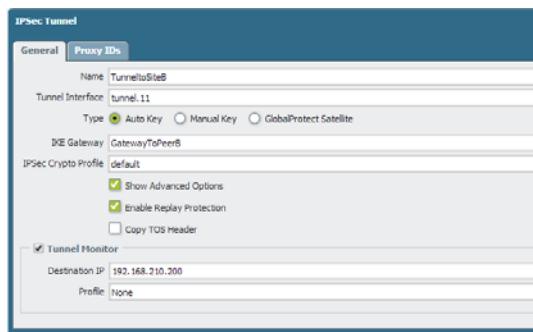
- Destination**—172.19.9.0/24
- Interface**—tunnel.12

### Quick Config: Site-to-Site VPN with Static Routing

<p><b>Step 4</b> Set up the Crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2).</p> <p>Complete this task on both peers and make sure to set identical values.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Network Profiles &gt; IKE Crypto</b>. In this example, we use the default profile.</li> </ol>  <ol style="list-style-type: none"> <li>2. Select <b>Network &gt; Network Profiles &gt; IPSec Crypto</b>. In this example, we use the default profile.</li> </ol> 
<p><b>Step 5</b> Set up the IKE Gateway.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Network Profiles &gt; IKE Gateway</b>.</li> <li>2. Click <b>Add</b> and configure the options in the <b>General</b> tab.</li> </ol> <p>In this example, the configuration for VPN Peer A is:</p> <ul style="list-style-type: none"> <li>• <b>Interface</b>—ethernet1/7</li> <li>• <b>Local IP address</b>—192.168.210.26/24</li> <li>• <b>Peer IP type/address</b>—static/192.168.210.120</li> <li>• <b>Preshared keys</b>—enter a value</li> <li>• <b>Local identification</b>—None; this means that the local IP address will be used as the local identification value.</li> </ul> <p>The configuration for VPN Peer B is:</p> <ul style="list-style-type: none"> <li>• <b>Interface</b>—ethernet1/11</li> <li>• <b>Local IP address</b>—192.168.210.120/24</li> <li>• <b>Peer IP type/address</b>—static/192.168.210.26</li> <li>• <b>Preshared keys</b>—enter same value as on Peer A</li> <li>• <b>Local identification</b>—None</li> </ul> <ol style="list-style-type: none"> <li>3. Select <b>Advanced Phase 1 Options</b> and select the IKE Crypto profile you created earlier to use for IKE phase 1.</li> </ol>

### Quick Config: Site-to-Site VPN with Static Routing

**Step 6** Set up the IPSec Tunnel.



1. Select **Network > IPSec Tunnels**.

2. Click **Add** and configure the options in the **General** tab.

In this example, the configuration for VPN Peer A is:

- **Tunnel Interface**—tunnel.11
- **Type**—Auto Key
- **IKE Gateway**—Select the IKE Gateway defined above.
- **IPSec Crypto Profile**—Select the IPSec Crypto profile defined in [Step 4](#).

The configuration for VPN Peer B is:

- **Tunnel Interface**—tunnel.12
- **Type**—Auto Key
- **IKE Gateway**—Select the IKE Gateway defined above.
- **IPSec Crypto Profile**—Select the IPSec Crypto defined in [Step 4](#).

3. (Optional) Select **Show Advanced Options**, select **Tunnel Monitor**, and specify a Destination IP address to ping for verifying connectivity. Typically, the tunnel interface IP address for the VPN Peer is used.

4. (Optional) To define the action on failure to establish connectivity, see [Define a Tunnel Monitoring Profile](#).

**Step 7** Create policies to allow traffic between the sites (subnets).

1. Select **Policies > Security**.

2. Create rules to allow traffic between the untrust and the vpn-tun zone and the vpn-tun and the untrust zone for traffic originating from specified source and destination IP addresses.

**Step 8** Save any pending configuration changes.

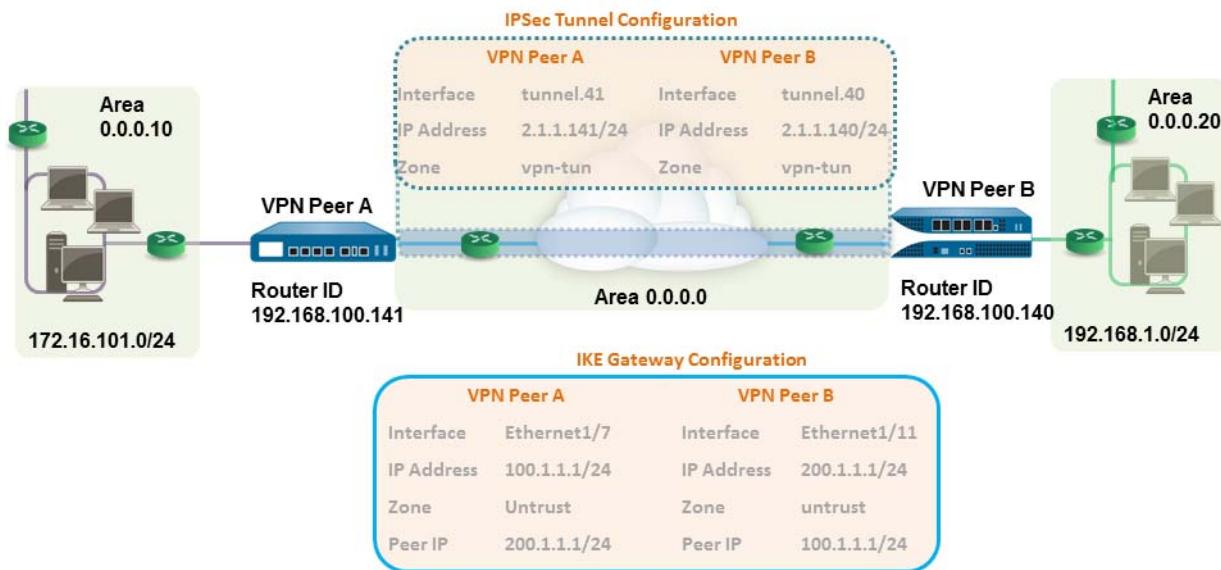
Click **Commit**.

**Step 9** Test VPN connectivity.

See [View the Status of the Tunnels](#).

## Site-to-Site VPN with OSPF

In this example, each site uses OSPF for dynamic routing of traffic. The tunnel IP address on each VPN peer is statically assigned and serves as the next hop for routing traffic between the two sites.



**Quick Config: Site-to-Site VPN with Dynamic Routing using OSPF**

**Step 1** Configure the Layer 3 interfaces on each firewall.

1. Select **Network > Interfaces > Ethernet** and then select the interface you want to configure for VPN.
2. Select **Layer3** from the **Interface Type** drop-down.
3. On the **Config** tab, select the **Security Zone** to which the interface belongs:
  - The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.
  - If you have not yet created the zone, select **New Zone** from the **Security Zone** drop-down, define a **Name** for the new zone and then click **OK**.
4. Select the **Virtual Router** to use.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.210.26/24.
6. To save the interface configuration, click **OK**.

In this example, the configuration for VPN Peer A is:

- **Interface**—ethernet1/7
- **Security Zone**—untrust
- **Virtual Router**—default
- **IPv4**—100.1.1.1/24

The configuration for VPN Peer B is:

- **Interface**—ethernet1/11
- **Security Zone**—untrust
- **Virtual Router**—default
- **IPv4**—200.1.1.1/24

### Quick Config: Site-to-Site VPN with Dynamic Routing using OSPF

- Step 2** Create a tunnel interface and attach it to a virtual router and security zone.

Interface	Management Profile	IP Address	Virtual Router	Security Zone
tunnel	none	none	none	none
tunnel.11		2.1.1.141/24	default	vpn_tun

- Select **Network > Interfaces > Tunnel** and click **Add**.
- In the **Interface Name** field, specify a numeric suffix, say, **.11**.
- On the **Config** tab, expand the **Security Zone** drop-down to define the zone as follows:
  - To use your trust zone as the termination point for the tunnel, select the zone from the drop-down.
  - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for new zone (for example *vpn\_tun*), and then click **OK**.
- Select the **Virtual Router**.
- Assign an IP address to the tunnel interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask/prefix to assign to the interface, for example, 172.19.9.2/24.

This IP address will be used as the next hop IP address to route traffic to the tunnel and can also be used to monitor the status of the tunnel.

- To save the interface configuration, click **OK**.

In this example, the configuration for VPN Peer A is:

- Interface**—tunnel.41
- Security Zone**—vpn\_tun
- Virtual Router**—default
- IPv4**—2.1.1.141/24

The configuration for VPN Peer B is:

- Interface**—tunnel.40
- Security Zone**—vpn\_tun
- Virtual Router**—default
- IPv4**—2.1.1.140/24

- Step 3** Set up the Crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2).

Complete this task on both peers and make sure to set identical values.

- Select **Network > Network Profiles > IKE Crypto**. In this example, we use the default profile.

Name	Encryption	Authentication	DH Group	Lifetime
default	aes128, 3des	sha1	group2	8 hours

- Select **Network > Network Profiles > IPSec Crypto**. In this example, we use the default profile.

Name	ESP/AH	Encryption	Authentication	DH Group	Lifetime	Lifesize
default	ESP	aes128, 3des	sha1	group2	1 hours	

**Quick Config: Site-to-Site VPN with Dynamic Routing using OSPF**

<p><b>Step 4</b> Set up the OSPF configuration on the virtual router and attach the OSPF areas with the appropriate interfaces on the firewall.</p> <p>For more information on the OSPF options that are available on the firewall, see <a href="#">Configure OSPF</a>.</p> <p>Use Broadcast as the link type when there are more than two OSPF routers that need to exchange routing information.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Virtual Routers</b>, and select the default router or add a new router.</li><li>2. Select <b>OSPF</b> (for IPv4) or <b>OSPFv3</b> (for IPv6) and select <b>Enable</b>.</li><li>3. In this example, the OSPF configuration for VPN Peer A is:<ul style="list-style-type: none"><li>– <b>Router ID:</b> 192.168.100.141</li><li>– <b>Area ID:</b> 0.0.0.0 that is assigned to the tunnel.1 interface with Link type: p2p</li><li>– <b>Area ID:</b> 0.0.0.10 that is assigned to the interface Ethernet1/1 and Link Type: Broadcast</li></ul>The OSPF configuration for VPN Peer B is:<ul style="list-style-type: none"><li>– <b>Router ID:</b> 192.168.100.140</li><li>– <b>Area ID:</b> 0.0.0.0 that is assigned to the tunnel.1 interface with Link type: p2p</li><li>– <b>Area ID:</b> 0.0.0.20 that is assigned to the interface Ethernet1/15 and Link Type: Broadcast</li></ul></li></ol>
<p><b>Step 5</b> Set up the IKE Gateway.</p> <p>This examples uses static IP addresses for both VPN peers. Typically, the corporate office uses a statically configured IP address, and the branch side can be a dynamic IP address; dynamic IP addresses are not best suited for configuring stable services such as VPN.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Network Profiles &gt; IKE Gateway</b>.</li><li>2. Click <b>Add</b> and configure the options in the <b>General</b> tab.<p>In this example, the configuration for VPN Peer A is:</p><ul style="list-style-type: none"><li>• <b>Interface</b>—ethernet1/7</li><li>• <b>Local IP address</b>—100.1.1.1/24</li><li>• <b>Peer IP address</b>—200.1.1.1/24</li><li>• <b>Preshared keys</b>—enter a value</li></ul><p>The configuration for VPN Peer B is:</p><ul style="list-style-type: none"><li>• <b>Interface</b>—ethernet1/11</li><li>• <b>Local IP address</b>—200.1.1.1/24</li><li>• <b>Peer IP address</b>—100.1.1.1/24</li><li>• <b>Preshared keys</b>—enter same value as on Peer A</li></ul><li>3. Select the IKE Crypto profile you created earlier to use for IKE phase 1.</li></li></ol>

**Quick Config: Site-to-Site VPN with Dynamic Routing using OSPF**

<b>Step 6</b> Set up the IPSec Tunnel.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; IPSec Tunnels</b>.</li><li>2. Click <b>Add</b> and configure the options in the <b>General</b> tab. In this example, the configuration for VPN Peer A is:<ul style="list-style-type: none"><li>• <b>Tunnel Interface</b>—tunnel.41</li><li>• <b>Type</b>—Auto Key</li><li>• <b>IKE Gateway</b>—Select the IKE Gateway defined above.</li><li>• <b>IPSec Crypto Profile</b>—Select the IKE Gateway defined above.</li></ul>The configuration for VPN Peer B is:<ul style="list-style-type: none"><li>• <b>Tunnel Interface</b>—tunnel.40</li><li>• <b>Type</b>—Auto Key</li><li>• <b>IKE Gateway</b>—Select the IKE Gateway defined above.</li><li>• <b>IPSec Crypto Profile</b>—Select the IKE Gateway defined above.</li></ul></li><li>3. Select <b>Show Advanced Options</b>, select <b>Tunnel Monitor</b>, and specify a Destination IP address to ping for verifying connectivity.</li><li>4. To define the action on failure to establish connectivity, see <a href="#">Define a Tunnel Monitoring Profile</a>.</li></ol>
<b>Step 7</b> Create policies to allow traffic between the sites (subnets).	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b>.</li><li>2. Create rules to allow traffic between the untrust and the vpn-tun zone and the vpn-tun and the untrust zone for traffic originating from specified source and destination IP addresses.</li></ol>

### Quick Config: Site-to-Site VPN with Dynamic Routing using OSPF

**Step 8** Verify OSPF adjacencies and routes from the CLI.

Verify that both the firewalls can see each other as neighbors with full status. Also confirm that the IP address of the VPN peer's tunnel interface and the OSPF Router ID. Use the following CLI commands on each VPN peer.

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor
Options: 0x80:reserved, O:Opaque-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
          N/F:NSSA option, MC:multicast, EIAS external LSA capability, T:TOS capability
=====
virtual router:           vrl
neighbor address:        2.1.1.140
local address binding:   0.0.0.0
type:                   dynamic
status:                 full
neighbor router ID:     192.168.100.140
area id:                0.0.0.0
neighbor priority:      1
lifetime remain:        39
messages pending:       0
LSA request pending:    0
options:                0x42: O E
hello suppressed:       no
```

```
admin@FW-B> show routing protocol ospf neighbor
Options: 0x80:reserved, O:Opaque-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
          N/F:NSSA option, MC:multicast, EIAS external LSA capability, T:TOS capability
=====
virtual router:           vrl
neighbor address:        2.1.1.141
local address binding:   0.0.0.0
type:                   dynamic
status:                 full
neighbor router ID:     192.168.100.141
area id:                0.0.0.0
neighbor priority:      1
lifetime remain:        39
messages pending:       0
LSA request pending:    0
options:                0x42: O E
hello suppressed:       no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf
flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgf
      Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2

VIRTUAL ROUTER: vrl (id 1)
=====
destination      nexthop      metric flags      age      interface
2.1.1.0/24       0.0.0.0      10  Oi      6760  tunnel.41
172.16.101.0/24  0.0.0.0      10  Oi      6854  ethernet1/1
192.168.1.0/24   2.1.1.140    20  A Oo      6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf
flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
      Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2

VIRTUAL ROUTER: vrl (id 1)
=====
destination      nexthop      metric flags      age      interface
2.1.1.0/24       0.0.0.0      10  Oi      20033 tunnel.40
172.16.101.0/24  2.1.1.141    20  A Oo      6896  tunnel.40
192.168.1.0/24   0.0.0.0      10  Oi      8058  ethernet1/15
total routes shown: 3
```

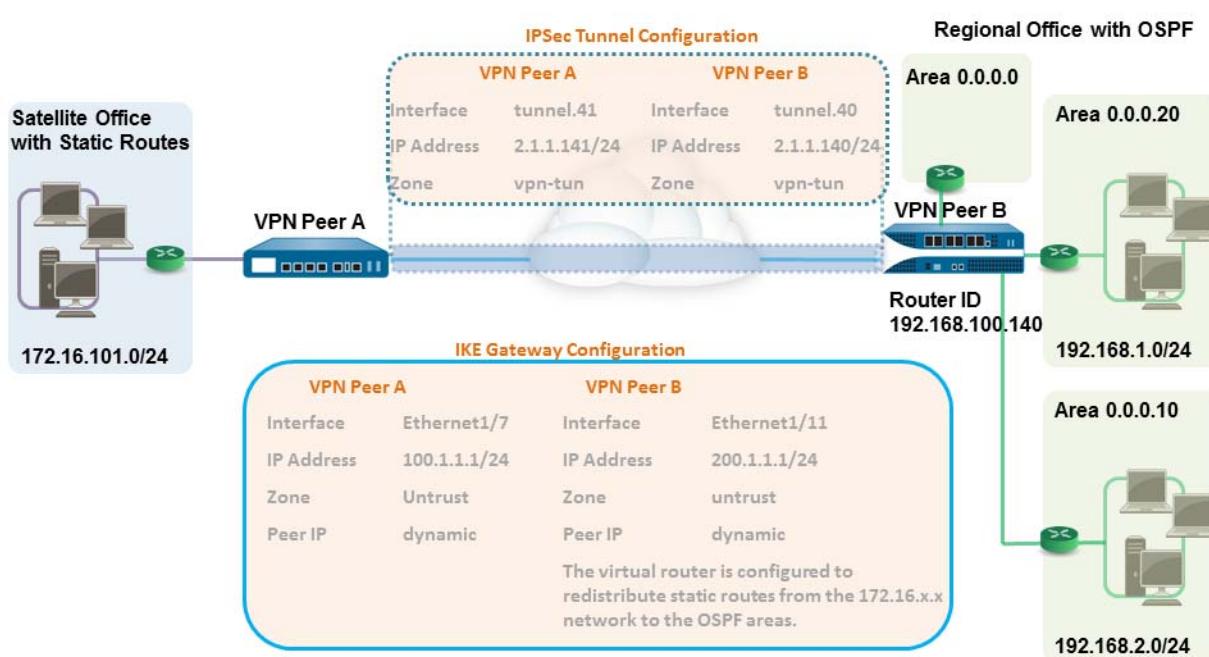
**Step 9** Test VPN connectivity.

See [Set Up Tunnel Monitoring](#) and [View the Status of the Tunnels](#).

## Site-to-Site VPN with Static and Dynamic Routing

In this example, one site uses static routes and the other site uses OSPF. When the routing protocol is not the same between the locations, the tunnel interface on each firewall must be configured with a static IP address. Then, to allow the exchange of routing information, the firewall that participates in both the static and dynamic routing process must be configured with a *Redistribution profile*. Configuring the redistribution profile enables the virtual router to redistribute and filter routes between protocols—static routes, connected routes, and hosts—from the static autonomous system to the OSPF autonomous system. Without this redistribution profile, each protocol functions on its own and does not exchange any route information with other protocols running on the same virtual router.

In this example, the satellite office has static routes and all traffic destined to the 192.168.x.x network is routed to tunnel.41. The virtual router on VPN Peer B participates in both the static and the dynamic routing process and is configured with a redistribution profile in order to propagate (*export*) the static routes to the OSPF autonomous system.



### Quick Config: Site-to-Site VPN with Static and Dynamic Routing

<p><b>Step 1</b> Configure the Layer 3 interfaces on each firewall.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and then select the interface you want to configure for VPN.</li> <li>2. Select <b>Layer3</b> from the <b>Interface Type</b> drop-down.</li> <li>3. On the <b>Config</b> tab, select the <b>Security Zone</b> to which the interface belongs: <ul style="list-style-type: none"> <li>• The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.</li> <li>• If you have not yet created the zone, select <b>New Zone</b> from the <b>Security Zone</b> drop-down, define a <b>Name</b> for the new zone and then click <b>OK</b>.</li> </ul> </li> <li>4. Select the <b>Virtual Router</b> to use.</li> <li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.210.26/24.</li> <li>6. To save the interface configuration, click <b>OK</b>.</li> </ol> <p>In this example, the configuration for VPN Peer A is:</p> <ul style="list-style-type: none"> <li>• <b>Interface</b>—ethernet1/7</li> <li>• <b>Security Zone</b>—untrust</li> <li>• <b>Virtual Router</b>—default</li> <li>• <b>IPv4</b>—100.1.1.1/24</li> </ul> <p>The configuration for VPN Peer B is:</p> <ul style="list-style-type: none"> <li>• <b>Interface</b>—ethernet1/11</li> <li>• <b>Security Zone</b>—untrust</li> <li>• <b>Virtual Router</b>—default</li> <li>• <b>IPv4</b>—200.1.1.1/24</li> </ul>
<p><b>Step 2</b> Set up the Crypto profiles (IKE Crypto profile for phase 1 and IPSec Crypto profile for phase 2).</p> <p>Complete this task on both peers and make sure to set identical values.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Network Profiles &gt; IKE Crypto</b>. In this example, we use the default profile.</li> </ol>  <ol style="list-style-type: none"> <li>2. Select <b>Network &gt; Network Profiles &gt; IPSec Crypto</b>. In this example, we use the default profile.</li> </ol> 

**Quick Config: Site-to-Site VPN with Static and Dynamic Routing****Step 3** Set up the IKE Gateway.

With pre-shared keys, to add authentication scrutiny when setting up the IKE phase-1 tunnel, you can set up Local and Peer Identification attributes and a corresponding value that is matched in the IKE negotiation process.

1. Select **Network > Network Profiles > IKE Gateway**.

2. Click **Add** and configure the options in the **General** tab.

In this example, the configuration for VPN Peer A is:

- **Interface**—ethernet1/7
- **Local IP address**—100.1.1.1/24
- **Peer IP type**—dynamic
- **Preshared keys**—enter a value
- **Local identification**—select **FQDN(hostname)** and enter the value for VPN Peer A.
- **Peer identification**—select **FQDN(hostname)** and enter the value for VPN Peer B

The configuration for VPN Peer B is:

- **Interface**—ethernet1/11
- **Local IP address**—200.1.1.1/24
- **Peer IP address**—dynamic
- **Preshared keys**—enter same value as on Peer A
- **Local identification**—select **FQDN(hostname)** and enter the value for VPN Peer B
- **Peer identification**—select **FQDN(hostname)** and enter the value for VPN Peer A

3. Select the IKE Crypto profile you created earlier to use for IKE phase 1.

### Quick Config: Site-to-Site VPN with Static and Dynamic Routing

- Step 4** Create a tunnel interface and attach it to a virtual router and security zone.

Interface	Management Profile	IP Address	Virtual Router	Security Zone
tunnel		none	none	none
tunnel.11		2.1.1.141/24	default	vpn_tun

1. Select **Network > Interfaces > Tunnel** and click **Add**.
2. In the **Interface Name** field, specify a numeric suffix, say, **.41**.
3. On the **Config** tab, expand the **Security Zone** drop-down to define the zone as follows:
  - To use your trust zone as the termination point for the tunnel, select the zone from the drop-down.
  - (Recommended) To create a separate zone for VPN tunnel termination, click **New Zone**. In the Zone dialog, define a **Name** for new zone (for example *vpn\_tun*), and then click **OK**.
4. Select the **Virtual Router**.
5. Assign an IP address to the tunnel interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask/prefix to assign to the interface, for example, 172.19.9.2/24.

This IP address will be used to route traffic to the tunnel and to monitor the status of the tunnel.

6. To save the interface configuration, click **OK**.

In this example, the configuration for VPN Peer A is:

- **Interface**—tunnel.41
- **Security Zone**—vpn\_tun
- **Virtual Router**—default
- **IPv4**—2.1.1.141/24

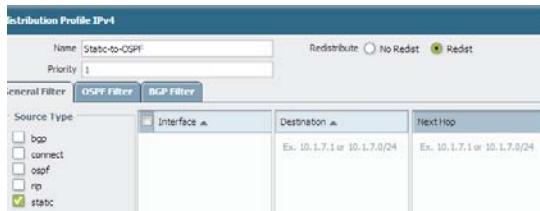
The configuration for VPN Peer B is:

- **Interface**—tunnel.42
- **Security Zone**—vpn\_tun
- **Virtual Router**—default
- **IPv4**—2.1.1.140/24

- Step 5** Specify the interface to route traffic to a destination on the 192.168.x.x network.

1. On VPN Peer A, select the virtual router.
2. Select **Static Routes**, and **Add** tunnel.41 as the **Interface** for routing traffic with a **Destination** in the 192.168.x.x network.

### Quick Config: Site-to-Site VPN with Static and Dynamic Routing

<p><b>Step 6</b> Set up the static route and the OSPF configuration on the virtual router and attach the OSPF areas with the appropriate interfaces on the firewall.</p>	<ol style="list-style-type: none"> <li>On VPN Peer B, select <b>Network &gt; Virtual Routers</b>, and select the default router or add a new router.</li> <li>Select <b>Static Routes</b> and <b>Add</b> the tunnel IP address as the next hop for traffic in the 172.168.x.x. network. Assign the desired route metric; using a lower value makes the a higher priority for route selection in the forwarding table.</li> <li>Select <b>OSPF</b> (for IPv4) or <b>OSPFv3</b> (for IPv6) and select <b>Enable</b>.</li> <li>In this example, the OSPF configuration for VPN Peer B is: <ul style="list-style-type: none"> <li>Router ID: 192.168.100.140</li> <li>Area ID: 0.0.0.0 is assigned to the interface Ethernet 1/12 Link type: Broadcast</li> <li>Area ID: 0.0.0.10 that is assigned to the interface Ethernet1/1 and Link Type: Broadcast</li> <li>Area ID: 0.0.0.20 is assigned to the interface Ethernet1/15 and Link Type: Broadcast</li> </ul> </li> </ol>
<p><b>Step 7</b> Create a redistribution profile to inject the static routes into the OSPF autonomous system.</p>  	<ol style="list-style-type: none"> <li>Create a redistribution profile on VPN Peer B. <ol style="list-style-type: none"> <li>Select <b>Network &gt; Virtual Routers</b>, and select the router you used above.</li> <li>Select <b>Redistribution Profiles</b>, and click <b>Add</b>.</li> <li>Enter a Name for the profile and select <b>Redist</b> and assign a <b>Priority</b> value. If you have configured multiple profiles, the profile with the lowest priority value is matched first.</li> <li>Set <b>Source Type</b> as <b>static</b>, and click <b>OK</b>. The static route defined in Step 6-2 will be used for the redistribution.</li> </ol> </li> <li>Inject the static routes into the OSPF system. <ol style="list-style-type: none"> <li>Select <b>OSPF&gt; Export Rules</b> (for IPv4) or <b>OSPFv3&gt; Export Rules</b> (for IPv6).</li> <li>Click <b>Add</b>, and select the redistribution profile that you just created.</li> <li>Select how the external routes are brought into the OSPF system. The default option, <b>Ext2</b> calculates the total cost of the route using only the external metrics. To use both internal and external OSPF metrics, use <b>Ext1</b>.</li> <li>Assign a <b>Metric</b> (cost value) for the routes injected into the OSPF system. This option allows you to change the metric for the injected route as it comes into the OSPF system.</li> <li>Click <b>OK</b> to save the changes.</li> </ol> </li> </ol>

**Quick Config: Site-to-Site VPN with Static and Dynamic Routing**

<p><b>Step 8</b> Set up the IPSec Tunnel.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; IPSec Tunnels</b>.</li><li>2. Click <b>Add</b> and configure the options in the <b>General</b> tab. In this example, the configuration for VPN Peer A is:<ul style="list-style-type: none"><li>• <b>Tunnel Interface</b>—tunnel.41</li><li>• <b>Type</b>—Auto Key</li><li>• <b>IKE Gateway</b>—Select the IKE Gateway defined above.</li><li>• <b>IPSec Crypto Profile</b>—Select the IKE Gateway defined above.</li></ul>The configuration for VPN Peer B is:<ul style="list-style-type: none"><li>• <b>Tunnel Interface</b>—tunnel.40</li><li>• <b>Type</b>—Auto Key</li><li>• <b>IKE Gateway</b>—Select the IKE Gateway defined above.</li><li>• <b>IPSec Crypto Profile</b>—Select the IKE Gateway defined above.</li></ul></li><li>3. Select <b>Show Advanced Options</b>, select <b>Tunnel Monitor</b>, and specify a Destination IP address to ping for verifying connectivity.</li><li>4. To define the action on failure to establish connectivity, see <a href="#">Define a Tunnel Monitoring Profile</a>.</li></ol>
<p><b>Step 9</b> Create policies to allow traffic between the sites (subnets).</p>	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b>.</li><li>2. Create rules to allow traffic between the untrust and the vpn-tun zone and the vpn-tun and the untrust zone for traffic originating from specified source and destination IP addresses.</li></ol>

### Quick Config: Site-to-Site VPN with Static and Dynamic Routing

**Step 10** Verify OSPF adjacencies and routes from the CLI.

Verify that both the firewalls can see each other as neighbors with full status. Also confirm that the IP address of the VPN peer's tunnel interface and the OSPF Router ID. Use the following CLI commands on each VPN peer.

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor
Options: 0xB0:reserved, 0:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
M/P/INSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
=====
virtual router: vr1
neighbor address: 2.1.1.140
local address binding: 0.0.0.0
type: dynamic
status: full
neighbor router ID: 192.168.100.140
area id: 0.0.0.0
neighbor priority: 1
lifetime remain: 39
messages pending: 0
LSA request pending: 0
options: 0x42: O E
hello suppressed: no
```

```
admin@FW-B> show routing protocol ospf neighbor
Options: 0xB0:reserved, 0:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
M/P/INSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
=====
virtual router: vr1
neighbor address: 2.1.1.141
local address binding: 0.0.0.0
type: dynamic
status: full
neighbor router ID: 192.168.100.141
area id: 0.0.0.0
neighbor priority: 1
lifetime remain: 39
messages pending: 0
LSA request pending: 0
options: 0x42: O E
hello suppressed: no
```

- **show routing route**

The following is an example of the output on each VPN peer.

VPN PeerA						
destination	next hop	metric	flags	age	interface	next-AS
192.168.1.0/24	2.1.1.141	20	A S		tunnel.41	
192.168.2.0/24	2.1.1.141	20	A S		tunnel.41	
172.16.101.0/24	0.0.0.0	1	A H		ethernet1/1	
2.1.1.140/34	2.1.1.141	20	A S		tunnel.41	

VPN PeerB						
destination	next hop	metric	flags	age	interface	next-AS
192.168.1.0/24	0.0.0.0	10	A Ou		ethernet1/1	
192.168.2.0/24	0.0.0.0	10	A Ou		ethernet1/1	
172.16.101.0/24	2.1.1.140	20	A H		tunnel.40	
2.1.1.141/24	2.1.1.140	10	A C		tunnel.40	

**Step 11** Test VPN connectivity.

See [Set Up Tunnel Monitoring](#) and [View the Status of the Tunnels](#).



# Large Scale VPN (LSVPN)

---

The GlobalProtect Large Scale VPN (LSVPN) feature on the Palo Alto Networks next-generation firewall simplifies the deployment of traditional hub and spoke VPNs, enabling you to quickly deploy enterprise networks with several branch offices with a minimum amount of configuration required on the remote *satellite* devices. This solution uses certificates for device authentication and IPSec to secure data.



LSVPN enables site-to-site VPNs between Palo Alto Networks firewalls. To set up a site-to-site VPN between a Palo Alto Networks firewall and another device, see [VPNs](#).

The following topics describe the LSVN components and how to set them up to enable site-to-site VPN services between Palo Alto Networks firewalls:

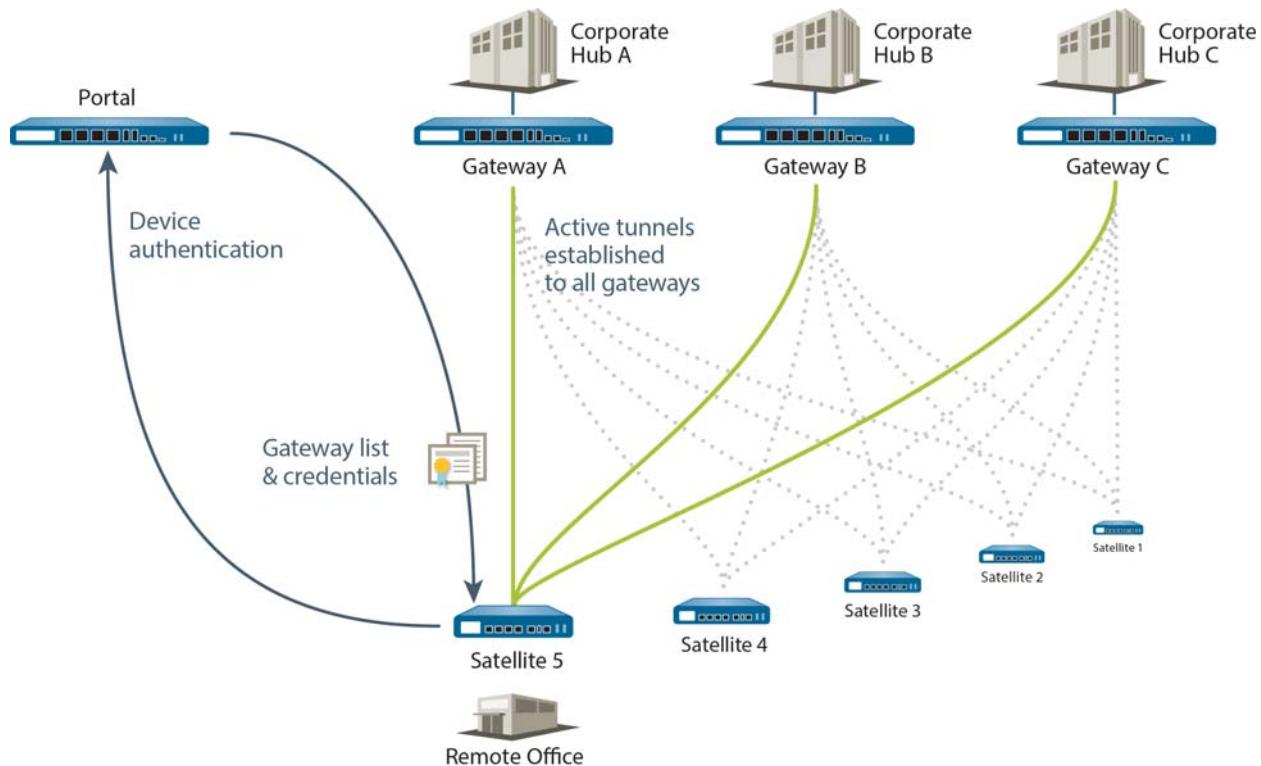
- ▲ [LSVPN Overview](#)
- ▲ [Create Interfaces and Zones for the LSVN](#)
- ▲ [Enable SSL Between GlobalProtect LSVN Components](#)
- ▲ [Configure the Portal to Authenticate Satellites](#)
- ▲ [Configure GlobalProtect Gateways for LSVN](#)
- ▲ [Configure the GlobalProtect Portal for LSVN](#)
- ▲ [Prepare the Satellite Device to Join the LSVN](#)
- ▲ [Verify the LSVN Configuration](#)
- ▲ [LSVPN Quick Configs](#)

## LSVPN Overview

GlobalProtect provides a complete infrastructure for managing secure access to corporate resources from your remote sites. This infrastructure includes the following components:

- **GlobalProtect Portal**—Provides the management functions for your GlobalProtect LSVPN infrastructure. Every satellite that participates in the GlobalProtect LSVPN receives configuration information from the portal, including configuration information to enable the satellites (the spokes) to connect to the gateways (the hubs). You configure the portal on an interface on any Palo Alto Networks next-generation firewall.
- **GlobalProtect Gateways**—A Palo Alto Networks firewall that provides the tunnel end point for satellite connections. The resources that the satellites access is protected by security policy on the gateway. It is not required to have a separate portal and gateway; a single firewall can function both as portal and gateway.
- **GlobalProtect Satellite**—A Palo Alto Networks firewall at a remote site that establishes IPSec tunnels with the gateway(s) at your corporate office(s) for secure access to centralized resources. Configuration on the satellite firewall is minimal, enabling you to quickly and easily scale your VPN as you add new sites.

The following diagram illustrates how the GlobalProtect LSVPN components work together.



## Create Interfaces and Zones for the LSVPN

You must configure the following interfaces and zones for your LSVPN infrastructure:

- **GlobalProtect portal**—Requires a Layer 3 interface for GlobalProtect satellites to connect to. If the portal and gateway are on the same firewall, they can use the same interface. The portal must be in a zone that is accessible from your branch offices.
- **GlobalProtect gateways**—Requires three interfaces: a Layer 3 interface in the zone that is reachable by the remote satellites, an internal interface in the trust zone that connects to the protected resources, and a logical tunnel interface for terminating the VPN tunnels from the satellites. Unlike other site-to-site VPN solutions, the GlobalProtect gateway only requires a single tunnel interface, which it will use for tunnel connections with all of your remote satellites (point-to-multi-point). If you plan to use dynamic routing, you must assign an IP address to the tunnel interface.
- **GlobalProtect satellites**—Requires a single tunnel interface for establishing a VPN with the remote gateways (up to a maximum of 25 gateways). If you plan to use dynamic routing, you must assign an IP address to the tunnel interface.

For more information about portals, gateways, and satellites see [LSVPN Overview](#).

### Set Up Interfaces and Zones for the GlobalProtect LSVPN

<p><b>Step 1</b> Configure a Layer 3 interface.</p> <p>The portal and each gateway and satellite all require a Layer 3 interface to enable traffic to be routed between sites.</p> <p>If the gateway and portal are on the same firewall, you can use a single interface for both components.</p> <p> IPv6 addresses are not supported with LSVPN.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and then select the interface you want to configure for GlobalProtect LSVPN.</li><li>2. Select <b>Layer3</b> from the <b>Interface Type</b> drop-down.</li><li>3. On the <b>Config</b> tab, select the <b>Security Zone</b> to which the interface belongs:<ul style="list-style-type: none"><li>• The interface must be accessible from a zone outside of your trust network. Consider creating a dedicated VPN zone for visibility and control over your VPN traffic.</li><li>• If you have not yet created the zone, select <b>New Zone</b> from the <b>Security Zone</b> drop-down, define a <b>Name</b> for the new zone and then click <b>OK</b>.</li></ul></li><li>4. Select the <b>Virtual Router</b> to use.</li><li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 203.0.11.100/24.</li><li>6. To save the interface configuration, click <b>OK</b>.</li></ol>
---	---

### Set Up Interfaces and Zones for the GlobalProtect LSVPN (Continued)

<p><b>Step 2</b> On the firewall(s) hosting GlobalProtect gateway(s), configure the logical tunnel interface that will terminate VPN tunnels established by the GlobalProtect satellites.</p> <p> IP addresses are not required on the tunnel interface unless plan to use dynamic routing. However, assigning an IP address to the tunnel interface can be useful for troubleshooting connectivity issues.</p> <p> Make sure to enable User-ID in the zone where the VPN tunnels terminate.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces &gt; Tunnel</b> and click <b>Add</b>.</li> <li>2. In the <b>Interface Name</b> field, specify a numeric suffix, such as <b>.2</b>.</li> <li>3. On the <b>Config</b> tab, expand the <b>Security Zone</b> drop-down to define the zone as follows: <ul style="list-style-type: none"> <li>• To use your trust zone as the termination point for the tunnel, select the zone from the drop-down.</li> <li>• (Recommended) To create a separate zone for VPN tunnel termination, click <b>New Zone</b>. In the Zone dialog, define a <b>Name</b> for new zone (for example <i>lsvpn-tun</i>), select the <b>Enable User Identification</b> check box, and then click <b>OK</b>.</li> </ul> </li> <li>4. Select the <b>Virtual Router</b>.</li> <li>5. (Optional) If you want to assign an IP address to the tunnel interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example <b>203.0.11.33/24</b>.</li> <li>6. To save the interface configuration, click <b>OK</b>.</li> </ol>																		
<p><b>Step 3</b> If you created a separate zone for tunnel termination of VPN connections, create a security policy to enable traffic flow between the VPN zone and your trust zone.</p>	<p>For example, the following policy rule enables traffic between the <i>lsvpn-tun</i> zone and the <i>L3-Trust</i> zone.</p> <table border="1" data-bbox="163 1030 1383 1136"> <thead> <tr> <th>Name</th><th>Zone</th><th>Address</th><th>User</th><th>Zone</th><th>Address</th><th>Application</th><th>Service</th><th>Action</th></tr> </thead> <tbody> <tr> <td>LSVPN Access</td><td> lsvpn-tun</td><td>any</td><td>any</td><td> L3-Trust</td><td>any</td><td> adobe-creati...</td><td> application-d...</td><td><input checked="" type="checkbox"/></td></tr> </tbody> </table>	Name	Zone	Address	User	Zone	Address	Application	Service	Action	LSVPN Access	 lsvpn-tun	any	any	 L3-Trust	any	 adobe-creati...	 application-d...	<input checked="" type="checkbox"/>
Name	Zone	Address	User	Zone	Address	Application	Service	Action											
LSVPN Access	 lsvpn-tun	any	any	 L3-Trust	any	 adobe-creati...	 application-d...	<input checked="" type="checkbox"/>											
<p><b>Step 4</b> Save the configuration.</p>	<p>Click <b>Commit</b>.</p>																		

## Enable SSL Between GlobalProtect LVPN Components

All interaction between the GlobalProtect components occurs over an SSL/TLS connection. Therefore, you must generate and/or install the required certificates before configuring each component so that you can reference the appropriate certificate(s) and/or certificate profiles in the configurations for each component. The following sections describe the supported methods of certificate deployment, descriptions and best practice guidelines for the various GlobalProtect certificates, and provide instructions for generating and deploying the required certificates:

- ▲ [About Certificate Deployment](#)
- ▲ [Deploy Server Certificates to the GlobalProtect LVPN Components](#)

### About Certificate Deployment

There are two basic approaches to deploying certificates for GlobalProtect LVPN:

- **Enterprise Certificate Authority**—If you already have your own enterprise certificate authority, you can use this internal CA to issue an intermediate CA certificate for the GlobalProtect portal to enable it to issue certificates to the GlobalProtect gateways and satellites.
- **Self-Signed Certificates**—You can generate a self-signed root CA certificate on the firewall and use it to issue server certificates for the portal, gateway(s), and satellite(s). As a best practice, create a self-signed root CA certificate on the portal and use it to issue server certificates for the gateways and satellites. This way, the private key used for certificate signing stays on the portal.

### Deploy Server Certificates to the GlobalProtect LVPN Components

The GlobalProtect LVPN components use SSL/TLS to mutually authenticate. Before deploying the LVPN, you must assign an SSL/TLS service profile to each portal and gateway. The profile specifies the server certificate and allowed TLS versions for communication with satellite devices. You don't need to create SSL/TLS service profiles for the satellite devices because the portal will issue a server certificate for each device during the first connection as part of the device registration process.

In addition, you must import the root certificate authority (CA) certificate used to issue the server certificates onto each firewall that you plan to host as a gateway or satellite device. Finally, on each gateway and satellite device participating in the LVPN, you must configure a certificate profile that will enable them to establish an SSL/TLS connection using mutual authentication.

The following workflow shows the best practice steps for deploying SSL certificates to the GlobalProtect LVPN components:

## Deploy SSL Server Certificates to the GlobalProtect Components

<p><b>Step 1</b> On the firewall hosting the GlobalProtect portal, create the root CA certificate for signing the certificates of the GlobalProtect components.</p>	<p><b>Create a Self-Signed Root CA Certificate:</b></p> <ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Generate</b>.</li> <li>2. Enter a <b>Certificate Name</b>, such as <b>LVPN_CA</b>.</li> <li>3. Do not select a value in the <b>Signed By</b> field (this is what indicates that it is self-signed).</li> <li>4. Select the <b>Certificate Authority</b> check box and then click <b>OK</b> to generate the certificate.</li> </ol>
<p><b>Step 2</b> Create SSL/TLS service profiles for the GlobalProtect portal and gateways.</p> <p>For the portal and each gateway, you must assign an SSL/TLS service profile that references a unique self-signed server certificate.</p> <p> The best practice is to issue all of the required certificates on the portal, so that the signing certificate (with the private key) doesn't have to be exported.</p> <p> If the GlobalProtect portal and gateway are on the same firewall interface, you can use the same server certificate for both components.</p>	<ol style="list-style-type: none"> <li>1. Use the root CA on the portal to <a href="#">Generate a Certificate on the Device</a> for each gateway you will deploy:             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Generate</b>.</li> <li>b. Enter a <b>Certificate Name</b>.</li> <li>c. Enter the FQDN (recommended) or IP address of the interface where you plan to configure the gateway in the <b>Common Name</b> field.</li> <li>d. In the <b>Signed By</b> field, select the <b>LVPN_CA</b> certificate you just created.</li> <li>e. In the Certificate Attributes section, click <b>Add</b> and define the attributes to uniquely identify the gateway. If you add a <b>Host Name</b> attribute (which populates the SAN field of the certificate), it must exactly match the value you defined for the <b>Common Name</b>.</li> <li>f. <b>Generate</b> the certificate.</li> </ol> </li> <li>2. <a href="#">Configure an SSL/TLS Service Profile</a> for the portal and each gateway:             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; SSL/TLS Service Profile</b> and click <b>Add</b>.</li> <li>b. Enter a <b>Name</b> to identify the profile and select the server <b>Certificate</b> you just created for the portal or gateway.</li> <li>c. Define the range of TLS versions (<b>Min Version</b> to <b>Max Version</b>) allowed for communicating with satellite devices and click <b>OK</b>.</li> </ol> </li> </ol>

<b>Deploy SSL Server Certificates to the GlobalProtect Components (Continued)</b>	
<p><b>Step 3</b> Deploy the self-signed server certificates to the gateways.</p> <p><b>Best Practices:</b></p>  <ul style="list-style-type: none"> <li>• Export the self-signed server certificates issued by the root CA from the portal and import them onto the gateways.</li> <li>• Be sure to issue a unique server certificate for each gateway.</li> <li>• The Common Name (CN) and, if applicable, the Subject Alternative Name (SAN) fields of the certificate must match the IP address or fully qualified domain name (FQDN) of the interface where you configure the gateway.</li> </ul>	<ol style="list-style-type: none"> <li>1. On the portal, select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b>, select the gateway certificate you want to deploy, and click <b>Export</b>.</li> <li>2. Select <b>Encrypted Private Key and Certificate (PKCS12)</b> from the <b>File Format</b> drop-down.</li> <li>3. Enter (and re-enter) a <b>Passphrase</b> to encrypt the private key associated with the certificate and then click <b>OK</b> to download the PKCS12 file to your computer.</li> <li>4. On the gateway, select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Import</b>.</li> <li>5. Enter a <b>Certificate Name</b>.</li> <li>6. Enter the path and name to the <b>Certificate File</b> you just downloaded from the portal, or <b>Browse</b> to find the file.</li> <li>7. Select <b>Encrypted Private Key and Certificate (PKCS12)</b> as the <b>File Format</b>.</li> <li>8. Enter the path and name to the PKCS12 file in the <b>Key File</b> field or <b>Browse</b> to find it.</li> <li>9. Enter and re-enter the <b>Passphrase</b> you used to encrypt the private key when you exported it from the portal and then click <b>OK</b> to import the certificate and key.</li> </ol>
<p><b>Step 4</b> Import the root CA certificate used to issue server certificates for the LVPN components.</p> <p>You must import the root CA certificate onto all gateways and satellites. For security reasons, make sure you export the certificate only, and not the associated private key.</p>	<ol style="list-style-type: none"> <li>1. Download the root CA certificate from the portal.             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b>.</li> <li>b. Select the root CA certificate used to issue certificates for the LVPN components and click <b>Export</b>.</li> <li>c. Select <b>Base64 Encoded Certificate (PEM)</b> from the <b>File Format</b> drop-down and click <b>OK</b> to download the certificate. (Do not export the private key.)</li> </ol> </li> <li>2. On the firewalls hosting the gateways and satellites, import the root CA certificate.             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Import</b>.</li> <li>b. Enter a <b>Certificate Name</b> that identifies the certificate as your client CA certificate.</li> <li>c. <b>Browse</b> to the <b>Certificate File</b> you downloaded from the CA.</li> <li>d. Select <b>Base64 Encoded Certificate (PEM)</b> as the <b>File Format</b> and then click <b>OK</b>.</li> <li>e. Select the certificate you just imported on the <b>Device Certificates</b> tab to open it.</li> <li>f. Select <b>Trusted Root CA</b> and then click <b>OK</b>.</li> <li>g. <b>Commit</b> the changes.</li> </ol> </li> </ol>

**Deploy SSL Server Certificates to the GlobalProtect Components (Continued)**

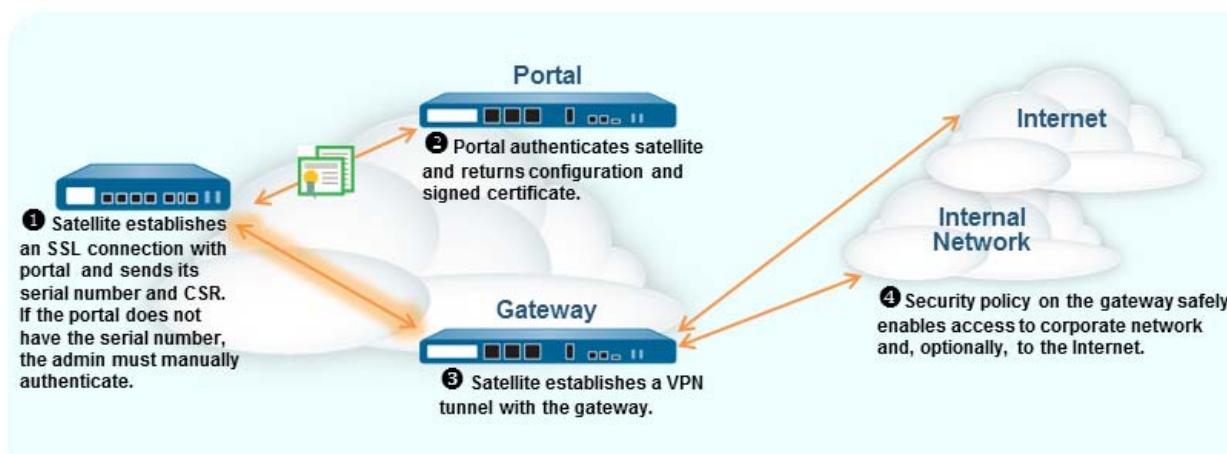
<b>Step 5</b> Create a certificate profile.  The GlobalProtect LVPN portal and each gateway require a certificate profile that specifies which certificate to use to authenticate the satellite devices.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Certificate Management &gt; Certificate Profile</b> and click <b>Add</b> and enter a profile <b>Name</b>.</li><li>2. Make sure <b>Username Field</b> is set to <b>None</b>.</li><li>3. In the <b>CA Certificates</b> field, click <b>Add</b>, select the Trusted Root CA certificate you imported in <a href="#">Step 4</a>.</li><li>4. (Optional, but recommended) Enable use of CRL and/or OCSP to enable certificate status verification.</li><li>5. Click <b>OK</b> to save the profile.</li></ol>
<b>Step 6</b> Save the configuration.	Click <b>Commit</b> .

## Configure the Portal to Authenticate Satellites

In order to register with the LSVPN, each satellite must establish an SSL/TLS connection with the portal. After establishing the connection, the portal authenticates the satellite device to ensure that it is authorized to join the LSVPN. After successfully authenticating the satellite, the portal will issue a server certificate for the satellite and push the LSVPN configuration specifying the gateways to which the satellite can connect and the root CA certificate required to establish an SSL connection with the gateways.

There are two ways that the satellite can authenticate to the portal during its initial connection:

- **Serial number**—You can configure the portal with the serial number of the satellite firewalls that are authorized to join the LSVPN. During the initial satellite connection to the portal, the satellite presents its serial number to the portal and if the portal has the serial number in its configuration, the satellite will be successfully authenticated. You add the serial numbers of authorized satellites when you configure the portal. See [Configure the Portal](#).
- **Username and password**—If you would rather provision your satellites without manually entering the serial numbers of the satellite devices into the portal configuration, you can instead require the satellite administrator to authenticate when establishing the initial connection to the portal. Although the portal will always look for the serial number in the initial request from the satellite, if it cannot identify the serial number, the satellite administrator must provide a username and password to authenticate to the portal. Because the portal will always fall back to this form of authentication, you must create an authentication profile in order to commit the portal configuration. This requires that you set up an authentication profile for the portal LSVPN configuration even if you plan to authenticate satellites using the serial number.



The following workflow describes how to set up the portal to authenticate satellites against an existing authentication service. GlobalProtect LSVPN supports external authentication using a local database, LDAP (including Active Directory), Kerberos, TACACS+, or RADIUS.

<b>Set Up Satellite Authentication</b>	
<p><b>Step 1</b> (External authentication only) Create a server profile on the portal.</p> <p>The server profile defines how the firewall connects to an external authentication service to validate the authentication credentials that the satellite device administrator enters.</p> <p> If you use local authentication, skip this step and instead add a local user for the satellite device administrator: see <a href="#">Create the local database</a>.</p>	<p>Configure a server profile for the authentication service type:</p> <ul style="list-style-type: none"><li>• <a href="#">Configure a RADIUS Server Profile</a>.</li><li>• <a href="#">Configure a TACACS+ Server Profile</a>.</li><li>• <a href="#">Configure an LDAP Server Profile</a>. If you use LDAP to connect to Active Directory (AD), create a separate LDAP server profile for every AD domain.</li><li>• <a href="#">Configure a Kerberos Server Profile</a>.</li></ul>
<p><b>Step 2</b> <a href="#">Configure an authentication profile</a>.</p> <p>The authentication profile defines which server profile to use to authenticate satellite devices.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Authentication Profile</b> and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> for the profile and then select the authentication <b>Type</b>. If the <b>Type</b> is an external service, select the <b>Server Profile</b> you created in <b>Step 1</b>. If you added a local user instead, set the <b>Type</b> to <b>Local Database</b>.</li><li>3. Click <b>OK</b> and <b>Commit</b>.</li></ol>

# Configure GlobalProtect Gateways for LSVPN

Because the GlobalProtect configuration that the portal delivers to the satellites includes the list of gateways the satellite can connect to, it is a good idea to configure the gateways before configuring the portal.

- ▲ Prerequisite Tasks
- ▲ Configure the Gateway

## Prerequisite Tasks

Before you can configure the GlobalProtect gateway, you must complete the following tasks:

- [Create Interfaces and Zones for the LSVPN](#) on the interface where you will configure each gateway. You must configure both the physical interface and the virtual tunnel interface.
- [Enable SSL Between GlobalProtect LSVPN Components](#) by configuring the gateway server certificates, SSL/TLS service profiles, and certificate profile required to establish a mutual SSL/TLS connection from the GlobalProtect satellite devices to the gateway.

## Configure the Gateway

After you have completed the [Prerequisite Tasks](#), configure each GlobalProtect gateway to participate in the LSVPN as follows:

<b>Configure the Gateway for LSVPN</b>	
<b>Step 1</b> Add a gateway.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; GlobalProtect &gt; Gateways</b> and click <b>Add</b>.</li><li>2. On the <b>General</b> tab, enter a <b>Name</b> for the gateway. The gateway name should not contain any spaces and as a best practice it should include the location or other descriptive information that will help identify the gateway.</li><li>3. (Optional) Select the virtual system to which this gateway belongs from the <b>Location</b> field.</li></ol>
<b>Step 2</b> Specify the network information to enable satellite devices to connect to the gateway.  If you haven't yet created the network interface for the gateway, see <a href="#">Create Interfaces and Zones for the LSVPN</a> for instructions. If you haven't yet created an SSL/TLS Service profile for the gateway, see <a href="#">Deploy Server Certificates to the GlobalProtect LSVPN Components</a> .	<ol style="list-style-type: none"><li>1. Select the <b>Interface</b> that satellite devices will use for ingress access to the gateway.</li><li>2. Select the <b>IP Address</b> for gateway access.</li><li>3. Select the <b>SSL/TLS Service Profile</b> for the gateway.</li></ol>

<b>Configure the Gateway for LSVPN (Continued)</b>	
<b>Step 3</b> Select the certificate profile for the gateway to use to authenticate satellite devices attempting to establish tunnels.  If you have not yet set up the certificate profile, see <a href="#">Enable SSL Between GlobalProtect LSVPN Components</a> for instructions.	Select the <b>Certificate Profile</b> to you created for SSL communication between the LSVPN components.
<b>Step 4</b> Configure the tunnel parameters and enable tunneling.	<ol style="list-style-type: none"> <li>On the GlobalProtect Gateway dialog, select <b>Satellite Configuration &gt; Tunnel Settings</b>.</li> <li>Select the <b>Tunnel Configuration</b> check box to enable tunneling.</li> <li>Select the <b>Tunnel Interface</b> you defined in <b>Step 2</b> in <a href="#">Create Interfaces and Zones for the LSVPN</a>.</li> <li>(Optional) If you want to preserve the Type of Service (ToS) information in the encapsulated packets, select the <b>Copy TOS</b> check box.</li> </ol>
<b>Step 5</b> (Optional) Enable tunnel monitoring.  Tunnel monitoring enables satellite devices to monitor its gateway tunnel connection, allowing it to failover to a backup gateway if the connection fails. Failover to another gateway is the only type of tunnel monitoring profile supported with LSVPN.	<ol style="list-style-type: none"> <li>Select the <b>Tunnel Monitoring</b> check box.</li> <li>Specify the <b>Destination IP</b> address the satellite devices should use to determine if the gateway is active. Alternatively, if you configured an IP address for the tunnel interface, you can leave this field blank and the tunnel monitor will instead use the tunnel interface to determine if the connection is active.</li> <li>Select <b>Failover</b> from the <b>Tunnel Monitor Profile</b> drop-down (this is the only supported tunnel monitor profile for LSVPN).</li> </ol>
<b>Step 6</b> Select the IPSec Crypto profile to use when establishing tunnel connections.  The profile specifies the type of IPSec encryption and the authentication method for securing the data that will traverse the tunnel. Because both tunnel endpoints in an LSVPN are trusted firewalls within your organization, you can typically use the default (predefined) profile, which uses ESP as the IPSec protocol, group2 for the DH group, AES-128-CBC for encryption, and SHA-1 for authentication.	In the <b>IPSec Crypto Profile</b> drop-down, select <b>default</b> to use the predefined profile or select <b>New IPSec Crypto Profile</b> to define a new profile. For details on the authentication and encryption options, see <a href="#">Define IPSec Crypto Profiles</a> .

<b>Configure the Gateway for LSVPN (Continued)</b>	
<p><b>Step 7</b> Configure the network settings to assign the satellite devices during establishment of the IPSec tunnel.</p> <p> You can also configure the satellite device to push the DNS settings to its local clients by configuring a DHCP server on the firewall hosting the satellite. In this configuration, the satellite will push DNS settings it learns from the gateway to the DHCP clients.</p>	<ol style="list-style-type: none"> <li>On the GlobalProtect Gateway dialog, select <b>Satellite Configuration &gt; Network Settings</b>.</li> <li>(Optional) If clients local to the satellite device need to resolve FQDNs on the corporate network, configure the gateway to push DNS settings to the satellites in one of the following ways: <ul style="list-style-type: none"> <li>Manually define the <b>Primary DNS</b>, <b>Secondary DNS</b>, and <b>DNS Suffix</b> settings to push to the satellites.</li> <li>If the gateway has an interface that is configured as a DHCP client, you can set the <b>Inheritance Source</b> to that interface and the GlobalProtect satellites will be assigned the same settings received by the DHCP client.</li> </ul> </li> <li>To specify the <b>IP Pool</b> of addresses to assign the tunnel interface on the satellite devices when the VPN is established, click <b>Add</b> and then specify the IP address range(s) to use.</li> <li>To define what destination subnets to route through the tunnel click <b>Add</b> in the <b>Access Route</b> area and then enter the routes as follows: <ul style="list-style-type: none"> <li>If you want to route all traffic from the satellites through the tunnel, leave this field blank. Note that in this case, all traffic except traffic destined for the local subnet will be tunneled to the gateway.</li> <li>To route only some traffic through the gateway (called <i>split tunneling</i>), specify the destination subnets that must be tunneled. In this case, the satellite will route traffic that is not destined for a specified access route using its own routing table. For example, you may choose to only tunnel traffic destined for your corporate network, and use the local satellite to safely enable Internet access.</li> <li>If you want to enable routing between satellites, enter the summary route for the network protected by each satellite.</li> </ul> </li> </ol>
<p><b>Step 8</b> (Optional) Define what routes, if any, the gateway will accept from satellites.</p> <p>By default, the gateway will not add any routes satellites advertise to its routing table. If you do not want the gateway to accept routes from satellites, you do not need to complete this step.</p>	<ol style="list-style-type: none"> <li>To enable the gateway to accept routes advertised by satellites, select <b>Satellite Configuration &gt; Route Filter</b>.</li> <li>Select the <b>Accept published routes</b> check box.</li> <li>To filter which of the routes advertised by the satellites to add to the gateway routing table, click <b>Add</b> and then define the subnets to include. For example, if all the satellites are configured with subnet 192.168.x.0/24 on the LAN side, configuring a permitted route of 192.168.0.0/16 to enable the gateway to only accept routes from the satellite if it is in the 192.168.0.0/16 subnet.</li> </ol>
<p><b>Step 9</b> Save the gateway configuration.</p>	<ol style="list-style-type: none"> <li>Click <b>OK</b> to save the settings and close the GlobalProtect Gateway dialog.</li> <li><b>Commit</b> the configuration.</li> </ol>

# Configure the GlobalProtect Portal for LSVPN

The GlobalProtect portal provides the management functions for your GlobalProtect LSVPN. Every satellite system that participates in the LSVPN receives configuration information from the portal, including information about available gateways as well as the certificate it needs in order to connect to the gateways.

The following sections provide procedures for setting up the portal:

- ▲ [Prerequisite Tasks](#)
- ▲ [Configure the Portal](#)
- ▲ [Define the Satellite Configurations](#)

## Prerequisite Tasks

Before configuring the GlobalProtect portal, you must complete the following tasks:

- [Create Interfaces and Zones for the LSVPN](#) on the interface where you will configure the portal.
- [Enable SSL Between GlobalProtect LSVPN Components](#) by creating an SSL/TLS service profile for the portal server certificate, issuing gateway server certificates, and configuring the portal to issue server certificates for the GlobalProtect satellite devices.
- [Configure the Portal to Authenticate Satellites](#) by defining the authentication profile that the portal will use to authenticate satellite devices if the serial number is not available.
- [Configure GlobalProtect Gateways for LSVPN](#).

## Configure the Portal

After you have completed the [Prerequisite Tasks](#), configure the GlobalProtect portal as follows:

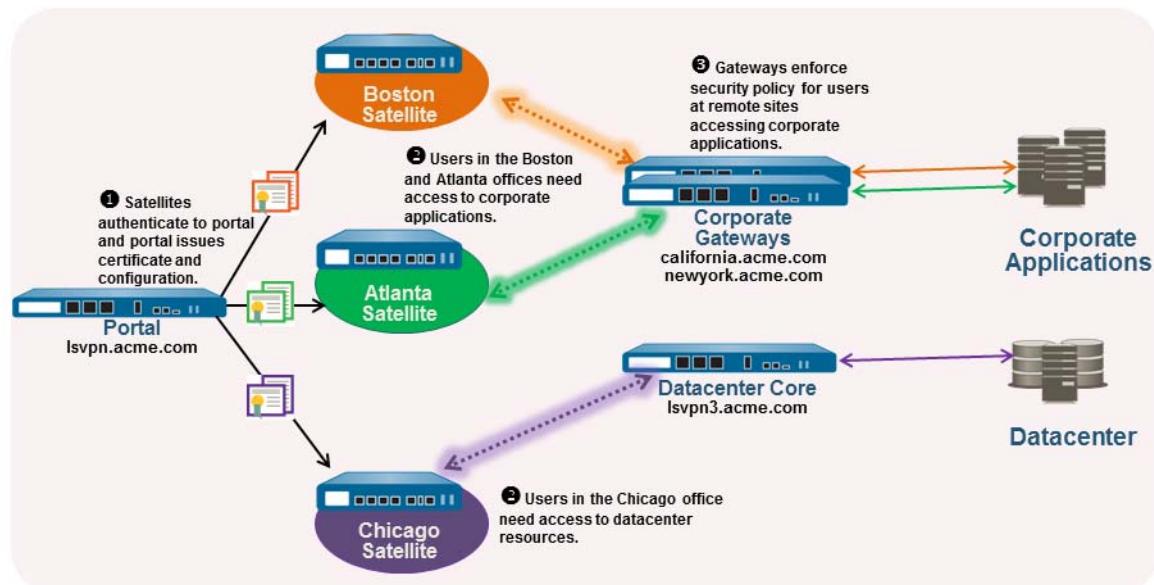
<b>Configure the Portal for LSVPN</b>	
Step 1 Add the portal.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; GlobalProtect &gt; Portals</b> and click <b>Add</b>.</li><li>2. On the <b>Portal Configuration</b> tab, enter a <b>Name</b> for the portal. The portal name should not contain any spaces.</li><li>3. (Optional) Select the virtual system to which this portal belongs from the <b>Location</b> field.</li></ol>

<b>Configure the Portal for LSVPN (Continued)</b>	
<p><b>Step 2</b> Specify the network information to enable satellite devices to connect to the portal.</p> <p>If you haven't yet created the network interface for the portal, see <a href="#">Create Interfaces and Zones for the LSVPN</a> for instructions. If you haven't yet created an SSL/TLS service profile for the portal and issued gateway certificates, see <a href="#">Deploy Server Certificates to the GlobalProtect LSVPN Components</a>.</p>	<ol style="list-style-type: none"> <li>Select the <b>Interface</b> that satellite devices will use for ingress access to the portal.</li> <li>Select the <b>IP Address</b> for satellite device access to the portal.</li> <li>Select the <b>SSL/TLS Service Profile</b> to enable the satellite device to establish an SSL/TLS connection to the portal.</li> </ol>
<p><b>Step 3</b> Specify an authentication profile for authenticating satellite devices.</p> <p> If the portal can't validate the serial numbers of connecting satellite devices, it will fall back to the authentication profile. Therefore, you must configure an authentication profile before you can save the portal configuration (by clicking <b>OK</b>).</p>	<ul style="list-style-type: none"> <li>Select the <b>Authentication Profile</b> you defined for authenticating satellite devices.</li> <li>If you haven't yet configured the authentication profile, select <b>New Authentication Profile</b> to <a href="#">Configure an authentication profile</a>.</li> </ul>
<p><b>Step 4</b> Continue with defining the configurations to push to the satellite devices or, if you have already created the satellite device configurations, save the portal configuration.</p>	Click <b>OK</b> to save the portal configuration or continue to <a href="#">Define the Satellite Configurations</a> .

## Define the Satellite Configurations

When a GlobalProtect satellite connects and successfully authenticates to the GlobalProtect portal, the portal delivers a satellite configuration, which specifies what gateways the satellite can connect to. If all your satellites will use the same gateway and certificate configurations, you can create a single satellite configuration to deliver to all satellites upon successful authentication. However, if you require different satellite configurations—for example if you want one group of satellites to connect to one gateway and another group of satellites to connect to a different gateway—you can create a separate satellite configuration for each. The portal will then use the enrollment username/group name or the serial number of the satellite device to determine which satellite configuration to deploy. As with security rule evaluation, the portal looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration to the satellite.

For example, the following figure shows a network in which some branch offices require VPN access to the corporate applications protected by your perimeter firewalls and another site needs VPN access to the datacenter.



Use the following procedure to create one or more satellite configurations.

#### Create a GlobalProtect Satellite Configuration

<p><b>Step 1</b> Specify the certificates required to enable satellites to participate in the LSVPN.</p>	<ol style="list-style-type: none"> <li>Select <b>Network &gt; GlobalProtect &gt; Portals</b> and select the portal configuration for which you want to add a satellite configuration and then select the <b>Satellite Configuration</b> tab.</li> <li>In the <b>Trusted Root CA</b> field, click <b>Add</b> and then select the CA certificate used to issue the gateway server certificates. The portal will deploy the root CA certificate you add here to all satellites as part of the configuration to enable the satellite to establish an SSL connection with the gateways. As a best practice, all of your gateways should use the same issuer.           <p>If the root CA certificate used to issue your gateway server certificates is not on the portal, you can <b>Import</b> it now. See <a href="#">Enable SSL Between GlobalProtect LSVPN Components</a> for details on how to import a root CA certificate.</p> </li> <li>Select the Root CA certificate that the portal will use to issue certificates to satellites upon successfully authenticating them from the <b>Issuing Certificate</b> drop-down.</li> </ol>
<p><b>Step 2</b> Add a satellite configuration.</p> <p>The satellite configuration specifies the GlobalProtect LSVPN configuration settings to deploy to the connecting satellites. You must define at least one satellite configuration.</p>	<p>In the Satellite Configuration section, click <b>Add</b> and enter a <b>Name</b> for the configuration.</p> <p>If you plan to create multiple configurations, make sure the name you define for each is descriptive enough to allow you to distinguish them.</p>

<b>Create a GlobalProtect Satellite Configuration (Continued)</b>	
<p><b>Step 3</b> Specify which satellites to deploy this configuration to.</p> <p>The portal uses the <b>Enrollment User/User Group</b> settings and/or <b>Devices</b> serial numbers to match a satellite to a configuration. Therefore, if you have multiple configurations, be sure to order them properly. As soon as the portal finds a match, it will deliver the configuration. Therefore, more specific configurations must precede more general ones. See <a href="#">Step 6</a> for instructions on ordering the list of satellite configurations.</p>	<p>Specify the match criteria for the satellite configuration as follows:</p> <ul style="list-style-type: none"> <li>To restrict this configuration to satellite devices with specific serial numbers, select the <b>Devices</b> tab, click <b>Add</b>, and enter serial number (you do not need to enter the satellite hostname; it will be automatically added when the satellite connects). Repeat this step for each satellite you want to receive this configuration.</li> <li>Select the <b>Enrollment User/User Group</b> tab, click <b>Add</b>, and then select the user or group you want to receive this configuration. Satellites that do not match on serial number will be required to authenticate as a user specified here (either an individual user or group member).</li> </ul> <p> Before you can restrict the configuration to specific groups, you must <a href="#">Map Users to Groups</a>.</p>
<p><b>Step 4</b> Specify the gateways that satellites with this configuration can establish VPN tunnels with.</p> <p> Routes published by the gateway are installed on the satellite as static routes. The metric for the static route is 10x the routing priority. If you have more than one gateway, make sure to also set the routing priority to ensure that routes advertised by backup gateways have higher metrics compared to the same routes advertised by primary gateways. For example, if you set the routing priority for the primary gateway and backup gateway to 1 and 10 respectively, the satellite will use 10 as the metric for the primary gateway and 100 as the metric for the backup gateway.</p>	<ol style="list-style-type: none"> <li>On the <b>Gateways</b> tab, click <b>Add</b>.</li> <li>Enter a descriptive <b>Name</b> for the gateway. The name you enter here should match the name you defined when you configured the gateway and should be descriptive enough identify the location of the gateway.</li> <li>Enter the FQDN or IP address of the interface where the gateway is configured in the <b>Gateways</b> field. The address you specify must exactly match the Common Name (CN) in the gateway server certificate.</li> <li>(Optional) If you are adding two or more gateways to the configuration, the <b>Routing Priority</b> helps the satellite pick the preferred gateway. Enter a value in the range of 1-25, with lower numbers having the higher priority (that is, the gateway the satellite will connect to if all gateways are available). The satellite will multiply the routing priority by 10 to determine the routing metric.</li> </ol>
<p><b>Step 5</b> Save the satellite configuration.</p>	<ol style="list-style-type: none"> <li>Click <b>OK</b> to save the satellite configuration.</li> <li>If you want to add another satellite configuration, repeat <a href="#">Step 2</a> through <a href="#">Step 5</a>.</li> </ol>
<p><b>Step 6</b> Arrange the satellite configurations so that the proper configuration is deployed to each satellite.</p>	<ul style="list-style-type: none"> <li>To move a satellite configuration up on the list of configurations, select the configuration and click <b>Move Up</b>.</li> <li>To move a satellite configuration down on the list of configurations, select the configuration and click <b>Move Down</b>.</li> </ul>
<p><b>Step 7</b> Save the portal configuration.</p>	<ol style="list-style-type: none"> <li>Click <b>OK</b> to save the settings and close the GlobalProtect Portal dialog.</li> <li><b>Commit</b> your changes.</li> </ol>

# Prepare the Satellite Device to Join the LSVPN

In order to participate in the LSVPN, the satellite devices require a minimal amount of configuration. Because the required configuration is minimal, you can pre-configure the devices before shipping them to your branch offices for installation.

## Prepare the Satellite Device to Join the GlobalProtect LSVPN

<b>Step 1</b> Configure a Layer 3 interface.	This is the physical interface the satellite will use to connect to the portal and the gateway. This interface must be in a zone that allows access outside of the local trust network. As a best practice, create a dedicated zone for VPN connections for visibility and control over traffic destined for the corporate gateways.
<b>Step 2</b> Configure the logical tunnel interface for the tunnel to use to establish VPN tunnels with the GlobalProtect gateways.   IP addresses are not required on the tunnel interface unless you plan to use dynamic routing. However, assigning an IP address to the tunnel interface can be useful for troubleshooting connectivity issues.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces &gt; Tunnel</b> and click <b>Add</b>.</li><li>2. In the <b>Interface Name</b> field, specify a numeric suffix, such as <b>.2</b>.</li><li>3. On the <b>Config</b> tab, expand the <b>Security Zone</b> drop-down and select an existing zone or create a separate zone for VPN tunnel traffic by clicking <b>New Zone</b> and defining a <b>Name</b> for new zone (for example <i>lsvpnsat</i>).</li><li>4. In the <b>Virtual Router</b> drop-down, select <b>default</b>.</li><li>5. (Optional) If you want to assign an IP address to the tunnel interface, select the <b>IPv4</b> tab, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 2.2.2.11/24.</li><li>6. To save the interface configuration, click <b>OK</b>.</li></ol>

<b>Prepare the Satellite Device to Join the GlobalProtect LSVPN (Continued)</b>	
<p><b>Step 3</b> If you generated the portal server certificate using a Root CA that is not trusted by the satellite devices (for example, if you used self-signed certificates), import the root CA certificate used to issue the portal server certificate.</p> <p>The root CA certificate is required to enable the satellite device to establish the initial connection with the portal to obtain the LSVPN configuration.</p>	<ol style="list-style-type: none"> <li>1. Download the CA certificate that was used to generate the portal server certificates. If you are using self-signed certificates, export the root CA certificate from the portal as follows:             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b>.</li> <li>b. Select the CA certificate, and click <b>Export</b>.</li> <li>c. Select <b>Base64 Encoded Certificate (PEM)</b> from the <b>File Format</b> drop-down and click <b>OK</b> to download the certificate. (You do not need to export the private key.)</li> </ol> </li> <li>2. Import the root CA certificate you just exported onto each satellite device as follows.             <ol style="list-style-type: none"> <li>a. Select <b>Device &gt; Certificate Management &gt; Certificates &gt; Device Certificates</b> and click <b>Import</b>.</li> <li>b. Enter a <b>Certificate Name</b> that identifies the certificate as your client CA certificate.</li> <li>c. <b>Browse</b> to the <b>Certificate File</b> you downloaded from the CA.</li> <li>d. Select <b>Base64 Encoded Certificate (PEM)</b> as the <b>File Format</b> and then click <b>OK</b>.</li> <li>e. Select the certificate you just imported on the <b>Device Certificates</b> tab to open it.</li> <li>f. Select <b>Trusted Root CA</b> and then click <b>OK</b>.</li> </ol> </li> </ol>
<p><b>Step 4</b> Configure the IPSec tunnel configuration.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; IPSec Tunnels</b> and click <b>Add</b>.</li> <li>2. On the <b>General</b> tab, enter a descriptive <b>Name</b> for the IPSec configuration.</li> <li>3. Select the <b>Tunnel Interface</b> you created for the satellite device.</li> <li>4. Select <b>GlobalProtect Satellite</b> as the <b>Type</b>.</li> <li>5. Enter the IP address or FQDN of the portal as the <b>Portal Address</b>.</li> <li>6. Select the Layer 3 <b>Interface</b> you configured for the satellite device.</li> <li>7. Select the <b>Local IP Address</b> to use on the selected interface.</li> </ol>

### Prepare the Satellite Device to Join the GlobalProtect LSVPN (Continued)

<p><b>Step 5</b> (Optional) Configure the satellite to publish local routes to the gateway.</p> <p>Pushing routes to the gateway enables traffic to the subnets local to the satellite via the gateway. However, you must also configure the gateway to accept the routes as detailed in <a href="#">Step 8</a> in <a href="#">Configure the Gateway</a>.</p>	<ol style="list-style-type: none"> <li>To enable the satellite to push routes to the gateway, on the <b>Advanced</b> tab select <b>Publish all static and connected routes to Gateway</b>.  If you select this check box, the firewall will forward all static and connected routes from the satellite to the gateway. However, to prevent the creation of routing loops, the firewall will apply some route filters, such as the following: <ul style="list-style-type: none"> <li>• Default routes</li> <li>• Routes within a virtual router other than the virtual router associated with the tunnel interface</li> <li>• Routes using the tunnel interface</li> <li>• Routes using the physical interface associated with the tunnel interface</li> </ul> </li> <li>(Optional) If you only want to push routes for specific subnets rather than all routes, click <b>Add</b> in the Subnet section and specify which subnet routes to publish.</li> </ol>																												
<p><b>Step 6</b> Save the satellite configuration.</p>	<ol style="list-style-type: none"> <li>Click <b>OK</b> to save the IPSec tunnel settings.</li> <li>Click <b>Commit</b>.</li> </ol>																												
<p><b>Step 7</b> If required, provide the credentials to allow the satellite to authenticate to the portal.</p> <p>This step is only required if the portal was unable to find a serial number match in its configuration or if the serial number didn't work. In this case, the satellite will not be able to establish the tunnel with the gateway(s).</p>	<ol style="list-style-type: none"> <li>Select <b>Network &gt; IPSec Tunnels</b> and click the <b>Gateway Info</b> link in the Status column of the tunnel configuration you created for the LSVPN.</li> <li>Click the <b>enter credentials</b> link in the <b>Portal Status</b> field and username and password required to authenticate the satellite to the portal.</li> </ol> <p>After the portal successfully authenticates to the portal, it will receive its signed certificate and configuration, which it will use to connect to the gateway(s). You should see the tunnel establish and the <b>Status</b> change to <b>Active</b>.</p>  <table border="1" data-bbox="693 1351 1379 1668"> <thead> <tr> <th colspan="7">GlobalProtect Satellite Configuration and Runtime Status</th> </tr> <tr> <th>Name</th> <th>IP</th> <th>Port</th> <th>Protocol</th> <th>Local IP</th> <th>Tunnel Monitor</th> <th>Route Sharing</th> </tr> </thead> <tbody> <tr> <td>levpn5020</td> <td>172.16.222.254</td> <td>443</td> <td>SSL</td> <td>172.16.222.30</td> <td>Interval - 0 sec Threshold - 0 sec</td> <td>Received GW Access Routes: 172.16.0.0/16, 4.2.2.1/32, 4.2.2.2/32 All routes accepted</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	GlobalProtect Satellite Configuration and Runtime Status							Name	IP	Port	Protocol	Local IP	Tunnel Monitor	Route Sharing	levpn5020	172.16.222.254	443	SSL	172.16.222.30	Interval - 0 sec Threshold - 0 sec	Received GW Access Routes: 172.16.0.0/16, 4.2.2.1/32, 4.2.2.2/32 All routes accepted							
GlobalProtect Satellite Configuration and Runtime Status																													
Name	IP	Port	Protocol	Local IP	Tunnel Monitor	Route Sharing																							
levpn5020	172.16.222.254	443	SSL	172.16.222.30	Interval - 0 sec Threshold - 0 sec	Received GW Access Routes: 172.16.0.0/16, 4.2.2.1/32, 4.2.2.2/32 All routes accepted																							

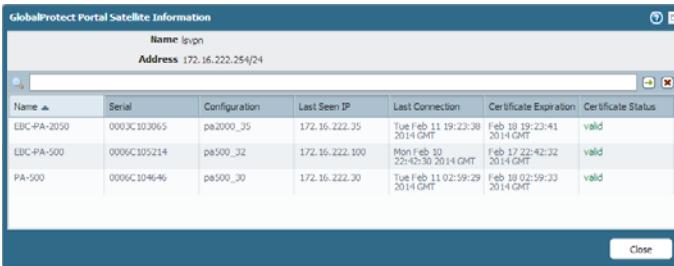
## Verify the LVPN Configuration

After configuring the portal, gateways, and satellite devices, verify that the satellites are able to connect to the portal and gateway and establish VPN tunnels with the gateway(s).

### Verify the LVPN Configuration

**Step 1** Verify satellite connectivity with portal.

From the firewall hosting the portal, verify that satellites are successfully connecting by selecting **Network > GlobalProtect > Portal** and clicking **Satellite Info** in the Info column of the portal configuration entry.



**Step 1** Verify satellite connectivity with the gateway(s).

On each firewall hosting a gateway, verify that satellites are able to establish VPN tunnels by selecting **Network > GlobalProtect > Gateways** and click **Satellite Info** in the Info column of the gateway configuration entry. Satellites that have successfully established tunnels with the gateway will display on the **Active Satellites** tab.



**Step 1** Verify LVPN tunnel status on the satellite.

On each firewall hosting a satellite, verify the tunnel status by selecting **Network > IPSec Tunnels** and verify active Status as indicated by a green icon.

Name	Status	Type	IKE Gateway/Satellite				Tunnel Interface			
			Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone
levon5000		global-protect-satellite	ethernet...	172.16....		Gateway Info	tunnel.2	levon (Show Routes)	vsys1	levonsat

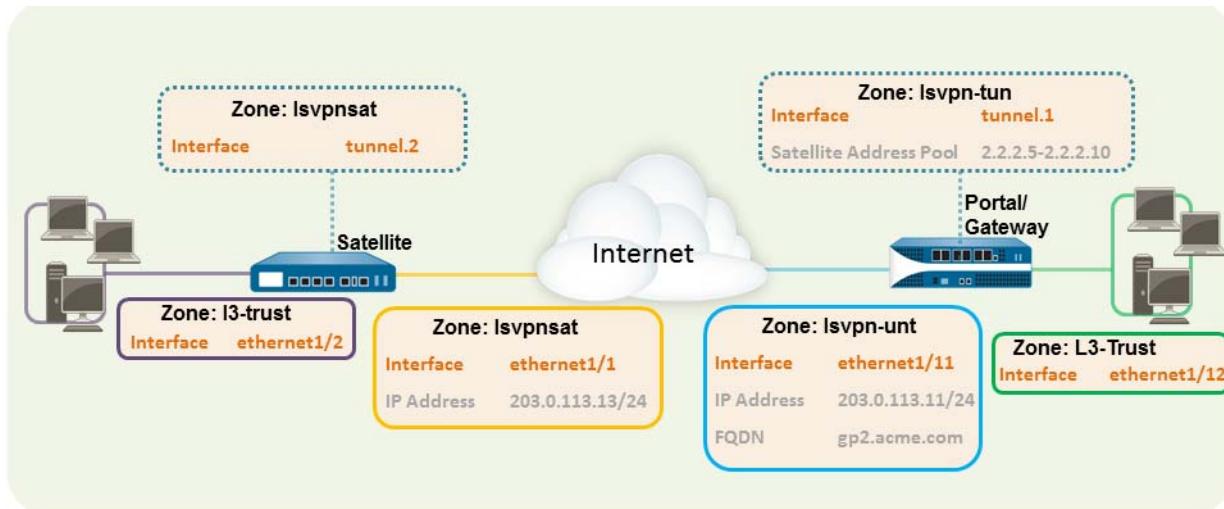
## LSVPN Quick Configs

The following sections provide step-by-step instructions for configuring some common GlobalProtect LSVN deployments:

- ▲ [Basic LSVN Configuration with Static Routing](#)
- ▲ [Advanced LSVN Configuration with Dynamic Routing](#)

## Basic LVPN Configuration with Static Routing

This quick config shows the fastest way to get up and running with LVPN. In this example, a single firewall at the corporate headquarters site is configured as both a portal and a gateway. Satellite devices can be quickly and easily deployed with minimal configuration for optimized scalability.



The following workflow shows the steps for setting up this basic configuration:

### Quick Config: Basic LVPN with Static Routing

Step 1 Configure a Layer 3 interface.	<p>In this example, the Layer 3 interface on the portal/gateway requires the following configuration:</p> <ul style="list-style-type: none"> <li><b>Interface</b>—ethernet1/11</li> <li><b>Security Zone</b>—lvpn-unt</li> <li><b>IPv4</b>—203.0.113.11/24</li> </ul>
Step 2 On the firewall(s) hosting GlobalProtect gateway(s), configure the logical tunnel interface that will terminate VPN tunnels established by the GlobalProtect satellites.  To enable visibility into users and groups connecting over the VPN, enable User-ID in the zone where the VPN tunnels terminate.	<p>In this example, the Tunnel interface on the portal/gateway requires the following configuration:</p> <ul style="list-style-type: none"> <li><b>Interface</b>—tunnel.1</li> <li><b>Security Zone</b>—lvpn-tun</li> </ul>

**Quick Config: Basic LVPN with Static Routing (Continued)**

<b>Step 3</b>	Create the security policy rule to enable traffic flow between the VPN zone where the tunnel terminates (lvpn-tun) and the trust zone where the corporate applications reside (L3-Trust).	The following is an example of a policy rule for allowing traffic to flow between the VPN zone and the trust zone:																		
		<table border="1"> <thead> <tr> <th>Name</th><th>Zone</th><th>Address</th><th>User</th><th>Zone</th><th>Address</th><th>Application</th><th>Service</th><th>Action</th></tr> </thead> <tbody> <tr> <td>lvpn Access</td><td>lvpn-tun</td><td>any</td><td>any</td><td>L3-Trust</td><td>any</td><td>adobe-creat... ms-exchange ms-office365</td><td>application-d...</td><td>✓</td></tr> </tbody> </table>	Name	Zone	Address	User	Zone	Address	Application	Service	Action	lvpn Access	lvpn-tun	any	any	L3-Trust	any	adobe-creat... ms-exchange ms-office365	application-d...	✓
Name	Zone	Address	User	Zone	Address	Application	Service	Action												
lvpn Access	lvpn-tun	any	any	L3-Trust	any	adobe-creat... ms-exchange ms-office365	application-d...	✓												
<b>Step 4</b>	Assign an SSL/TLS Service profile to the portal/gateway. The profile must reference a self-signed server certificate.  The certificate subject name must match the FQDN or IP address of the Layer 3 interface you create for the portal/gateway.	<ol style="list-style-type: none"> <li>On the firewall hosting the GlobalProtect portal, create the root CA certificate for signing the certificates of the GlobalProtect components. In this example, the root CA certificate, lvpn-CA, will be used to issue the server certificate for the portal/gateway. In addition, the portal will use this root CA certificate to sign the CSRs from the satellite devices.</li> <li>Create SSL/TLS service profiles for the GlobalProtect portal and gateways.</li> </ol> <p>Because the portal and gateway are on the same interface in this example, they can share an SSL/TLS Service profile that uses the same server certificate. In this example, the profile is named lvpnserver.</p>																		
<b>Step 5</b>	Create a certificate profile.	In this example, the certificate profile lvpn-profile, references the root CA certificate lvpn-CA. The gateway will use this certificate profile to authenticate satellite devices attempting to establish VPN tunnels.																		
<b>Step 6</b>	Configure an authentication profile for the portal to use if the satellite device serial number is not available.	<ol style="list-style-type: none"> <li>Create one type of server profile on the portal: <ul style="list-style-type: none"> <li>Configure a RADIUS Server Profile.</li> <li>Configure a TACACS+ Server Profile.</li> <li>Configure an LDAP Server Profile. If you use LDAP to connect to Active Directory (AD), create a separate LDAP server profile for every AD domain.</li> <li>Configure a Kerberos Server Profile.</li> </ul> </li> <li>Configure an authentication profile. In this example, the profile lvpn-sat is used to authenticate satellite devices.</li> </ol>																		

**Quick Config: Basic LVPN with Static Routing (Continued)**

Step 7 Configure the Gateway for LVPN.	<p>Select <b>Network &gt; GlobalProtect &gt; Gateways</b> and <b>Add</b> a configuration. This example requires the following gateway configuration:</p> <ul style="list-style-type: none"><li>• <b>Interface</b>—ethernet1/11</li><li>• <b>IP Address</b>—203.0.113.11/24</li><li>• <b>SSL/TLS Server Profile</b>—lsvpnserver</li><li>• <b>Certificate Profile</b>—lsvpn-profile</li><li>• <b>Tunnel Interface</b>—tunnel.1</li><li>• <b>Primary DNS/Secondary DNS</b>—4.2.2.1/4.2.2.2</li><li>• <b>IP Pool</b>—2.2.2.111-2.2.2.120</li><li>• <b>Access Route</b>—10.2.10.0/24</li></ul>
Step 8 Configure the Portal for LVPN.	<p>Select <b>Network &gt; GlobalProtect &gt; Portal</b> and <b>Add</b> a configuration. This example requires the following portal configuration:</p> <ul style="list-style-type: none"><li>• <b>Interface</b>—ethernet1/11</li><li>• <b>IP Address</b>—203.0.113.11/24</li><li>• <b>SSL/TLS Server Profile</b>—lsvpnserver</li><li>• <b>Authentication Profile</b>—lsvpn-sat</li></ul>
Step 9 Create a GlobalProtect Satellite Configuration.	<p>On the <b>Satellite Configuration</b> tab in the portal configuration, <b>Add</b> a Satellite Configuration and a Trusted Root CA and specify the CA the portal will use to issue certificates for the satellites. In this example the required settings are as following:</p> <ul style="list-style-type: none"><li>• <b>Gateway</b>—203.0.113.11</li><li>• <b>Issuing Certificate</b>—lsvpn-CA</li><li>• <b>Trusted Root CA</b>—lsvpn-CA</li></ul>

**Quick Config: Basic LVPN with Static Routing (Continued)**

<p><b>Step 10</b> Prepare the Satellite Device to Join the LVPN.</p>	<p>The satellite configuration in this example requires the following settings:</p> <p><b>Interface Configuration</b></p> <ul style="list-style-type: none"><li>• Layer 3 interface—ethernet1/1, 203.0.113.13/24</li><li>• Tunnel interface—tunnel.2</li><li>• Zone—lsvpnsat</li></ul> <p><b>Root CA Certificate from Portal</b></p> <ul style="list-style-type: none"><li>• lsvpn-CA</li></ul> <p><b>IPSec Tunnel Configuration</b></p> <ul style="list-style-type: none"><li>• <b>Tunnel Interface</b>—tunnel.2</li><li>• <b>Portal Address</b>—203.0.113.11</li><li>• <b>Interface</b>—ethernet1/1</li><li>• <b>Local IP Address</b>—203.0.113.13/24</li><li>• <b>Publish all static and connected routes to Gateway</b>—enabled</li></ul>
--	---

## Advanced LVPN Configuration with Dynamic Routing

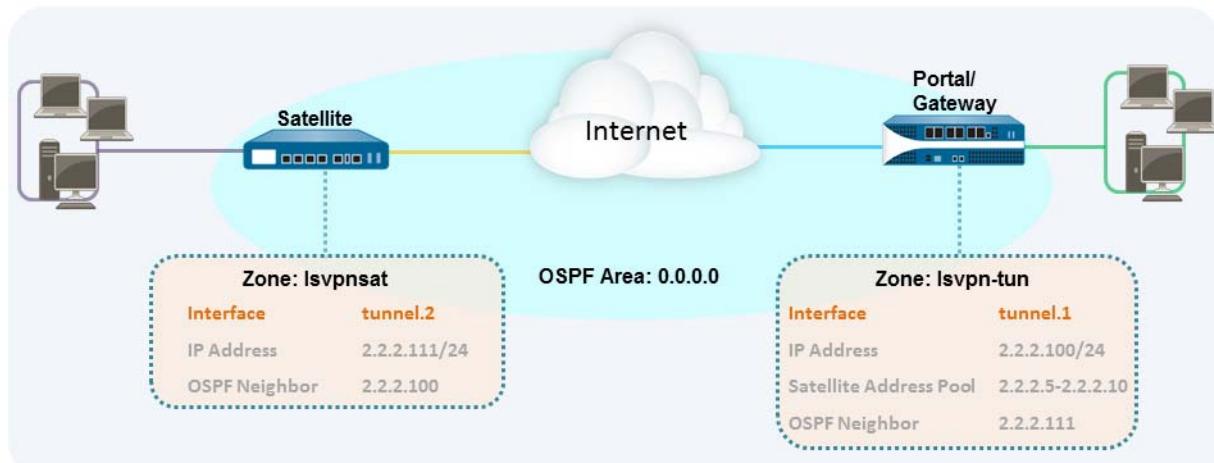
In larger LVPN deployments with multiple gateways and many satellites, investing a little more time in the initial configuration to set up dynamic routing will simplify the maintenance of gateway configurations because access routes will update dynamically. The following example configuration shows how to extend the basic LVPN configuration to configure OSPF as the dynamic routing protocol.

Setting up an LVPN to use OSPF for dynamic routing requires the following additional steps on the gateways and the satellites:

- Manual assignment of IP addresses to tunnel interfaces on all gateways and satellites.
- Configuration of OSPF point-to-multipoint (P2MP) on the virtual router on all gateways and satellites. In addition, as part of the OSPF configuration on each gateway, you must manually define the tunnel IP address of each satellite as an OSPF neighbor. Similarly, on each satellite, you must manually define the tunnel IP address of each gateway as an OSPF neighbor.

Although dynamic routing requires additional setup during the initial configuration of the LVPN, it reduces the maintenance tasks associated with keeping routes up to date as topology changes occur on your network.

The following figure shows an LVPN dynamic routing configuration. This example shows how to configure OSPF as the dynamic routing protocol for the VPN.



For a basic setup of a LVPN, follow the steps in [Basic LVPN Configuration with Static Routing](#). You can then complete the steps in the following workflow to extend the configuration to use dynamic routing rather than static routing.

<b>Quick Config: LSVPN with Dynamic Routing</b>	
<b>Step 1</b> Add an IP address to the tunnel interface configuration on each gateway and each satellite.	<p>Complete the following steps on each gateway and each satellite:</p> <ol style="list-style-type: none"> <li>Select <b>Network &gt; Interfaces &gt; Tunnel</b> and select the tunnel configuration you created for the LSVPN to open the Tunnel Interface dialog.</li> </ol> <p>If you have not yet created the tunnel interface, see <a href="#">Step 2</a> in <a href="#">Quick Config: Basic LSVPN with Static Routing</a>.</p> <ol style="list-style-type: none"> <li>On the <b>IPv4</b> tab, click <b>Add</b> and then enter an IP address and subnet mask. For example, to add an IP address for the gateway tunnel interface you would enter 2.2.2.100/24.</li> <li>Click <b>OK</b> to save the configuration.</li> </ol>
<b>Step 2</b> Configure the dynamic routing protocol on the gateway.	<p>To configure OSPF on the gateway:</p> <ol style="list-style-type: none"> <li>Select <b>Network &gt; Virtual Routers</b> and select the virtual router associated with your VPN interfaces.</li> <li>On the <b>Areas</b> tab, click <b>Add</b> to create the backbone area, or, if it is already configured, click on the area ID to edit it.</li> <li>If you are creating a new area, enter an <b>Area ID</b> on the <b>Type</b> tab.</li> <li>On the <b>Interface</b> tab, click <b>Add</b> and select the tunnel <b>Interface</b> you created for the LSVPN.</li> <li>Select <b>p2mp</b> as the <b>Link Type</b>.</li> <li>Click <b>Add</b> in the Neighbors section and enter the IP address of the tunnel interface of each satellite device, for example 2.2.2.111.</li> <li>Click <b>OK</b> twice to save the virtual router configuration and then <b>Commit</b> the changes on the gateway.</li> <li>Repeat this step each time you add a new satellite to the LSVPN.</li> </ol>
<b>Step 3</b> Configure the dynamic routing protocol on the satellite.	<p>To configure OSPF on the satellite:</p> <ol style="list-style-type: none"> <li>Select <b>Network &gt; Virtual Routers</b> and select the virtual router associated with your VPN interfaces.</li> <li>On the <b>Areas</b> tab, click <b>Add</b> to create the backbone area, or, if it is already configured, click on the area ID to edit it.</li> <li>If you are creating a new area, enter an <b>Area ID</b> on the <b>Type</b> tab.</li> <li>On the <b>Interface</b> tab, click <b>Add</b> and select the tunnel <b>Interface</b> you created for the LSVPN.</li> <li>Select <b>p2mp</b> as the <b>Link Type</b>.</li> <li>Click <b>Add</b> in the Neighbors section and enter the IP address of the tunnel interface of each GlobalProtect gateway, for example 2.2.2.100.</li> <li>Click <b>OK</b> twice to save the virtual router configuration and then <b>Commit</b> the changes on the gateway.</li> <li>Repeat this step each time you add a new gateway.</li> </ol>

### Quick Config: LSVPN with Dynamic Routing (Continued)

- Step 4** Verify that the gateways and satellites are able to form router adjacencies.

- On each satellite and each gateway, confirm that peer adjacencies have formed and that routing table entries have been created for the peers (that is, the satellites have routes to the gateways and the gateways have routes to the satellites). Select **Network > Virtual Router** and click the **More Runtime Stats** link for the virtual router you are using for the LSVPN. On the Routing tab, verify that the LSVPN peer has a route.

Destination	Next Hop	Metric	Flags	Age	Interface
2.2.2.0/24	2.2.2.100	0	A C		tunnel.1
2.2.2.100/32	0.0.0.0	0	A H		
2.2.2.111/32	2.2.2.111	10	A Oi	1360303	tunnel.1

- On the **OSPF > Interface** tab, verify that the **Type** is **p2mp**.

Name	Address	Type	Passive	Area Id	Router Priority	Status
tunnel.1	2.2.2.100	p2mp		0.0.0.0	1	p2p

- On the **OSPF > Neighbor** tab, verify that the firewalls hosting your gateways have established router adjacencies with the firewalls hosting your satellites and vice versa. Also verify that the **Status** is **Full**, indicating that full adjacencies have been established.

Neighbor Address	Neighbor Router Id	Local Address Binding	Area Id	Neighbor Priority	Remaining Lifetime	Status
2.2.2.111	2.2.2.111	2.2.2.100	0.0.0.0	1	31	full





# Networking

---

All Palo Alto Networks® next-generation firewalls provide a flexible networking architecture that includes support for dynamic routing, switching, and VPN connectivity, and enables you to deploy the firewall into nearly any networking environment. When configuring the Ethernet ports on your firewall, you can choose from virtual wire, Layer 2, or Layer 3 interface deployments. In addition, to allow you to integrate into a variety of network segments, you can configure different types of interfaces on different ports. The [Interface Deployments](#) section provides basic information on each type of deployment. For more detailed deployment information, refer to [Designing Networks with Palo Alto Networks Firewalls](#).

The following topics describe networking concepts and how to integrate Palo Alto Networks next-generation firewalls into your network.

- ▲ [Interface Deployments](#)
- ▲ [Virtual Routers](#)
- ▲ [Static Routes](#)
- ▲ [RIP](#)
- ▲ [OSPF](#)
- ▲ [BGP](#)
- ▲ [Session Settings and Timeouts](#)
- ▲ [DHCP](#)
- ▲ [NAT](#)
- ▲ [NPTv6](#)
- ▲ [LACP](#)
- ▲ [ECMP](#)
- ▲ [LLDP](#)

For information on route distribution, refer to [Understanding Route Redistribution and Filtering](#).

# Interface Deployments

A Palo Alto Networks firewall can operate in multiple deployments at once because the deployments occur at the interface level. The following sections describe the deployments.

- ▲ Virtual Wire Deployments
- ▲ Layer 2 Deployments
- ▲ Layer 3 Deployments
- ▲ Tap Mode Deployments

## Virtual Wire Deployments

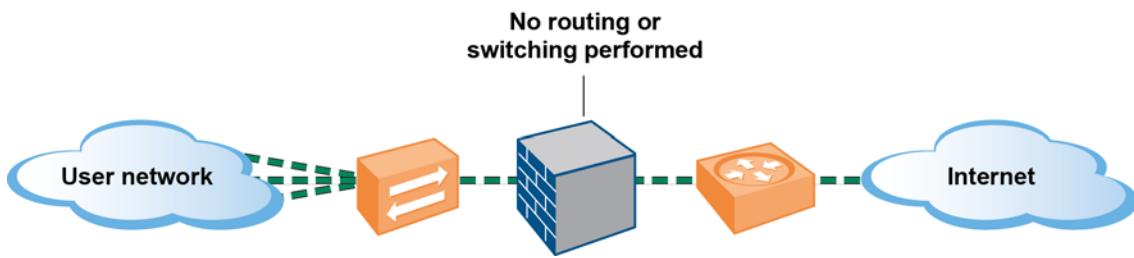
In a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together and should be used only when no switching or routing is needed.

A virtual wire deployment allows the following conveniences:

- Simplifies installation and configuration.
- Does not require any configuration changes to surrounding or adjacent network devices.

The virtual wire deployment shipped as the factory default configuration (default-vwire) binds together Ethernet ports 1 and 2 and allows all untagged traffic. You can, however, use a virtual wire to connect any two ports and configure it to block or allow traffic based on the virtual LAN (VLAN) tags; the VLAN tag “0” indicates untagged traffic. You can also create multiple subinterfaces, add them into different zones and then classify traffic according to a VLAN tag, or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

**Figure: Virtual Wire Deployment**



## Virtual Wire Subinterfaces

Virtual wire subinterfaces provide flexibility in enforcing distinct policies when you need to manage traffic from multiple customer networks. It allows you to separate and classify traffic into different zones (the zones can belong to separate virtual systems, if required) using the following criteria:

- **VLAN tags** —The example in [Figure: Virtual Wire Deployment with Subinterfaces \(VLAN Tags only\)](#), shows an Internet Service Provider (ISP) using virtual wire subinterfaces with VLAN tags to separate traffic for two different customers.
- **VLAN tags in conjunction with IP classifiers (address, range, or subnet)** — The following example shows an ISP with two separate virtual systems on a firewall that manages traffic from two different customers. On each virtual system, the example illustrates how virtual wire subinterfaces with VLAN tags and IP classifiers are used to classify traffic into separate zones and apply relevant policy for customers from each network.

#### Virtual Wire Subinterface Workflow

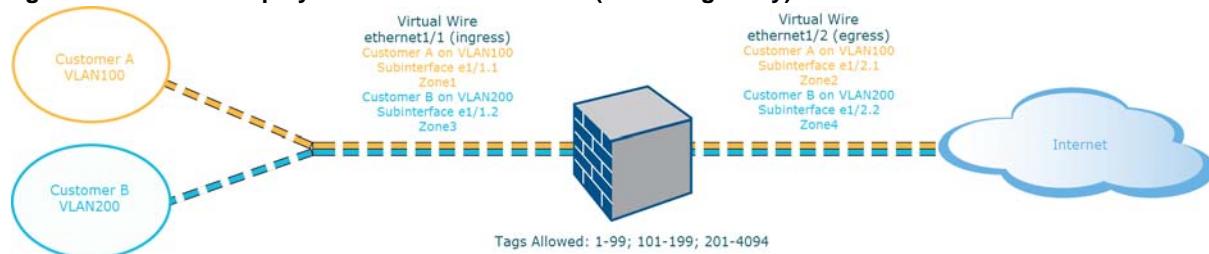
1. Configure two Ethernet interfaces as type virtual wire, and assign these interfaces to a virtual wire.
2. Create subinterfaces on the parent Virtual Wire to separate CustomerA and CustomerB traffic. Make sure that the VLAN tags defined on each pair of subinterfaces that are configured as virtual wire(s) are identical. This is essential because a virtual wire does not switch VLAN tags.
3. Create new subinterfaces and define IP classifiers. This task is optional and only required if you wish to add additional subinterfaces with IP classifiers for further managing traffic from a customer based on the combination of VLAN tags and a specific source IP address, range or subnet.

You can also use IP classifiers for managing untagged traffic. To do so, you must create a sub-interface with the vlan tag “0”, and define sub-interface(s) with IP classifiers for managing untagged traffic using IP classifiers



IP classification may only be used on the subinterfaces associated with one side of the virtual wire. The subinterfaces defined on the corresponding side of the virtual wire must use the same VLAN tag, but must not include an IP classifier.

**Figure: Virtual Wire Deployment with Subinterfaces (VLAN Tags only)**



[Figure: Virtual Wire Deployment with Subinterfaces \(VLAN Tags only\)](#) depicts CustomerA and CustomerB connected to the firewall through one physical interface, ethernet1/1, configured as a Virtual Wire; it is the ingress interface. A second physical interface, ethernet1/2, is also part of the Virtual Wire; it is the egress interface that provides access to the Internet. For CustomerA, you also have subinterfaces ethernet1/1.1 (ingress) and ethernet1/1.2 (egress). For CustomerB, you have the subinterface ethernet1/1.2 (ingress) and ethernet1/2.2 (egress). When configuring the subinterfaces, you must assign the appropriate VLAN tag and zone in order to apply policies for each customer. In this example, the policies for CustomerA are created between Zone1 and Zone2, and policies for CustomerB are created between Zone3 and Zone4.

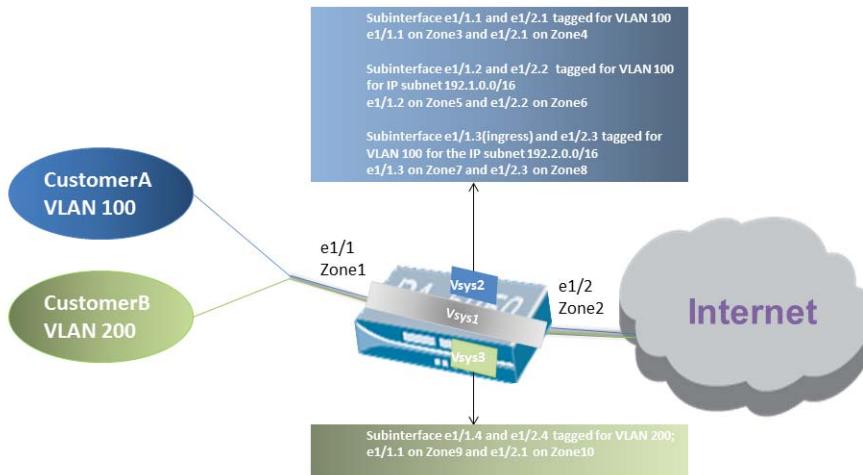
When traffic enters the firewall from CustomerA or CustomerB, the VLAN tag on the incoming packet is first matched against the VLAN tag defined on the ingress subinterfaces. In this example, a single subinterface matches the VLAN tag on the incoming packet, hence that subinterface is selected. The policies defined for the zone are evaluated and applied before the packet exits from the corresponding subinterface.



The same VLAN tag must not be defined on the parent virtual wire interface and the subinterface. Verify that the VLAN tags defined on the Tag Allowed list of the parent virtual wire interface (**Network > Virtual Wires**) are not included on a subinterface.

**Figure: Virtual Wire Deployment with Subinterfaces (VLAN Tags and IP Classifiers)** depicts CustomerA and CustomerB connected to one physical firewall that has two virtual systems (vsys), in addition to the default virtual system (vsys1). Each virtual system is an independent virtual firewall that is managed separately for each customer. Each vsys has attached interfaces/subinterfaces and security zones that are managed independently.

**Figure: Virtual Wire Deployment with Subinterfaces (VLAN Tags and IP Classifiers)**



Vsys1 is set up to use the physical interfaces ethernet1/1 and ethernet1/2 as a virtual wire; ethernet1/1 is the ingress interface and ethernet1/2 is the egress interface that provides access to the Internet. This virtual wire is configured to accept all tagged and untagged traffic with the exception of VLAN tags 100 and 200 that are assigned to the subinterfaces.

CustomerA is managed on vsys2 and CustomerB is managed on vsys3. On vsys2 and vsys3, the following vwire subinterfaces are created with the appropriate VLAN tags and zones to enforce policy measures.

Customer	Vsys	Vwire Subinterfaces	Zone	VLAN Tag	IP Classifier
A	2	e1/1.1 (ingress) e1/2.1 (egress)	Zone3 Zone4	100 100	None
	2	e1/1.2 (ingress) e1/2.2 (egress)	Zone5 Zone6	100 100	IP subnet 192.1.0.0/16
	2	e1/1.3 (ingress) e1/2.3 (egress)	Zone7 Zone8	100 100	IP subnet 192.2.0.0/16
B	3	e1/1.4 (ingress) e1/2.4 (egress)	Zone9 Zone10	200 200	None

When traffic enters the firewall from CustomerA or CustomerB, the VLAN tag on the incoming packet is first matched against the VLAN tag defined on the ingress subinterfaces. In this case, for CustomerA, there are multiple subinterfaces that use the same VLAN tag. Hence, the firewall first narrows the classification to a subinterface based on the source IP address in the packet. The policies defined for the zone are evaluated and applied before the packet exits from the corresponding subinterface.

For return-path traffic, the firewall compares the destination IP address as defined in the IP classifier on the customer-facing subinterface and selects the appropriate virtual wire to route traffic through the accurate subinterface.

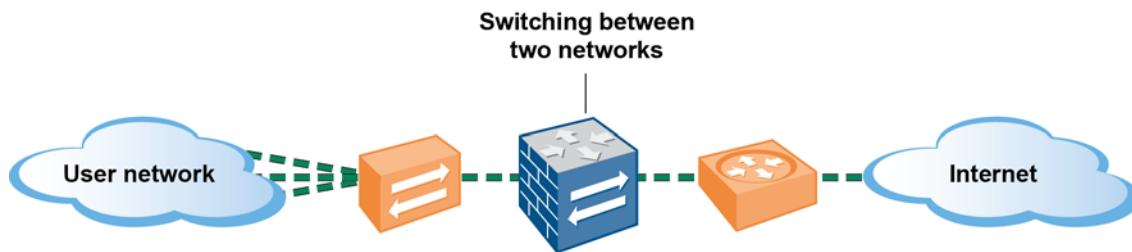


The same VLAN tag must not be defined on the parent virtual wire interface and the subinterface. Verify that the VLAN tags defined on the Tag Allowed list of the parent virtual wire interface ([Network > Virtual Wires](#)) are not included on a subinterface.

## Layer 2 Deployments

In a Layer 2 deployment, the firewall provides switching between two or more networks. Each group of interfaces must be assigned to a VLAN object in order for the firewall to switch between them. The firewall will perform VLAN tag switching when layer 2 subinterfaces are attached to a common VLAN object. Choose this option when switching is required.

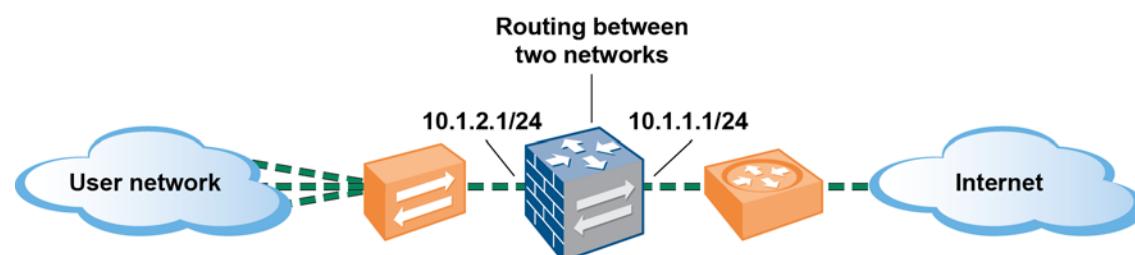
**Figure: Layer 2 Deployment**



## Layer 3 Deployments

In a Layer 3 deployment, the firewall routes traffic between multiple ports. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing is required.

**Figure: Layer 3 Deployment**



In addition, because the firewall must route traffic in a Layer 3 deployment, you must configure a virtual router. See [Virtual Routers](#).

## Point-to-Point Protocol over Ethernet Support

You can configure the firewall to be a Point-to-Point Protocol over Ethernet (PPPoE) termination point to support connectivity in a Digital Subscriber Line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.

You can choose the PPPoE option and configure the associated settings when an interface is defined as a Layer 3 interface.



PPPoE is not supported in HA active/active mode.

## DHCP Client

You can configure the firewall interface to act as a DHCP client and receive a dynamically assigned IP address. The firewall also provides the capability to propagate settings received by the DHCP client interface into a DHCP server operating on the firewall. This is most commonly used to propagate DNS server settings from an Internet service provider to client machines operating on the network protected by the firewall.



DHCP client is not supported in HA active/active mode.

For more information, see [DHCP](#).

## Tap Mode Deployments

A network tap is a device that provides a way to access data flowing across a computer network. Tap mode deployment allows you to passively monitor traffic flows across a network by way of a switch SPAN or mirror port.

The SPAN or mirror port permits the copying of traffic from other ports on the switch. By dedicating an interface on the firewall as a tap mode interface and connecting it with a switch SPAN port, the switch SPAN port provides the firewall with the mirrored traffic. This provides application visibility within the network without being in the flow of network traffic.



When deployed in tap mode, the firewall is not able to take action, such as block traffic or apply QoS traffic control.

## Virtual Routers

The firewall uses virtual routers to obtain routes to other subnets by manually defining a route (static routes) or through participation in Layer 3 routing protocols (dynamic routes). The best routes obtained through these methods are used to populate the firewall's IP route table. When a packet is destined for a different subnet, the Virtual Router obtains the best route from this IP route table and forwards the packet to the next hop router defined in the table.

The Ethernet interfaces and VLAN interfaces defined on the firewall receive and forward the Layer 3 traffic. The destination zone is derived from the outgoing interface based on the forwarding criteria, and policy rules are consulted to identify the security policies to be applied. In addition to routing to other network devices, virtual routers can route to other virtual routers within the same firewall if a next hop is specified to point to another virtual router.

You can configure the virtual router to participate with dynamic routing protocols (BGP, OSPF, or RIP) as well as adding static routes. You can also create multiple virtual routers, each maintaining a separate set of routes that are not shared between virtual routers, enabling you to configure different routing behaviors for different interfaces.

Each Layer 3 interface, loopback interface, and VLAN interface defined on the firewall must be associated with a virtual router. While each interface can belong to only one virtual router, multiple routing protocols and static routes can be configured for a virtual router. Regardless of the static routes and dynamic routing protocols configured for a virtual router, a common general configuration is required. The firewall uses Ethernet switching to reach other devices on the same IP subnet.

The following Layer 3 routing protocols are supported from Virtual Routers:

- RIP
- OSPF
- OSPFv3
- BGP

### Define a Virtual Router General Configuration

<b>Step 1</b> Gather the required information from your network administrator.	<ul style="list-style-type: none"><li>● Interfaces that you want to route</li><li>● Administrative distances for static, OSPF internal, OSPF external, IBGP, EBGP and RIP</li></ul>
<b>Step 2</b> Create the virtual router and name it.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Virtual Routers</b>.</li><li>2. Click <b>Add</b> and enter a name for the virtual router.</li><li>3. Select interfaces to apply to the virtual router.</li><li>4. Click <b>OK</b>.</li></ol>
<b>Step 3</b> Select interfaces to apply to the virtual router.	<ol style="list-style-type: none"><li>1. Click <b>Add</b> in the Interfaces box.</li><li>2. Select an already defined interface from the drop-down.</li><li>3. Repeat Step 2 for all interfaces that you want to add to the virtual router.</li></ol>

**Define a Virtual Router General Configuration (Continued)**

<b>Step 4</b>	Set Administrative Distances for static and dynamic routing.	Set Administrative Distances as required. <ul style="list-style-type: none"><li>• <b>Static</b>—Range is 10-240; default is 10.</li><li>• <b>OSPF Internal</b>—Range is 10-240; default is 30.</li><li>• <b>OSPF External</b>—Range is 10-240; default is 110.</li><li>• <b>IBGP</b>—Range is 10-240; default is 200.</li><li>• <b>EBGP</b>—Range is 10-240; default is 20.</li><li>• <b>RIP</b>—Range is 10-240; default is 120.</li></ul>
<b>Step 5</b>	Save virtual router general settings.	Click <b>OK</b> to save your settings.
<b>Step 6</b>	Commit your changes.	Click <b>Commit</b> . The device may take up to 90 seconds to save your changes.

# Static Routes

The following procedure shows how to integrate the firewall into the network using static routing.

Set Up Interfaces and Zones	
<p><b>Step 1</b> Configure a default route to your Internet router.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Virtual Router</b> and then select the <b>default</b> link to open the Virtual Router dialog.</li><li>2. Select the <b>Static Routes</b> tab and click <b>Add</b>. Enter a <b>Name</b> for the route and enter the route in the <b>Destination</b> field (for example, 0.0.0.0/0).</li><li>3. Select the <b>IP Address</b> radio button in the <b>Next Hop</b> field and then enter the IP address and netmask for your Internet gateway (for example, 208.80.56.1).</li><li>4. Click <b>OK</b> twice to save the virtual router configuration.</li></ol>
<p><b>Step 2</b> Configure the external interface (the interface that connects to the Internet).</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces</b> and then select the interface you want to configure. In this example, we are configuring Ethernet1/3 as the external interface.</li><li>2. Select the <b>Interface Type</b>. Although your choice here depends on your network topology, this example shows the steps for <b>Layer3</b>.</li><li>3. In the <b>Virtual Router</b> drop-down, select <b>default</b>.</li><li>4. On the <b>Config</b> tab, select <b>New Zone</b> from the <b>Security Zone</b> drop-down. In the Zone dialog, define a <b>Name</b> for new zone, for example Untrust, and then click <b>OK</b>.</li><li>5. To assign an IP address to the interface, select the <b>IPv4</b> tab and <b>Static</b> radio button. Click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 208.80.56.100/24.</li><li>6. To enable you to ping the interface, select <b>Advanced &gt; Other Info</b>, expand the <b>Management Profile</b> drop-down, and select <b>New Management Profile</b>. Enter a <b>Name</b> for the profile, select <b>Ping</b> and then click <b>OK</b>.</li><li>7. To save the interface configuration, click <b>OK</b>.</li></ol>

## Set Up Interfaces and Zones (Continued)

<p><b>Step 3</b> Configure the interface that connects to your internal network.</p>	<p>In this example, the interface connects to a network segment that uses private IP addresses. Because private IP addresses cannot be routed externally, you will have to configure NAT. See <a href="#">Configure NAT</a> for details.</p> <ol style="list-style-type: none"> <li>Select <b>Network &gt; Interfaces</b> and select the interface you want to configure. In this example, we are configuring Ethernet1/4 as the internal interface.</li> <li>Select <b>Layer3</b> from the <b>Interface Type</b> drop-down.</li> <li>On the <b>Config</b> tab, expand the <b>Security Zone</b> drop-down and select <b>New Zone</b>. In the Zone dialog, define a <b>Name</b> for new zone, for example Trust, and then click <b>OK</b>.</li> <li>Select the same Virtual Router you used in <a href="#">Step 2</a>, default in this example.</li> <li>To assign an IP address to the interface, select the <b>IPv4</b> tab and the <b>Static</b> radio button, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.1.4/24.</li> <li>To enable you to ping the interface, select the management profile that you created in <a href="#">Step 2-6</a>.</li> <li>To save the interface configuration, click <b>OK</b>.</li> </ol>
<p><b>Step 4</b> Configure the interface that connects to the DMZ.</p>	<ol style="list-style-type: none"> <li>Select the interface you want to configure.</li> <li>Select <b>Layer3</b> from the <b>Interface Type</b> drop-down. In this example, we are configuring Ethernet1/13 as the DMZ interface.</li> <li>On the <b>Config</b> tab, expand the <b>Security Zone</b> drop-down and select <b>New Zone</b>. In the Zone dialog, define a <b>Name</b> for new zone, for example DMZ, and then click <b>OK</b>.</li> <li>Select the Virtual Router you used in <a href="#">Step 2</a>, default in this example.</li> <li>To assign an IP address to the interface, select the <b>IPv4</b> tab and the <b>Static</b> radio button, click <b>Add</b> in the IP section, and enter the IP address and network mask to assign to the interface, for example 10.1.1.1/24.</li> <li>To enable you to ping the interface, select the management profile that you created in <a href="#">Step 2-6</a>.</li> <li>To save the interface configuration, click <b>OK</b>.</li> </ol>
<p><b>Step 5</b> Save the interface configuration.</p>	Click <b>Commit</b> .
<p><b>Step 6</b> Cable the firewall.</p>	Attach straight through cables from the interfaces you configured to the corresponding switch or router on each network segment.
<p><b>Step 7</b> Verify that the interfaces are active.</p>	From the web interface, select <b>Network &gt; Interfaces</b> and verify that icon in the Link State column is green. You can also monitor link state from the <b>Interfaces</b> widget on the <b>Dashboard</b> . 

# RIP

Routing Information Protocol (RIP) is an interior gateway protocol (IGP) that was designed for small IP networks. RIP relies on hop count to determine routes; the best routes have the fewest number of hops. RIP is based on UDP and uses port 520 for route updates. By limiting routes to a maximum of 15 hops, the protocol helps prevent the development of routing loops, but also limits the supported network size. If more than 15 hops are required, traffic is not routed. RIP also can take longer to converge than OSPF and other routing protocols. The firewall supports RIP v2.

Perform the following procedure to configure RIP.

Configure RIP	
Step 1	Configure general virtual router configuration settings. See <a href="#">Virtual Routers</a> for details.
Step 2	Configure general RIP configuration settings. <ol style="list-style-type: none"><li>Select the <b>RIP</b> tab.</li><li>Select the <b>Enable</b> check box to enable the RIP protocol.</li><li>Select the <b>Reject Default Route</b> check box if you do not want to learn any default routes through RIP. This is the recommended default setting.</li><li>De-select the <b>Reject Default Route</b> check box if you want to permit redistribution of default routes through RIP.</li></ol>
Step 3	Configure interfaces for the RIP protocol. <ol style="list-style-type: none"><li>On <b>Interfaces</b> tab, select an interface from the drop-down in the Interface configuration section.</li><li>Select an already defined interface from the drop-down.</li><li>Select the <b>Enable</b> check box.</li><li>Select the <b>Advertise</b> check box to advertise a default route to RIP peers with the specified metric value.</li><li>You can optionally select a profile from the <b>Auth Profile</b> drop-down. See <a href="#">Step 5</a> for details.</li><li>Select normal, passive or send-only from the <b>Mode</b> drop-down.</li><li>Click <b>OK</b>.</li></ol>
Step 4	Configure RIP timers. <ol style="list-style-type: none"><li>On the <b>Timers</b> tab, enter a value in the <b>Interval Seconds (sec)</b> box. This setting defines the length of the timer interval in seconds (range is 1-60; default is 1). This duration is used for the remaining RIP timing fields.</li><li>Enter an <b>Update Intervals</b> value to define the number of intervals between route update announcements (range is 1-3600; default is 30).</li><li>Specify the <b>Delete Intervals</b> to define the number of intervals between the time that the route expires to its deletion (range is 1-3600; default is 180).</li><li>Specify the <b>Expire Intervals</b> to define the number of intervals between the time that the route was last updated to its expiration (range is 1-3600; default is 120).</li></ol>

## Configure RIP

<p><b>Step 5</b> (Optional) Configure Auth Profiles.</p>	<p>By default, the firewall does not use RIP authentication for the exchange between RIP neighbors. Optionally, you can configure RIP authentication between RIP neighbors by either a simple password or using MD5 authentication.</p> <p><b>Simple Password RIP authentication</b></p> <ol style="list-style-type: none"><li>1. Select <b>Auth Profiles</b> and click <b>Add</b>.</li><li>2. Enter a name for the authentication profile to authenticate RIP messages.</li><li>3. Select <b>Simple Password</b> as the <b>Password Type</b>.</li><li>4. Enter a simple password and then confirm.</li></ol> <p><b>MD5 RIP authentication</b></p> <ol style="list-style-type: none"><li>1. Select <b>Auth Profiles</b> and click <b>Add</b>.</li><li>2. Enter a name for the authentication profile to authenticate RIP messages.</li><li>3. Select <b>MD5</b> as the <b>Password Type</b>.</li><li>4. Click <b>Add</b>.</li><li>5. Enter one or more password entries, including:<ul style="list-style-type: none"><li>• Key-ID (range is 0-255)</li><li>• Key</li></ul></li><li>6. You can optionally select <b>Preferred</b> status.</li><li>7. Click <b>OK</b> to specify the key to be used to authenticate outgoing message.</li><li>8. Click <b>OK</b> again in the Virtual Router - RIP Auth Profile dialog box.</li></ol>
--	---

# OSPF

Open Shortest Path First (OSPF) is an interior gateway protocol (IGP) that is most often used to dynamically manage network routes in large enterprise network. It determines routes dynamically by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSAs). The information gathered from the LSAs is used to construct a topology map of the network. This topology map is shared across routers in the network and used to populate the IP routing table with available routes.

Changes in the network topology are detected dynamically and used to generate a new topology map within seconds. A shortest path tree is computed of each route. Metrics associated with each routing interface are used to calculate the best route. These can include distance, network throughput, link availability etc. Additionally, these metrics can be configured statically to direct the outcome of the OSPF topology map.

Palo Alto networks implementation of OSPF fully supports the following RFCs:

- [RFC 2328](#) (for IPv4)
- [RFC 5340](#) (for IPv6)

The following topics provide more information about the OSPF and procedures for configuring OSPF on the firewall:

- ▲ [OSPF Concepts](#)
- ▲ [Configure OSPF](#)
- ▲ [Configure OSPFv3](#)
- ▲ [Configure OSPF Graceful Restart](#)
- ▲ [Confirm OSPF Operation](#)

Also refer to [How to Configure OSPF Tech Note](#).

## OSPF Concepts

The following topics introduce the OSPF concepts you will need to understand in order to configure the firewall to participate in an OSPF network:

- ▲ [OSPFv3](#)
- ▲ [OSPF Neighbors](#)
- ▲ [OSPF Areas](#)
- ▲ [OSPF Router Types](#)

## OSPFv3

OSPFv3 provides support for the OSPF routing protocol within an IPv6 network. As such, it provides support for IPv6 addresses and prefixes. It retains most of the structure and functions in OSPFv2 (for IPv4) with some minor changes. The following are some of the additions and changes to OSPFv3:

- **Support for multiple instances per link**—With OSPFv3, you can run multiple instances of the OSPF protocol over a single link. This is accomplished by assigning an OSPFv3 instance ID number. An interface that is assigned to an instance ID drops packets that contain a different ID.
- **Protocol Processing Per-link**—OSPFv3 operates per-link instead of per-IP-subnet as on OSPFv2.
- **Changes to Addressing**—IPv6 addresses are not present in OSPFv3 packets, except for LSA payloads within link state update packets. Neighboring routers are identified by the Router ID.
- **Authentication Changes**—OSPFv3 doesn't include any authentication capabilities. Configuring OSPFv3 on a firewall requires an authentication profile that specifies Encapsulating Security Payload (ESP) or IPv6 Authentication Header (AH). The re-keying procedure specified in RFC 4552 is not supported in this release.
- **Support for multiple instances per-link**—Each instance corresponds to an instance ID contained in the OSPFv3 packet header.
- **New LSA Types**—OSPFv3 supports two new LSA types: Link LSA and Intra Area Prefix LSA.

All additional changes are described in detail in RFC 5340.

## OSPF Neighbors

Two OSPF-enabled routers connected by a common network and in the same OSPF area that form a relationship are OSPF neighbors. The connection between these routers can be through a common broadcast domain or by a point-to-point connection. This connection is made through the exchange of hello OSPF protocol packets. These neighbor relationships are used to exchange routing updates between routers.

## OSPF Areas

OSPF operates within a single autonomous system (AS). Networks within this single AS, however, can be divided into a number of areas. By default, Area 0 is created. Area 0 can either function alone or act as the OSPF backbone for a larger number of areas. Each OSPF area is named using a 32-bit identifier which in most cases is written in the same dotted-decimal notation as an IP4 address. For example, Area 0 is usually written as 0.0.0.0.

The topology of an area is maintained in its own link state database and is hidden from other areas, which reduces the amount of traffic routing required by OSPF. The topology is then shared in a summarized form between areas by a connecting router.

**Table: OSPF Area Types**

Area Type	Description
Backbone Area	The backbone area (Area 0) is the core of an OSPF network. All other areas are connected to it and all traffic between areas must traverse it. All routing between areas is distributed through the backbone area. While all other OSPF areas must connect to the backbone area, this connection doesn't need to be direct and can be made through a virtual link.
Normal OSPF Area	In a normal OSPF area there are no restrictions; the area can carry all types of routes.
Stub OSPF Area	A stub area does not receive routes from other autonomous systems. Routing from the stub area is performed through the default route to the backbone area.
NSSA Area	The Not So Stubby Area (NSSA) is a type of stub area that can import external routes, with some limited exceptions.

## OSPF Router Types

Within an OSPF area, routers are divided into the following categories.

- **Internal Router**—A router with that has OSPF neighbor relationships only with devices in the same area.
- **Area Border Router (ABR)**—A router that has OSPF neighbor relationships with devices in multiple areas. ABRs gather topology information from their attached areas and distribute it to the backbone area.
- **Backbone Router**—A backbone router is any OSPF router that is attached to the OSPF backbone. Since ABRs are always connected to the backbone, they are always classified as backbone routers.
- **Autonomous System Boundary Router (ASBR)**—An ASBR is a router that attaches to more than one routing protocol and exchanges routing information between them.

## Configure OSPF

OSPF determines routes dynamically by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSAs). The router keeps information about the links between it and the destination and can make highly efficient routing decisions. A cost is assigned to each router interface, and the best routes are determined to be those with the lowest costs, when summed over all the encountered outbound router interfaces and the interface receiving the LSA.

Hierarchical techniques are used to limit the number of routes that must be advertised and the associated LSAs. Because OSPF dynamically processes a considerable amount of route information, it has greater processor and memory requirements than does RIP.

Configure OSPF	
Step 1	Configure general virtual router configuration settings. See <a href="#">Virtual Routers</a> for details.
Step 2	Configure general OSPF configuration settings. <ol style="list-style-type: none"><li>Select the <b>OSPF</b> tab.</li><li>Select the <b>Enable</b> check box to enable the OSPF protocol.</li><li>Optionally enter the <b>Router ID</b>.</li><li>Select the <b>Reject Default Route</b> check box if you do not want to learn any default routes through OSPF. This is the recommended default setting. De-select the <b>Reject Default Route</b> check box if you want to permit redistribution of default routes through OSPF.</li></ol>

**Configure OSPF (Continued)**

**Step 3** Configure Areas - Type for the OSPF protocol.

1. On the **Areas** tab, click **Add**.
2. Enter an Area ID for the area in `x.x.x.x` format. This is the identifier that each neighbor must accept to be part of the same area.
3. On the **Type** tab, select one of the following from the area **Type** drop-down:
  - **Normal**—There are no restrictions; the area can carry all types of routes.
  - **Stub**—There is no outlet from the area. To reach a destination outside of the area, it is necessary to go through the border, which connects to other areas. If you select this option, configure the following:
    - **Accept Summary**—Link state advertisements (LSA) are accepted from other areas. If this option on a stub area Area Border Router (ABR) interface is disabled, the OSPF area will behave as a Totally Stubby Area (TSA) and the ABR will not propagate any summary LSAs.
    - **Advertise Default Route**—Default route LSAs will be included in advertisements to the stub area along with a configured metric value in the configured range 1-255.
  - **NSSA** (Not-So-Stubby Area)—The firewall can only leave the area by routes other than OSPF routes. If selected, configure **Accept Summary** and **Advertise Default Route** as described for **Stub**. If you select this option, configure the following:
    - **Type**—Select either **Ext 1** or **Ext 2** route type to advertise the default LSA.
    - **Ext Ranges**—Click **Add** in the section to enter ranges of external routes that you want to enable or suppress advertising for.
4. **Priority**—Enter the OSPF priority for this interface (0-255). This is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) according to the OSPF protocol. When the value is zero, the router will not be elected as a DR or BDR.
  - **Auth Profile**—Select a previously-defined authentication profile.
  - **Timing**—It is recommended that you keep the default timing settings.
  - **Neighbors**—For p2pmp interfaces, enter the neighbor IP address for all neighbors that are reachable through this interface.
5. Select **normal**, **passive** or **send-only** as the **Mode**.
6. Click **OK**.

<b>Configure OSPF (Continued)</b>	
<b>Step 4</b> Configure Areas - Range for the OSPF protocol	<ol style="list-style-type: none"> <li>On the <b>Range</b> tab, click <b>Add</b> to aggregate LSA destination addresses in the area into subnets.</li> <li><b>Advertise</b> or <b>SUPPRESS</b> advertising LSAs that match the subnet, and click <b>OK</b>. Repeat to add additional ranges.</li> </ol>
<b>Step 5</b> Configure Areas - Interfaces for the OSPF protocol	<ol style="list-style-type: none"> <li>On the <b>Interface</b> tab, click <b>Add</b> and enter the following information for each interface to be included in the area:             <ul style="list-style-type: none"> <li><b>Interface</b>—Select an interface from the drop-down box.</li> <li><b>Enable</b>—Selecting this option causes the OSPF interface settings to take effect.</li> <li><b>Passive</b>—Select the check box to if you do not want the OSPF interface to send or receive OSPF packets. Although OSPF packets are not sent or received if you choose this option, the interface is included in the LSA database.</li> <li><b>Link type</b>—Choose <b>Broadcast</b> if you want all neighbors that are accessible through the interface to be discovered automatically by multicasting OSPF hello messages, such as an Ethernet interface. Choose <b>p2p</b> (point-to-point) to automatically discover the neighbor. Choose <b>p2mp</b> (point-to-multipoint) when neighbors must be defined manually. Defining neighbors manually is allowed only for <b>p2mp</b> mode.</li> <li><b>Metric</b>—Enter an OSPF metric for this interface (range is 0-65535; default is 10).</li> <li><b>Priority</b>—Enter an OSPF priority for this interface. This is the priority for the router to be elected as a designated router (DR) or as a backup DR (BDR) (range is 0-255; default is 1). If zero is configured, the router will not be elected as a DR or BDR.</li> <li><b>Auth Profile</b>—Select a previously-defined authentication profile.</li> <li><b>Timing</b>—The following OSPF timing settings can be set. Palo Alto Networks recommends that you retain the default timing settings.               <ul style="list-style-type: none"> <li>— <b>Hello Interval (sec)</b>—Interval (in seconds) at which the OSPF process sends hello packets to its directly connected neighbors (range is 0-3600; default is 10).</li> <li>— <b>Dead Counts</b>—Number of times the hello interval can occur for a neighbor without OSPF receiving a hello packet from the neighbor, before OSPF considers that neighbor down (range is 3-20; default is 4). The <b>Hello Interval</b> multiplied by the <b>Dead Counts</b> equals the value of the dead timer.</li> </ul> </li> </ul> </li> </ol>

**Configure OSPF (Continued)**

	<ul style="list-style-type: none"><li>– <b>Retransmit Interval (sec)</b>—Length of time (in seconds) that OSPF waits to receive a link state advertisement (LSA) from a neighbor before OSPF retransmits the LSA (range is 0-3600; default is 10).</li><li>– <b>Transit Delay (sec)</b>—Length of time (in seconds) that an LSA is delayed before it is sent out of an interface (range is 0-3600; default is 1).</li><li>– <b>Graceful Restart Hello Delay (sec)</b>—Applies to an OSPF interface when Active/Passive High Availability is configured. <b>Graceful Restart Hello Delay</b> is the length of time (in seconds) during which the firewall sends Grace LSA packets at 1-second intervals (range is 1-10; default is 10). During this time, no hello packets are sent from the restarting firewall. During the restart, the dead timer (which is the <b>Hello Interval</b> multiplied by the <b>Dead Counts</b>) is also counting down. If the dead timer is too short, the adjacency will go down during the graceful restart because of the hello delay. Therefore, it is recommended that the dead timer be at least four times the value of the <b>Graceful Restart Hello Delay</b>. For example, a <b>Hello Interval</b> of 10 seconds and a <b>Dead Counts</b> of 4 yield a dead timer of 40 seconds. If the <b>Graceful Restart Hello Delay</b> is set to 10 seconds, that 10-second delay of hello packets is comfortably within the 40-second dead timer, so the adjacency will not time out during a graceful restart.</li></ul> <ol style="list-style-type: none"><li>• If <b>p2mp</b> is selected for <b>Link Type</b> interfaces, enter the neighbor IP addresses for all neighbors that are reachable through this interface.</li></ol>
<b>Step 6</b> Configure Areas - Virtual Links.	<ol style="list-style-type: none"><li>2. Click <b>OK</b>.</li><li>1. On the <b>Virtual Link</b> tab, click <b>Add</b> and enter the following information for each virtual link to be included in the backbone area:<ul style="list-style-type: none"><li>• <b>Name</b>—Enter a name for the virtual link.</li><li>• <b>Neighbor ID</b>—Enter the router ID of the router (neighbor) on the other side of the virtual link.</li><li>• <b>Transit Area</b>—Enter the area ID of the transit area that physically contains the virtual link.</li><li>• <b>Enable</b>—Select to enable the virtual link.</li><li>• <b>Timing</b>—It is recommended that you keep the default timing settings.</li><li>• <b>Auth Profile</b>—Select a previously-defined authentication profile.</li></ul></li><li>2. Click <b>OK</b>.</li></ol>

Configure OSPF (Continued)	
<p><b>Step 7</b> (Optional) Configure Auth Profiles.</p>	<p>By default, the firewall does not use OSPF authentication for the exchange between OSPF neighbors. Optionally, you can configure OSPF authentication between OSPF neighbors by either a simple password or using MD5 authentication.</p> <p><b>Simple Password OSPF authentication</b></p> <ol style="list-style-type: none"><li>1. On the <b>Auth Profiles</b> tab, click <b>Add</b>.</li><li>2. Enter a name for the authentication profile to authenticate OSPF messages.</li><li>3. Select <b>Simple Password</b> as the <b>Password Type</b>.</li><li>4. Enter a simple password and then confirm.</li></ol> <p><b>MD5 OSPF authentication</b></p> <ol style="list-style-type: none"><li>1. On the <b>Auth Profiles</b> tab, click <b>Add</b>.</li><li>2. Enter a name for the authentication profile to authenticate OSPF messages.</li><li>3. Select <b>MD5</b> as the <b>Password Type</b>.</li><li>4. Click <b>Add</b>.</li><li>5. Enter one or more password entries, including:<ul style="list-style-type: none"><li>• Key-ID (range is 0-255)</li><li>• Key</li><li>• Select the <b>Preferred</b> option to specify that the key be used to authenticate outgoing messages.</li></ul></li><li>6. Click <b>OK</b>.</li><li>7. Click <b>OK</b> again in the Virtual Router - OSPF Auth Profile dialog box.</li></ol>
<p><b>Step 8</b> Configure Advanced OSPF options.</p>	<ol style="list-style-type: none"><li>1. On the <b>Advanced</b> tab, select the <b>RFC 1583 Compatibility</b> check box to ensure compatibility with RFC 1583.</li><li>2. Configure a value for the <b>SPF Calculation Delay (sec)</b> timer. This timer allows you to tune the delay time between receiving new topology information and performing an SPF calculation. Lower values enable faster OSPF re-convergence. Routers peering with the firewall should be tuned in a similar manner to optimize convergence times.</li><li>3. Configure a value for the <b>LSA Interval (sec)</b> time. This timer specifies the minimum time between transmissions of two instances of the same LSA (same router, same type, same LSA ID). This is equivalent to MinLSInterval in RFC 2328. Lower values can be used to reduce re-convergence times when topology changes occur.</li></ol>

## Configure OSPFv3

<b>Configure OSPFv3</b>	
<b>Step 1</b> Configure general virtual router configuration settings.	See <a href="#">Virtual Routers</a> for details.
<b>Step 2</b> Configure general OSPF configuration settings.	<ol style="list-style-type: none"> <li>Select the <b>OSPF</b> tab.</li> <li>Select the <b>Enable</b> check box to enable the OSPF protocol.</li> <li>Select the <b>Reject Default Route</b> check box if you do not want to learn any default routes through OSPF. This is the recommended default setting.</li> <li>Clear the <b>Reject Default Route</b> check box if you want to permit redistribution of default routes through OSPF.</li> </ol>
<b>Step 3</b> Configure general OSPFv3 configuration settings.	<ol style="list-style-type: none"> <li>Select the <b>OSPFv3</b> tab.</li> <li>Select the <b>Enable</b> check box to enable the OSPF protocol.</li> <li>Select the <b>Reject Default Route</b> check box if you do not want to learn any default routes through OSPFv3. This is the recommended default setting.</li> </ol> <p>De-select the <b>Reject Default Route</b> check box if you want to permit redistribution of default routes through OSPFv3.</p>
<b>Step 4</b> Configure Auth Profile for the OSPFv3 protocol.  While OSPFv3 doesn't include any authentication capabilities of its own, it relies entirely on IPsec to secure communications between neighbors.	<p>When configuring an authentication profile, you must use Encapsulating Security Payload (ESP) or IPv6 Authentication Header (AH).</p> <p><b>ESP OSPFv3 authentication</b></p> <ol style="list-style-type: none"> <li>On the <b>Auth Profiles</b> tab, click <b>Add</b>.</li> <li>Enter a name for the authentication profile to authenticate OSPFv3 messages.</li> <li>Specify a Security Policy Index (<b>SPI</b>). The SPI must match between both ends of the OSPFv3 adjacency. The SPI number must be a hexadecimal value between 00000000 and FFFFFFFF.</li> <li>Select <b>ESP</b> for <b>Protocol</b>.</li> <li>Select a <b>Crypto Algorithm</b> from the drop-down. You can enter none or one of the following algorithms: SHA1, SHA256, SHA384, SHA512 or MD5.</li> <li>If a <b>Crypto Algorithm</b> other than none was selected, enter a value for <b>Key</b> and then confirm.</li> </ol>

## Configure OSPFv3 (Continued)

	<p><b>AH OSPFv3 authentication</b></p> <ol style="list-style-type: none"> <li>1. On the <b>Auth Profiles</b> tab, click <b>Add</b>.</li> <li>2. Enter a name for the authentication profile to authenticate OSPFv3 messages.</li> <li>3. Specify a Security Policy Index (<b>SPI</b>). The SPI must match between both ends of the OSPFv3 adjacency. The SPI number must be a hexadecimal value between 00000000 and FFFFFFFF.</li> <li>4. Select <b>AH</b> for <b>Protocol</b>.</li> <li>5. Select a <b>Crypto Algorithm</b> from the drop-down. You must enter one of the following algorithms: SHA1, SHA256, SHA384, SHA512 or MD5.</li> <li>6. Enter a value for <b>Key</b> and then confirm.</li> <li>7. Click <b>OK</b>.</li> <li>8. Click <b>OK</b> again in the Virtual Router - OSPF Auth Profile dialog.</li> </ol>
Step 5 Configure Areas - Type for the OSPF protocol.	<ol style="list-style-type: none"> <li>1. On the <b>Areas</b> tab, click <b>Add</b>.</li> <li>2. Enter an Area ID. This is the identifier that each neighbor must accept to be part of the same area.</li> <li>3. On the <b>General</b> tab, select one of the following from the area <b>Type</b> drop-down: <ul style="list-style-type: none"> <li>• <b>Normal</b>—There are no restrictions; the area can carry all types of routes.</li> <li>• <b>Stub</b>—There is no outlet from the area. To reach a destination outside of the area, it is necessary to go through the border, which connects to other areas. If you select this option, configure the following: <ul style="list-style-type: none"> <li>– <b>Accept Summary</b>—Link state advertisements (LSA) are accepted from other areas. If this option on a stub area Area Border Router (ABR) interface is disabled, the OSPF area will behave as a Totally Stubby Area (TSA) and the ABR will not propagate any summary LSAs.</li> <li>– <b>Advertise Default Route</b>—Default route LSAs will be included in advertisements to the stub area along with a configured metric value in the configured range 1-255.</li> </ul> </li> </ul> </li> </ol>

**Configure OSPFv3 (Continued)**

	<ul style="list-style-type: none"><li>• <b>NSSA</b> (Not-So-Stubby Area)—The firewall can only leave the area by routes other than OSPF routes. If selected, configure <b>Accept Summary</b> and <b>Advertise Default Route</b> as described for <b>Stub</b>. If you select this option, configure the following:<ul style="list-style-type: none"><li>– <b>Type</b>—Select either <b>Ext 1</b> or <b>Ext 2</b> route type to advertise the default LSA.</li><li>– <b>Ext Ranges</b>—Click <b>Add</b> in the section to enter ranges of external routes that you want to enable or suppress advertising for.</li></ul></li></ul>
<b>Step 6</b> Associate an OSPFv3 authentication profile to an area or an interface.	<p><b>To an Area</b></p> <ol style="list-style-type: none"><li>1. On the <b>Areas</b> tab, select an existing area from the table.</li><li>2. On the <b>General</b> tab, select a previously defined <b>Authentication Profile</b> from the <b>Authentication</b> drop-down.</li><li>3. Click <b>OK</b>.</li></ol> <p><b>To an Interface</b></p> <ol style="list-style-type: none"><li>1. On the <b>Areas</b> tab, select an existing area from the table.</li><li>2. Select the <b>Interface</b> tab and click <b>Add</b>.</li><li>3. Select the authentication profile you want to associate with the OSPF interface from the <b>Auth Profile</b> drop-down.</li></ol>
<b>Step 7</b> (Optional) Configure Export Rules	<ol style="list-style-type: none"><li>1. On the <b>Export</b> tab, click <b>Add</b>.</li><li>2. Select the <b>Allow Redistribute Default Route</b> check box to permit redistribution of default routes through OSPFv3.</li><li>3. Select the name of a redistribution profile. The value must be an IP subnet or valid redistribution profile name.</li><li>4. Select a metric to apply for <b>New Path Type</b>.</li><li>5. Specify a <b>New Tag</b> for the matched route that has a 32-bit value.</li><li>6. Assign a metric for the new rule (range is 1 - 65535).</li><li>7. Click <b>OK</b>.</li></ol>

### Configure OSPFv3 (Continued)

Step 8 Configure Advanced OSPFv3 options.	<ol style="list-style-type: none"><li>1. On the <b>Advanced</b> tab, select the <b>Disable Transit Routing for SPF Calculation</b> check box if you want the firewall to participate in OSPF topology distribution without being used to forward transit traffic.</li><li>2. Configure a value for the <b>SPF Calculation Delay (sec)</b> timer. This timer allows you to tune the delay time between receiving new topology information and performing an SPF calculation. Lower values enable faster OSPF re-convergence. Routers peering with the firewall should be tuned in a similar manner to optimize convergence times.</li><li>3. Configure a value for the <b>LSA Interval (sec) time</b>. This timer specifies the minimum time between transmissions of two instances of the same LSA (same router, same type, same LSA ID). This is equivalent to MinLSInterval in RFC 2328. Lower values can be used to reduce re-convergence times when topology changes occur.</li><li>4. Optionally, <a href="#">Configure OSPF Graceful Restart</a>.</li></ol>
---	---

## Configure OSPF Graceful Restart

OSPF Graceful Restart directs OSPF neighbors to continue using routes through a device during a short transition when it is out of service. This behavior increases network stability by reducing the frequency of routing table reconfiguration and the related route flapping that can occur during short periodic down times.

For a Palo Alto Networks firewall, OSPF Graceful Restart involves the following operations:

- **Firewall as a restarting device**—In a situation where the firewall will be down for a short period of time or is unavailable for short intervals, it sends Grace LSAs to its OSPF neighbors. The neighbors must be configured to run in Graceful Restart Helper mode. In Helper Mode, the neighbors receive the Grace LSAs that inform it that the firewall will perform a graceful restart within a specified period of time defined as the **Grace Period**. During the grace period, the neighbor continues to forward routes through the firewall and to send LSAs that announce routes through the firewall. If the firewall resumes operation before expiration of the grace period, traffic forwarding will continue as before without network disruption. If the firewall does not resume operation after the grace period has expired, the neighbors will exit helper mode and resume normal operation, which will involve reconfiguring the routing table to bypass the firewall.
- **Firewall as a Graceful Restart Helper**—In a situation where neighboring routers may be down for a short periods of time, the firewall can be configured to operate in Graceful Restart Helper mode. If configured in this mode, the firewall will be configured with a **Max Neighbor Restart Time**. When the firewall receives the Grace LSAs from its OSPF neighbor, it will continue to route traffic to the neighbor and advertise routes through the neighbor until either the grace period or max neighbor restart time expires. If neither expires before the neighbor returns to service, traffic forwarding continues as before without network disruption. If either period expires before the neighbor returns to service, the firewall will exit helper mode and resume normal operation, which will involve reconfiguring the routing table to bypass the neighbor.

### Configure OSPF Graceful Restart

1. Select **Network > Virtual Routers** and select the virtual router you want to configure.
2. Select **OSPF > Advanced**.
3. Verify that the following check boxes are selected (they are enabled by default):
  - **Enable Graceful Restart**
  - **Enable Helper Mode**
  - **Enable Strict LSA checking**

These check boxes should remain selected unless required by your topology.
4. Configure a **Grace Period** in seconds.
5. Configure a **Max Neighbor Restart Time** in seconds.

## Confirm OSPF Operation

Once an OSPF configuration has been committed, you can use any of the following operations to confirm that OSPF is operating:

- ▲ [View the Routing Table](#)
- ▲ [Confirm OSPF Adjacencies](#)
- ▲ [Confirm that OSPF Connections are Established](#)

### [View the Routing Table](#)

By viewing the routing table, you can see whether OSPF routes have been established. The routing table is accessible from either the web interface or the CLI. If you are using the CLI, use the following commands:

- `show routing route`
- `show routing fib`

The following procedure describes how to use the web interface to view the routing table.

### View the Routing Table

1. Select **Network > Virtual Routers**.

Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
default	ethernet1/1 ethernet1/2 loopback.3			Enabled Area Count: 1 Subnet Count: 1 Neighbor Count: 0 Virtual Link Count: 0 Virtual Neighbor Count: 0			<a href="#">More Runtime Stats</a>

### View the Routing Table

- Select the **Routing** tab and examine the **Flags** column of the routing table for routes that were learned by OSPF.



The screenshot shows a routing table with the following columns: Destination, Next Hop, Metric, Flags, Age, and Interface. The table lists several routes learned via OSPF, primarily through interface ethernet1/1 and ethernet1/3. The 'Flags' column includes entries like O, AC, AH, AO, and AO.

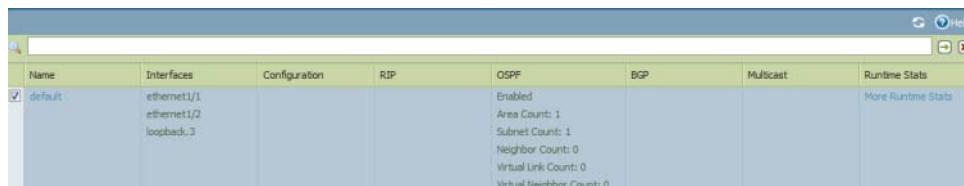
Destination	Next Hop	Metric	Flags	Age	Interface
192.0.2.0/30	0.0.0.0	10	O	7515	ethernet1/1
192.0.2.0/30	192.0.2.2	0	AC		ethernet1/1
192.0.2.2/32	0.0.0.0	0	AH		
192.0.2.4/30	192.0.2.13	20	AO	7364	ethernet1/3
192.0.2.8/30	192.0.2.1	20	AO	7399	ethernet1/1
192.0.2.12/30	0.0.0.0	10	O	7515	ethernet1/3
192.0.2.12/30	192.0.2.14	0	AC		ethernet1/3
192.0.2.14/32	0.0.0.0	0	AH		
192.0.2.16/30	0.0.0.0	10	O	7515	ethernet1/2
192.0.2.16/30	192.0.2.17	0	AC		ethernet1/2
192.0.2.17/32	0.0.0.0	0	AH		
192.0.2.20/30	0.0.0.0	10	O	7515	ethernet1/4
192.0.2.20/30	192.0.2.21	0	AC		ethernet1/4
192.0.2.21/32	0.0.0.0	0	AH		

### Confirm OSPF Adjacencies

By viewing the **Neighbor** tab as described in the following procedure, you can confirm that OSPF adjacencies have been established.

### View the Neighbor Tab to Confirm OSPF Adjacencies

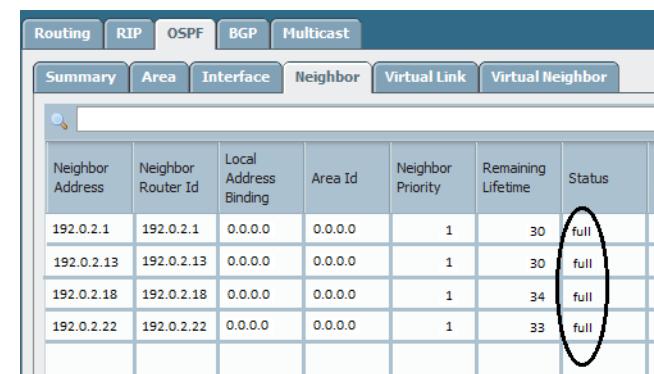
- Select **Network > Virtual Routers**.



The screenshot shows the configuration for the default virtual router. Under the OSPF tab, it indicates that OSPF is Enabled, with Area Count: 1, Subnet Count: 1, Neighbor Count: 0, Virtual Link Count: 0, and Virtual Neighbor Count: 0. A 'More Runtime Stats' link is also present.

Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
default	ethernet1/1 ethernet1/2 loopback3			Enabled Area Count: 1 Subnet Count: 1 Neighbor Count: 0 Virtual Link Count: 0 Virtual Neighbor Count: 0			<a href="#">More Runtime Stats</a>

- Select **OSPF > Neighbor** and examine the **Status** column to determine if OSPF adjacencies have been established.



The screenshot shows the OSPF Neighbor table with the following columns: Neighbor Address, Neighbor Router Id, Local Address Binding, Area Id, Neighbor Priority, Remaining Lifetime, Status, and Nbr. Four neighbors are listed, all with a Status of 'full'. The 'Status' column for the fourth neighbor is circled.

Neighbor Address	Neighbor Router Id	Local Address Binding	Area Id	Neighbor Priority	Remaining Lifetime	Status	Nbr
192.0.2.1	192.0.2.1	0.0.0.0	0.0.0.0	1	30	full	
192.0.2.13	192.0.2.13	0.0.0.0	0.0.0.0	1	30	full	
192.0.2.18	192.0.2.18	0.0.0.0	0.0.0.0	1	34	full	
192.0.2.22	192.0.2.22	0.0.0.0	0.0.0.0	1	33	full	

## Confirm that OSPF Connections are Established

By viewing the system log, you can confirm that OSPF connections have been established, as described in the following procedure:

### Examine the System Log

1. Select **Monitor > System** and look for messages to confirm that OSPF adjacencies have been established.

Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
default	ethernet1/1, ethernet1/2, loopback..3			Enabled Area Count: 1 Subnet Count: 1 Neighbor Count: 0 Virtual Link Count: 0 Virtual Neighbor Count: 0			More Runtime Stats

2. Select **OSPF > Neighbor** and examine the **Status** column to determine if OSPF adjacencies have been established.

Neighbor Address	Neighbor Router Id	Local Address Binding	Area Id	Neighbor Priority	Remaining Lifetime	Status	MP
192.0.2.1	192.0.2.1	0.0.0.0	0.0.0.0	1	30	full	
192.0.2.13	192.0.2.13	0.0.0.0	0.0.0.0	1	30	full	
192.0.2.18	192.0.2.18	0.0.0.0	0.0.0.0	1	34	full	
192.0.2.22	192.0.2.22	0.0.0.0	0.0.0.0	1	33	full	

## BGP

Border Gateway Protocol (BGP) is the primary Internet routing protocol. BGP determines network reachability based on IP prefixes that are available within autonomous systems (AS), where an AS is a set of IP prefixes that a network provider has designated to be part of a single routing policy.

In the routing process, connections are established between BGP peers (or neighbors). If a route is permitted by the policy, it is stored in the routing information base (RIB). Each time the local firewall RIB is updated, the firewall determines the optimal routes and sends an update to the external RIB, if export is enabled.

Conditional advertisement is used to control how BGP routes are advertised. The BGP routes must satisfy conditional advertisement rules before being advertised to peers.

BGP supports the specification of aggregates, which combine multiple routes into a single route. During the aggregation process, the first step is to find the corresponding aggregation rule by performing a longest match that compares the incoming route with the prefix values for other aggregation rules.

For more information on BGP, refer to [How to Configure BGP Tech Note](#).

The firewall provides a complete BGP implementation, which includes the following features:

- Specification of one BGP routing instance per virtual router.
- Routing policies based on route-map to control import, export and advertisement, prefix-based filtering, and address aggregation.
- Advanced BGP features that include route reflector, AS confederation, route flap dampening, and graceful restart.
- IGP-BGP interaction to inject routes to BGP using redistribution profiles.

BGP configuration consists of the following elements:

- Per-routing-instance settings, which include basic parameters such as local route ID and local AS and advanced options such as path selection, route reflector, AS confederation, route flap, and dampening profiles.
- Authentication profiles, which specify the MD5 authentication key for BGP connections.
- Peer group and neighbor settings, which include neighbor address and remote AS and advanced options such as neighbor attributes and connections.
- Routing policy, which specifies rule sets that peer groups and peers use to implement imports, exports, conditional advertisements, and address aggregation controls.

Perform the following procedure to configure BGP.

Configure BGP	
Step 1 Configure general virtual router configuration settings.	See <a href="#">Virtual Routers</a> for details.

Configure BGP (Continued)	
Step 2 Configure standard BGP configuration settings.	<ol style="list-style-type: none"><li>1. Select the <b>BGP</b> tab.</li><li>2. Select the <b>Enable</b> check box to enable the BGP protocol.</li><li>3. Assign an IP address to the virtual router in the <b>Router ID</b> box.</li><li>4. Enter the number of the AS to which the virtual router belongs in the <b>AS Number</b> box, based on the router ID. Range is 1-4294967295.</li></ol>
Step 3 Configure general BGP configuration settings.	<ol style="list-style-type: none"><li>1. Select <b>BGP &gt; General</b>.</li><li>2. Select the <b>Reject Default Route</b> check box to ignore any default routes that are advertised by BGP peers.</li><li>3. Select the <b>Install Route</b> check box to install BGP routes in the global routing table.</li><li>4. Select the <b>Aggregate MED</b> check box to enable route aggregation even when routes have different Multi-Exit Discriminator (MED) values.</li><li>5. Enter a value for the <b>Default Local Preference</b> that specifies a value than can be used to determine preferences among different paths.</li><li>6. Select one of the following values for the AS format for interoperability purposes:<ul style="list-style-type: none"><li>• 2 Byte (default value)</li><li>• 4 Byte</li></ul></li><li>7. Enable or disable each of the following values for <b>Path Selection</b>:<ul style="list-style-type: none"><li>• <b>Always Compare MED</b>—Enable this comparison to choose paths from neighbors in different autonomous systems.</li><li>• <b>Deterministic MED Comparison</b>—Enable this comparison to choose between routes that are advertised by IBGP peers (BGP peers in the same autonomous system).</li></ul></li><li>8. Click <b>Add</b> to include a new authentication profile and configure the following settings:<ul style="list-style-type: none"><li>• <b>Profile Name</b>—Enter a name to identify the profile.</li><li>• <b>Secret/Confirm Secret</b>—Enter and confirm a passphrase for BGP peer communications.</li></ul></li></ol>

**Configure BGP (Continued)**

<p><b>Step 4</b> Configure BGP Advanced settings (Optional)</p>	<ol style="list-style-type: none"><li>1. On the <b>Advanced</b> tab, select <b>Graceful Restart</b> and configure the following timers:<ul style="list-style-type: none"><li>• <b>Stale Route Time (sec)</b>—Specifies the length of time in seconds that a route can stay in the stale state (range is 1- 3600; default is 120).</li><li>• <b>Local Restart Time (sec)</b>—Specifies the length of time in seconds that the local device waits to restart. This value is advertised to peers (range is 1-3600; default is 120).</li><li>• <b>Max Peer Restart Time (sec)</b>—Specifies the maximum length of time in seconds that the local device accepts as a grace period restart time for peer devices (range is 1-3600; default is 120).</li></ul></li><li>2. Specify an IPv4 identifier to represent the reflector cluster in the <b>Reflector Cluster ID</b> box.</li><li>3. Specify the identifier for the AS confederation to be presented as a single AS to external BGP peers in the <b>Confederation Member AS</b> box.</li><li>4. Click <b>Add</b> and enter the following information for each Dampening Profile that you want to configure, select <b>Enable</b>, and click <b>OK</b>:<ul style="list-style-type: none"><li>• <b>Profile Name</b>—Enter a name to identify the profile.</li><li>• <b>Cutoff</b>—Specify a route withdrawal threshold above which a route advertisement is suppressed (range is 0.0-1000.0; default: is 1.25).</li><li>• <b>Reuse</b>—Specify a route withdrawal threshold below which a suppressed route is used again (range is 0.0-1000.0; default is 5).</li><li>• <b>Max Hold Time (sec)</b>—Specify the maximum length of time in seconds that a route can be suppressed, regardless of how unstable it has been (range is 0-3600 seconds; default is 900).</li><li>• <b>Decay Half Life Reachable (sec)</b>—Specify the length of time in seconds after which a route's stability metric is halved if the route is considered reachable (range is 0-3600 seconds; default: is 300).</li><li>• <b>Decay Half Life Unreachable (sec)</b>—Specify the length of time in seconds after which a route's stability metric is halved if the route is considered unreachable (range is 0-3600; default is 300).</li></ul></li><li>5. Click <b>OK</b>.</li></ol>
---	---

**Configure BGP (Continued)**

<p><b>Step 5</b> Configure the BGP peer group.</p>	<ol style="list-style-type: none"><li>1. Select the <b>Peer Group</b> tab and click <b>Add</b>.</li><li>2. Enter a <b>Name</b> for the peer group and select <b>Enable</b>.</li><li>3. Select the <b>Aggregated Confed AS Path</b> check box to include a path to the configured aggregated confederation AS.</li><li>4. Select the <b>Soft Reset with Stored Info</b> check box to perform a soft reset of the firewall after updating the peer settings.</li><li>5. Specify the type of peer or group from the <b>Type</b> drop-down and configure the associated settings (see below in this table for descriptions of Import Next Hop and Export Next Hop).<ul style="list-style-type: none"><li>• <b>IBGP—Export Next Hop:</b> Specify <b>Original</b> or <b>Use self</b></li><li>• <b>EBGP Confed—Export Next Hop:</b> Specify <b>Original</b> or <b>Use self</b></li><li>• <b>EBGP Confed—Export Next Hop:</b> Specify <b>Original</b> or <b>Use self</b></li><li>• <b>EBGP—Import Next Hop:</b> Specify <b>Original</b> or <b>Use self</b>, <b>Export Next Hop:</b> Specify <b>Resolve</b> or <b>Use self</b>. Select <b>Remove Private AS</b> if you want to force BGP to remove private AS numbers.</li></ul></li><li>6. Click <b>OK</b> to save.</li></ol>
<p><b>Step 6</b> Configure Import and Export rules.</p> <p>The import/export rules are used to import/export routes from/to other routers. For example, importing the default route from your Internet Service Provider.</p>	<ol style="list-style-type: none"><li>1. Select the <b>Import</b> tab and then click <b>Add</b> and enter a name in the <b>Rules</b> field and select the <b>Enable</b> check box.</li><li>2. Click <b>Add</b> and select the <b>Peer Group</b> to which the routes will be imported from.</li><li>3. Click the <b>Match</b> tab and define the options used to filter routing information. You can also define the Multi-Exit Discriminator (MED) value and a next hop value to routers or subnets for route filtering. The MED option is an external metric that lets neighbors know about the preferred path into an AS. A lower value is preferred over a higher value.</li><li>4. Click the <b>Action</b> tab and define the action that should occur (allow/deny) based on the filtering options defined in the <b>Match</b> tab. If <b>Deny</b> is selected, no further options need to be defined. If the <b>Allow</b> action is selected, define the other attributes.</li><li>5. Click the <b>Export</b> tab and define export attributes, which are similar to the <b>Import</b> settings, but are used to control route information that is exported from the firewall to neighbors.</li><li>6. Click <b>OK</b> to save.</li></ol>

## Configure BGP (Continued)

<p><b>Step 7</b> Configure conditional advertising, which allows you to control what route to advertise in the event that a different route is not available in the local BGP routing table (LocRIB), indicating a peering or reachability failure. This is useful in cases where you want to try to force routes to one AS over another, for example if you have links to the Internet through multiple ISPs and you want traffic to be routed to one provider instead of the other unless there is a loss of connectivity to the preferred provider.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Conditional Adv</b> tab, click <b>Add</b> and enter a name in the <b>Policy</b> field.</li> <li>2. Select the <b>Enable</b> check box.</li> <li>3. Click <b>Add</b> and in the <b>Used By</b> section enter the peer group(s) that will use the conditional advertisement policy.</li> <li>4. Select the <b>Non Exist Filter</b> tab and define the network prefix(es) of the preferred route. This specifies the route that you want to advertise, if it is available in the local BGP routing table. If a prefix is going to be advertised and matches a Non Exist filter, the advertisement will be suppressed.</li> <li>5. Select the <b>Advertise Filters</b> tab and define the prefix(es) of the route in the Local-RIB routing table that should be advertised in the event that the route in the non-exist filter is not available in the local routing table. If a prefix is going to be advertised and does not match a Non Exist filter, the advertisement will occur.</li> </ol>
<p><b>Step 8</b> Configure aggregate options to summaries routes in the BGP configuration.</p> <p>BGP route aggregation is used to control how BGP aggregates addresses. Each entry in the table results in one aggregate address being created. This will result in an aggregate entry in the routing table when at least one or more specific route matching the address specified is learned.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Aggregate</b> tab, click <b>Add</b> and enter a name for the aggregate address.</li> <li>2. In the <b>Prefix</b> field, enter the network prefix that will be the primary prefix for the aggregated prefixes.</li> <li>3. Select the <b>Suppress Filters</b> tab and define the attributes that will cause the matched routes to be suppressed.</li> <li>4. Select the <b>Advertise Filters</b> tab and define the attributes that will cause the matched routes to always be advertised to peers.</li> </ol>
<p><b>Step 9</b> Configure redistribution rules.</p> <p>This rule is used to redistribute host routes and unknown routes that are not on the local RIB to the peers routers.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Redist Rules</b> tab and click <b>Add</b>.</li> <li>2. In the <b>Name</b> field, enter an IP subnet or select a redistribution profile. You can also configure a new redistribution profile from the drop-down if needed.</li> <li>3. Click the <b>Enable</b> check box to enable the rule.</li> <li>4. In the <b>Metric</b> field, enter the route metric that will be used for the rule.</li> <li>5. In the <b>Set Origin</b> drop-down, select <b>incomplete</b>, <b>igp</b>, or <b>egp</b>.</li> <li>6. Optionally set MED, local preference, AS path limit and community values.</li> </ol>

## Session Settings and Timeouts

This section describes the global settings that affect TCP, UDP, and ICMPv6 sessions, in addition to IPv6, NAT64, NAT oversubscription, jumbo frame size, MTU, accelerated aging, and captive portal authentication. There is also a setting (Rematch Sessions) that allows you to apply newly configured security policies to sessions that are already in progress.

The **Device > Setup > Session** tab is where these session settings and timeouts are configured.

The screenshot shows the Palo Alto Networks Device setup interface. The left sidebar contains navigation links for Setup, Configuration Audit, Admin Roles, Password Profiles, Administrators, Virtual Systems, Shared Gateways, User Identification, VM Information Sources, High Availability, Certificate Management (Certificates, Certificate Profile, OCSP Responder), Response Pages, Log Settings, System, Config, HIP Match, Alarms, and Manage Logs. The main area has tabs for Management, Operations, Services, Content-ID, WildFire, Session (which is selected), and HSM. The Session tab is divided into two sections: 'Session Settings' and 'Session Timeouts'. The 'Session Settings' section includes Rematch Sessions (checked), ICMPv6 Token Bucket Size (100), ICMPv6 Error Packet Rate (per sec) (100), IPv6 Firewalling (checked), Enable Jumbo Frame (unchecked), Global MTU (1500), NAT64 IPv6 Minimum Network MTU (1280), NAT Oversubscription Rate (1x), Accelerated Aging (checked), Accelerated Aging Threshold (80), and Accelerated Aging Scaling Factor (2). The 'Session Timeouts' section lists various timeout values: Default (sec) (30), Discard Default (sec) (60), Discard TCP (sec) (90), Discard UDP (sec) (60), ICMP (sec) (6), Scan (sec) (10), TCP (sec) (3600), TCP handshake (sec) (10), TCP init (sec) (5), TCP Half Closed (sec) (120), TCP Time Wait (sec) (15), Unverified RST (sec) (30), UDP (sec) (30), and Captive Portal (sec) (30).

The first few topics below provide brief summaries of the Transport Layer of the OSI model, TCP, UDP, and ICMP. For more information about the protocols, refer to their respective RFCs. The remaining topics describe the session timeouts and settings.

- ▲ [Transport Layer Sessions](#)
- ▲ [TCP](#)
- ▲ [UDP](#)
- ▲ [ICMP](#)
- ▲ [Configure Session Timeouts](#)
- ▲ [Configure Session Settings](#)
- ▲ [Prevent TCP Split Handshake Session Establishment](#)

## Transport Layer Sessions

A network session is an exchange of messages that occurs between two or more communication devices, lasting for some period of time. A session is established and is torn down when the session ends. Different types of sessions occur at three layers of the OSI model: the Transport layer, the Session layer, and the Application layer.

The Transport Layer operates at Layer 4 of the OSI model, providing reliable or unreliable, end-to-end delivery and flow control of data. Internet protocols that implement sessions at the Transport layer include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

## TCP

Transmission Control Protocol (TCP) ([RFC 793](#)) is one of the main protocols in the Internet Protocol (IP) suite, and is so prevalent that it is frequently referenced together with IP as *TCP/IP*. TCP is considered a reliable transport protocol because it provides error-checking while transmitting and receiving segments, acknowledges segments received, and reorders segments that arrive in the wrong order. TCP also requests and provides retransmission of segments that were dropped. TCP is stateful and connection-oriented, meaning a connection between the sender and receiver is established for the duration of the session. TCP provides flow control of packets, so it can handle congestion over networks.

TCP performs a handshake during session setup to initiate and acknowledge a session. After the data is transferred, the session is closed in an orderly manner, where each side transmits a FIN packet and acknowledges it with an ACK packet. The handshake that initiates the TCP session is often a three-way handshake (an exchange of three messages) between the initiator and the listener, or it could be a variation, such as a four-way or five-way split handshake or a simultaneous open. The [TCP Split Handshake Drop](#) explains how to [Prevent TCP Split Handshake Session Establishment](#).

Applications that use TCP as their transport protocol include Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Telnet, Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), and Secure Shell (SSH).

The following topics describe details of the PAN-OS implementation of TCP.

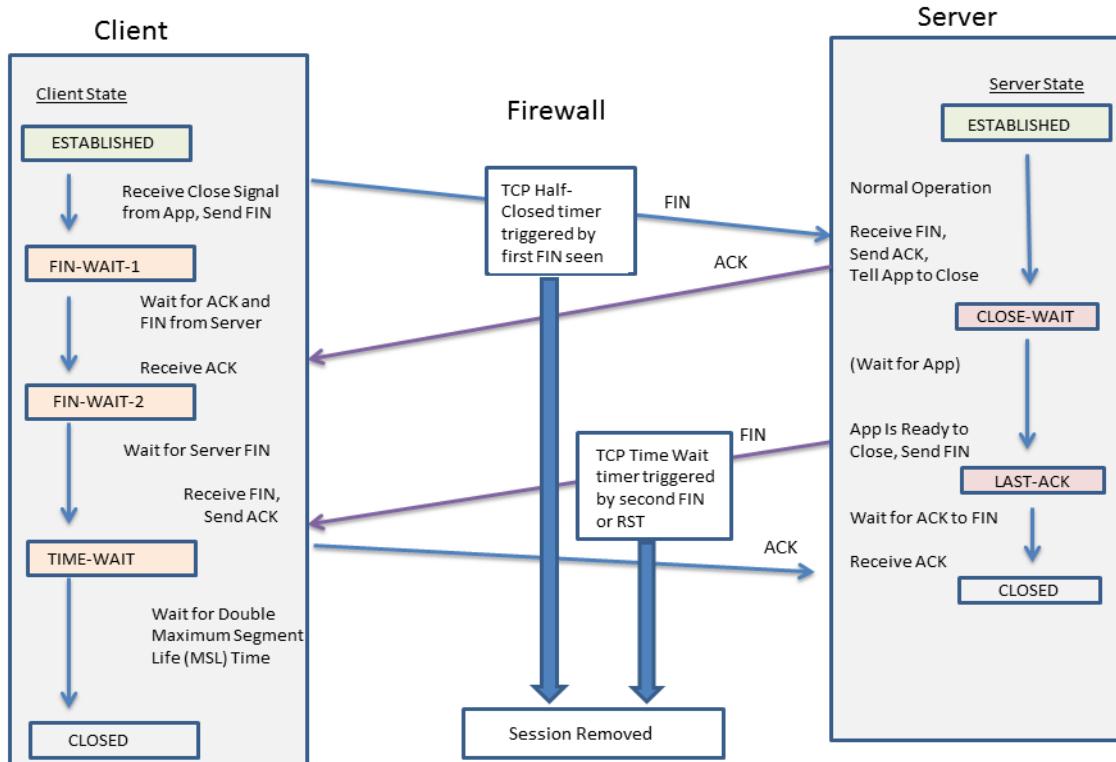
- ▲ [TCP Half Closed and TCP Time Wait Timers](#)
- ▲ [Unverified RST Timer](#)
- ▲ [TCP Split Handshake Drop](#)

### [TCP Half Closed and TCP Time Wait Timers](#)

The TCP connection termination procedure uses a TCP Half Closed timer, which is triggered by the first FIN the firewall sees for a session. The timer is named TCP Half Closed because only one side of the connection has sent a FIN. A second timer, TCP Time Wait, is triggered by the second FIN or a RST.

If the firewall were to have only one timer triggered by the first FIN, a setting that was too short could prematurely close the half-closed sessions. Conversely, a setting that was too long would make the session table grow too much and possibly use up all of the sessions. Two timers allow you to have a relatively long TCP Half Closed timer and a short TCP Time Wait timer, thereby quickly aging fully closed sessions and controlling the size of the session table.

The following figure illustrates when the firewall's two timers are triggered during the TCP connection termination procedure.



The TCP Time Wait timer should be set to a value less than the TCP Half Closed timer for the following reasons:

- The longer time allowed after the first FIN is seen gives the opposite side of the connection time to fully close the session.
- The shorter Time Wait time is because there is no need for the session to remain open for a long time after the second FIN or a RST is seen. A shorter Time Wait time frees up resources sooner, yet still allows time for the firewall to see the final ACK and possible retransmission of other datagrams.

If you configure a TCP Time Wait timer to a value greater than the TCP Half Closed timer, the commit will be accepted, but in practice the TCP Time Wait timer will not exceed the TCP Half Closed value.

The timers can be set globally or per application. The global settings are used for all applications by default. If you configure TCP wait timers at the application level, they override the global settings.

## Unverified RST Timer

If the firewall receives a Reset (RST) packet that cannot be verified (because it has an unexpected sequence number within the TCP window or it is from an asymmetric path), the Unverified RST timer controls the aging out of the session. It defaults to 30 seconds; the range is 1-600 seconds. The Unverified RST timer provides an additional security measure, explained in the second bullet below.

A RST packet will have one of three possible outcomes:

- A RST packet that falls outside the TCP window is dropped.

- A RST packet that falls inside the TCP window but does not have the exact expected sequence number is unverified and subject to the Unverified RST timer setting. This behavior helps prevent denial of service (DoS) attacks where the attack tries to disrupt existing sessions by sending random RST packets to the firewall.
- A RST packet that falls within the TCP window and has the exact expected sequence number is subject to the TCP Time Wait timer setting.

## TCP Split Handshake Drop

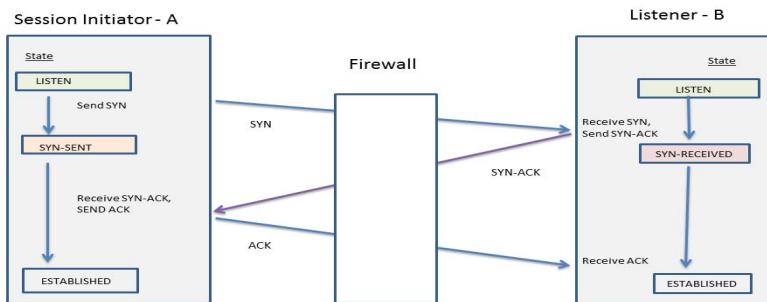
The **Split Handshake** option in a Zone Protection profile will prevent a TCP session from being established if the session establishment procedure does not use the well-known three-way handshake, but instead uses a variation, such as a four-way or five-way split handshake or a simultaneous open.

The Palo Alto Networks next-generation firewall correctly handles sessions and all Layer 7 processes for split handshake and simultaneous open session establishment without enabling the **Split Handshake** option.

Nevertheless, the **Split Handshake** option (which causes a TCP split handshake drop) is made available. When the **Split Handshake** option is configured for a Zone Protection profile and that profile is applied to a zone, TCP sessions for interfaces in that zone must be established using the standard three-way handshake; variations are not allowed.

The **Split Handshake** option is disabled by default.

The following illustrates the standard three-way handshake used to establish a TCP session with a PAN-OS firewall between the initiator (typically a client) and the listener (typically a server).



The **Split Handshake** option is configured for a Zone Protection profile that is assigned to a zone. An interface that is a member of the zone drops any synchronization (SYN) packets sent from the server, preventing the following variations of handshakes. The letter A in the figure indicates the session initiator and B indicates the listener. Each numbered segment of the handshake has an arrow indicating the direction of the segment from the sender to the receiver, and each segment indicates the control bit(s) setting.

4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

You can [Prevent TCP Split Handshake Session Establishment](#).

## UDP

User Datagram Protocol (UDP) ([RFC 768](#)) is another main protocol of the IP suite, and is an alternative to TCP. UDP is stateless and connectionless in that there is no handshake to set up a session, and no connection between the sender and receiver; the packets may take different routes to get to a single destination. UDP is considered an unreliable protocol because it does not provide acknowledgments, error-checking, retransmission, or reordering of datagrams. Without the overhead required to provide those features, UDP has reduced latency and is faster than TCP. UDP is referred to as a best-effort protocol because there is no mechanism or guarantee to ensure that the data will arrive at its destination.

Although UDP uses a checksum for data integrity, it performs no error checking at the network interface level. Error checking is assumed to be unnecessary or is performed by the application rather than UDP itself. UDP has no mechanism to handle flow control of packets.

UDP is often used for applications that require faster speeds and time-sensitive, real-time delivery, such as Voice over IP (VoIP), streaming audio and video, and online games. UDP is transaction-oriented, so it is also used for applications that respond to small queries from many clients, such as Domain Name System (DNS) and Trivial File Transfer Protocol (TFTP).

## ICMP

Internet Control Message Protocol (ICMP) ([RFC 792](#)) is another one of the main protocols of the Internet Protocol suite; it operates at the Network layer of the OSI model. ICMP is used for diagnostic and control purposes, to send error messages about IP operations, or messages about requested services or the reachability of a host or router. Network utilities such as traceroute and ping are implemented by using various ICMP messages.

ICMP is a connectionless protocol that does not open or maintain actual sessions. However, the ICMP messages between two devices can be considered a session.

Palo Alto Networks firewalls support ICMPv4 and ICMPv6. ICMPv4 and ICMPv6 error packets can be controlled by configuring a security policy for a zone, and selecting the **icmp** or **ipv6-icmp** application in the policy. Additionally, the ICMPv6 error packet rate can be controlled through the session settings, as described in the section [Configure Session Settings](#).

## ICMPv6 Rate Limiting

ICMPv6 rate limiting is a throttling mechanism to prevent flooding and DDoS attempts. The implementation employs an error packet rate and a token bucket, which work together to enable throttling and ensure that ICMP packets do not flood the network segments protected by the firewall.

First the global ICMPv6 error packet rate controls the rate at which ICMP error packets are allowed through the firewall; the default is 100 packets per second; the range is 10 to 65535 packets per second. If the firewall reaches the ICMP error packet rate, then the token bucket comes into play and throttling occurs, as follows.

The concept of a logical token bucket controls the rate at which ICMP messages can be transmitted. The number of tokens in the bucket is configurable, and each token represents an ICMP message that can be sent. The token count is decremented each time an ICMP message is sent; when the bucket reaches zero tokens, no more ICMP messages can be sent until another token is added to the bucket. The default size of the token bucket is 100 tokens (packets); the range is 10 to 65535 tokens.

To change the default token bucket size or error packet rate, see the section [Configure Session Settings](#).

## Configure Session Timeouts

A session timeout defines the duration of time for which PAN-OS maintains a session on the firewall after inactivity in the session. By default, when the session timeout for the protocol expires, PAN-OS closes the session.

On the firewall, you can define a number of timeouts for TCP, UDP, and ICMP sessions in particular. The Default timeout applies to any other type of session. All of these timeouts are global, meaning they apply to all of the sessions of that type on the firewall.

In addition to the global settings, you have the flexibility to define timeouts for an individual application in the **Objects > Applications** tab. The firewall applies application timeouts to an application that is in established state. When configured, timeouts for an application override the global TCP or UDP session timeouts.

Returning to the global settings, perform the optional tasks below if you need to change default values of the global session timeout settings for TCP, UDP, ICMP, Captive Portal authentication, or other types of sessions. All values are in seconds.



The defaults are optimal values. However, you can modify these according to your network needs. Setting a value too low could cause sensitivity to minor network delays and could result in a failure to establish connections with the firewall. Setting a value too high could delay failure detection.

### Change Session Timeouts

Step 1	Access the Session Settings.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Session</b>.</li><li>2. In the Session Timeouts section, click the Edit icon.</li></ol>
Step 2	(Optional) Change miscellaneous timeouts.	<ul style="list-style-type: none"><li>• <b>Default</b>—Maximum length of time that a non-TCP/UDP or non-ICMP session can be open without a response (range is 1-1599999; default is 30).</li><li>• <b>Discard Default</b>—Maximum length of time that a non-TCP/UDP session remains open after PAN-OS denies a session based on security policies configured on the firewall (range is 1-1599999; default is 60).</li><li>• <b>Scan</b>—Maximum length of time that any session remains open after it is considered inactive; an application is regarded as inactive when it exceeds the application trickling threshold defined for the application (range is 5-30; default is 10).</li><li>• <b>Captive Portal</b>—Authentication session timeout for the Captive Portal web form. To access the requested content, the user must enter the authentication credentials in this form and be successfully authenticated (range is 1-1599999; default is 30). To define other Captive Portal timeouts, such as the idle timer and the expiration time before the user must be re-authenticated, select <b>Device &gt; User Identification &gt; Captive Portal Settings</b>. See Configure Captive Portal in <a href="#">User-ID</a>.</li></ul>

<b>Change Session Timeouts (Continued)</b>	
<b>Step 3</b> (Optional) Change TCP timeouts.	<ul style="list-style-type: none"> <li>• <b>Discard TCP</b>—Maximum length of time that a TCP session remains open after it is denied based on a security policy configured on the firewall. Default: 90. Range: 1-1599999.</li> <li>• <b>TCP</b>—Maximum length of time that a TCP session remains open without a response, after a TCP session is in the Established state (after the handshake is complete and/or data is being transmitted). Default: 3600. Range: 1-1599999.</li> <li>• <b>TCP Handshake</b>—Maximum length of time permitted between receiving the SYN-ACK and the subsequent ACK to fully establish the session. Default: 10. Range: 1-60.</li> <li>• <b>TCP init</b>—Maximum length of time permitted between receiving the SYN and SYN-ACK prior to starting the TCP handshake timer. Default: 5. Range: 1-60.</li> <li>• <b>TCP Half Closed</b>—Maximum length of time between receiving the first FIN and receiving the second FIN or a RST. Default: 120. Range: 1-604800.</li> <li>• <b>TCP Time Wait</b>—Maximum length of time after receiving the second FIN or a RST. Default: 15. Range: 1-600.</li> <li>• <b>Unverified RST</b>—Maximum length of time after receiving a RST that cannot be verified (the RST is within the TCP window but has an unexpected sequence number, or the RST is from an asymmetric path). Default: 30. Range: 1-600.</li> <li>• See also the <b>Scan</b> timeout in the section <a href="#">(Optional) Change miscellaneous timeouts</a>.</li> </ul>
<b>Step 4</b> (Optional) Change UDP timeouts.	<ul style="list-style-type: none"> <li>• <b>Discard UDP</b>—Maximum length of time that a UDP session remains open after it is denied based on a security policy configured on the firewall. Default: 60. Range: 1-1599999.</li> <li>• <b>UDP</b>—Maximum length of time that a UDP session remains open without a UDP response. Default: 30. Range: 1-1599999.</li> <li>• See also the <b>Scan</b> timeout in the section <a href="#">(Optional) Change miscellaneous timeouts</a>.</li> </ul>
<b>Step 5</b> (Optional) Change ICMP timeouts.	<ul style="list-style-type: none"> <li>• <b>ICMP</b>—Maximum length of time that an ICMP session can be open without an ICMP response. Default: 6. Range: 1-1599999.</li> <li>• See also the <b>Discard Default</b> and <b>Scan</b> timeout in the section <a href="#">(Optional) Change miscellaneous timeouts</a>.</li> </ul>
<b>Step 6</b> Commit the changes.	Click <b>OK</b> and <b>Commit</b> the changes.

## Configure Session Settings

This topic describes various settings for sessions other than timeouts values. Perform these optional tasks if you need to change the default settings.

Change Session Settings	
Step 1 Access the Session Settings.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Session</b>.</li><li>2. In the <b>Session Settings</b> section, click the <b>Edit</b> icon.</li></ol>
Step 2 (Optional) Change session settings.	<ul style="list-style-type: none"><li>• <b>Rematch Sessions</b>—Causes the firewall to apply newly configured security policies to sessions that are already in progress. This capability is enabled by default. If this setting is disabled, any policy change applies only to sessions initiated after the policy change was committed. For example, if a Telnet session started while an associated policy was configured that allowed Telnet, and you subsequently committed a policy change to deny Telnet, the firewall applies the revised policy to the current session and blocks it.</li><li>• <b>ICMPv6 Token Bucket Size</b>—Default: 100 tokens. See the section <a href="#">ICMPv6 Rate Limiting</a>.</li><li>• <b>ICMPv6 Error Packet Rate (per sec)</b>—Default: 100. See the section <a href="#">ICMPv6 Rate Limiting</a>.</li><li>• <b>Enable IPv6 Firewalling</b>—Enables firewall capabilities for IPv6. All IPv6-based configurations are ignored if IPv6 is not enabled. Even if IPv6 is enabled for an interface, the <b>IPv6 Firewalling</b> setting must also be enabled for IPv6 to function.</li><li>• <b>Enable Jumbo Frame</b>—Enables jumbo frame support on Ethernet interfaces. Jumbo frames have a maximum transmission unit (MTU) of 9216 bytes and are available on certain platforms. <b>Global MTU</b>—Establishes the maximum transmission unit (MTU) available globally; this field is tied to the <b>Enable Jumbo Frame</b> field.<ul style="list-style-type: none"><li>• If you do not check <b>Enable Jumbo Frame</b>, the <b>Global MTU</b> defaults to 1500 bytes; the range is 576 to 1500 bytes.</li><li>• If you check <b>Enable Jumbo Frame</b>, the <b>Global MTU</b> defaults to 9192 bytes; the range is 9192 to 9216 bytes.</li></ul> If you enable jumbo frames and you have interfaces where the MTU is not specifically configured, those interfaces will automatically inherit the jumbo frame size. Therefore, before you enable jumbo frames, if you have any interface that you do not want to have jumbo frames, you must set the MTU for that interface to 1500 bytes or another value.</li><li>• <b>NAT64 IPv6 Minimum Network MTU</b>—Sets the global MTU for IPv6 translated traffic. The default of 1280 bytes is based on the standard minimum MTU for IPv6 traffic.</li></ul>

**Change Session Settings (Continued)**

	<ul style="list-style-type: none"><li>• <b>NAT Oversubscription Rate</b>—If NAT is configured to be Dynamic IP and Port (DIPP) translation, an oversubscription rate can be configured to multiply the number of times that the same translated IP address and port pair can be used concurrently. The rate is 1, 2, 4, or 8. The default setting is based on the <a href="#">firewall platform</a>.<ul style="list-style-type: none"><li>• A rate of 1 means no oversubscription; each translated IP address and port pair can be used only once at a time.</li><li>• If the setting is <b>Platform Default</b>, user configuration of the rate is disabled and the default oversubscription rate for the platform applies. Reducing the oversubscription rate decreases the number of source device translations, but provides higher NAT rule capacities.</li></ul></li><li>• <b>Accelerated Aging</b>—Enables faster aging-out of idle sessions. Select the check box to enable accelerated aging, and, if necessary, change the threshold (%) and scaling factor.<ul style="list-style-type: none"><li>• <b>Accelerated Aging Threshold</b>—Percentage of the session table that is full when accelerated aging begins. The default is 80%. When the session table reaches this threshold (% full), PAN-OS applies the <b>Accelerated Aging Scaling Factor</b> to the aging calculations for all sessions.</li><li>• <b>Accelerated Aging Scaling Factor</b>—Scaling factor used in the accelerated aging calculations. The default scaling factor is 2, meaning that the accelerated aging occurs at a rate twice as fast as the configured idle time. The configured idle time divided by 2 results in a faster timeout of one-half the time. To calculate the session's accelerated aging, PAN-OS divides the configured idle time (for that type of session) by the scaling factor to determine a shorter timeout. For example, if the scaling factor is 10, a session that would normally time out after 3600 seconds would time out 10 times faster (in 1/10 of the time), which is 360 seconds.</li></ul></li></ul>
<b>Step 3</b>	Commit the changes. Click <b>OK</b> and <b>Commit</b> the changes.
<b>Step 4</b>	Reboot the firewall after changing the jumbo frame configuration. <ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Operations</b>.</li><li>2. Click <b>Reboot Device</b>.</li></ol>

## Prevent TCP Split Handshake Session Establishment

You can configure a [TCP Split Handshake Drop](#) in a Zone Protection profile to prevent TCP sessions from being established unless they use the standard three-way handshake. This task assumes that the interface where this feature is desired is already assigned to a security zone.

<b>Configure a Zone Protection Profile to Prevent TCP Split Handshake Sessions</b>	
<b>Step 1</b> Configure a Zone Protection profile to prevent TCP sessions that use anything other than a three-way handshake to establish a session.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Network Profiles &gt; Zone Protection</b> and click <b>Add</b> to create a new profile (or select an existing profile).</li><li>2. If creating a new profile, enter a <b>Name</b> for the profile and an optional <b>Description</b>.</li><li>3. Select <b>Packet Based Attack Protection &gt; TCP Drop</b> and select the <b>Split Handshake</b> check box.</li><li>4. Click <b>OK</b>.</li></ol>
<b>Step 2</b> Apply the profile to one or more security zones.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Zones</b> and select the zone where you want to assign the zone protection profile.</li><li>2. In the Zone window, from the <b>Zone Protection Profile</b> drop-down, select the profile you configured in <a href="#">Step 1</a>. Alternatively, you could start creating a new profile here by clicking <b>Zone Protection Profile</b>, in which case you would continue accordingly.</li><li>3. Click <b>OK</b>.</li><li>4. (Optional) Repeat steps 1-3 to apply the profile to additional zones.</li></ol>
<b>Step 3</b> Save the configuration.	Click <b>OK</b> and <b>Commit</b> .

# DHCP

This section describes Dynamic Host Configuration Protocol (DHCP) and the tasks required to configure an interface on a Palo Alto Networks firewall to act as a DHCP server, client, or relay agent. By assigning these roles to different interfaces, the firewall can perform multiple roles.

- ▲ [DHCP Overview](#)
- ▲ [DHCP Messages](#)
- ▲ [DHCP Addressing](#)
- ▲ [DHCP Options](#)
- ▲ [Firewall as a DHCP Server and Client](#)
- ▲ [Configure an Interface as a DHCP Server](#)
- ▲ [Configure an Interface as a DHCP Client](#)
- ▲ [Configure an Interface as a DHCP Relay Agent](#)
- ▲ [Monitor and Troubleshoot DHCP](#)

## DHCP Overview

DHCP is a standardized protocol defined in [RFC 2131, Dynamic Host Configuration Protocol](#). DHCP has two main purposes: to provide TCP/IP and link-layer configuration parameters and to provide network addresses to dynamically configured hosts on a TCP/IP network.

DHCP uses a client-server model of communication. This model consists of three roles that the device can fulfill: DHCP client, DHCP server, and DHCP relay agent.

- A device acting as a DHCP client (host) can request an IP address and other configuration settings from a DHCP server. Users on client devices save configuration time and effort, and need not know the network's addressing plan or other resources and options they are inheriting from the DHCP server.
- A device acting as a DHCP server can service clients. By using any of three [DHCP Addressing](#) mechanisms, the network administrator saves configuration time and has the benefit of reusing a limited number of IP addresses when a client no longer needs network connectivity. The server can deliver IP addressing and many DHCP options to many clients.
- A device acting as a DHCP relay agent transmits DHCP messages between DHCP clients and servers.

DHCP uses [User Datagram Protocol \(UDP\)](#), [RFC 768](#), as its transport protocol. DHCP messages that a client sends to a server are sent to well-known port 67 (UDP—Bootstrap Protocol and DHCP). [DHCP Messages](#) that a server sends to a client are sent to port 68.

An interface on a Palo Alto Networks firewall can perform the role of a DHCP server, client, or relay agent. The interface of a DHCP server or relay agent must be a Layer 3 Ethernet, Aggregated Ethernet, or Layer 3 VLAN interface. You configure the firewall's interfaces with the appropriate settings for any combination of roles. The behavior of each role is summarized in [Firewall as a DHCP Server and Client](#).

The firewall supports DHCPv4 Server and DHCPv6 Relay. However, a single interface cannot support both DHCPv4 Server and DHCPv6 Relay.

The DHCP standard, [RFC 2131](#), is designed to support IPv4 and IPv6 addresses. The Palo Alto Networks implementations of DHCP server and DHCP client support IPv4 addresses only. Its DHCP relay implementation supports IPv4 and IPv6.

DHCP client is not supported in High Availability active/active mode.

## DHCP Messages

DHCP uses eight standard message types, which are identified by an option type number in the DHCP message. For example, when a client wants to find a DHCP server, it broadcasts a DHCPDISCOVER message on its local physical subnetwork. If there is no DHCP server on its subnet and if DHCP Helper or DHCP Relay is configured properly, the message is forwarded to DHCP servers on a different physical subnet. Otherwise, the message will go no further than the subnet on which it originated. One or more DHCP servers will respond with a DHCPOFFER message that contains an available network address and other configuration parameters.

When the client needs an IP address, it sends a DHCPREQUEST to one or more servers. Of course if the client is requesting an IP address, it doesn't have one yet, so [RFC 2131](#) requires that the broadcast message the client sends out have a source address of 0 in its IP header.

When a client requests configuration parameters from a server, it might receive responses from more than one server. Once a client has received its IP address, it is said that the client has at least an IP address and possibly other configuration parameters *bound* to it. DHCP servers manage such binding of configuration parameters to clients.

The following table lists the DHCP messages.

DHCP Message	Description
DHCPDISCOVER	Client broadcast to find available DHCP servers.
DHCPOFFER	Server response to client's DHCPDISCOVER, offering configuration parameters.
DHCPREQUEST	Client message to one or more servers to do any of the following: <ul style="list-style-type: none"> <li>Request parameters from one server and implicitly decline offers from other servers.</li> <li>Confirm that a previously allocated address is correct after, for example, a system reboot.</li> <li>Extend the lease of a network address.</li> </ul>
DHCPCACK	Server to client acknowledgment message containing configuration parameters, including a confirmed network address.
DCHPNAK	Server to client negative acknowledgment indicating the client's understanding of the network address is incorrect (for example, if the client has moved to a new subnet), or a client's lease has expired.
DCHPDECLINE	Client to server message indicating the network address is already being used.
DCHPRELEASE	Client to server message giving up the user of the network address and canceling the remaining time on the lease.
DCHPINFORM	Client to server message requesting only local configuration parameters; client has an externally configured network address.

## DHCP Addressing

- ▲ [DHCP Address Allocation Methods](#)
- ▲ [DHCP Leases](#)

### DHCP Address Allocation Methods

There are three ways that a DHCP server either assigns or sends an IP address to a client:

- **Automatic allocation**—The DHCP server assigns a permanent IP address to a client from its **IP Pools**. On the firewall, a **Lease** specified as **Unlimited** means the allocation is permanent.
- **Dynamic allocation**—The DHCP server assigns a reusable IP address from **IP Pools** of addresses to a client for a maximum period of time, known as a *lease*. This method of address allocation is useful when the customer has a limited number of IP addresses; they can be assigned to clients who need only temporary access to the network. See the [DHCP Leases](#) section.
- **Static allocation**—The network administrator chooses the IP address to assign to the client and the DHCP server sends it to the client. A static DHCP allocation is permanent; it is done by configuring a DHCP server and choosing a **Reserved Address** to correspond to the **MAC Address** of the client device. The DHCP assignment remains in place even if the client logs off, reboots, has a power outage, etc.

Static allocation of an IP address is useful, for example, if you have a printer on a LAN and you do not want its IP address to keep changing, because it is associated with a printer name through DNS. Another example is if a client device is used for something crucial and must keep the same IP address, even if the device is turned off, unplugged, rebooted, or a power outage occurs, etc.

Keep these points in mind when configuring a **Reserved Address**:

- It is an address from the **IP Pools**. You may configure multiple reserved addresses.
- If you configure no **Reserved Address**, the clients of the server will receive new DHCP assignments from the pool when their leases expire or if they reboot, etc. (unless you specified that a **Lease is Unlimited**).
- If you allocate all of the addresses in the **IP Pools** as a **Reserved Address**, there are no dynamic addresses free to assign to the next DHCP client requesting an address.
- You may configure a **Reserved Address** without configuring a **MAC Address**. In this case, the DHCP server will not assign the **Reserved Address** to any device. You might reserve a few addresses from the pool and statically assign them to a fax and printer, for example, without using DHCP.

### DHCP Leases

A lease is defined as the time period for which a DHCP server allocates a network address to a client. The lease might be extended (renewed) upon subsequent requests. If the client no longer needs the address, it can release the address back to the server before the lease is up. The server is then free to assign that address to a different client if it has run out of unassigned addresses.

The lease period configured for a DHCP server applies to all of the addresses that a single DHCP server (interface) dynamically assigns to its clients. That is, all of that interface's addresses assigned dynamically are of **Unlimited** duration or have the same **Timeout** value. A different DHCP server configured on the firewall may have a different lease term for its clients. A **Reserved Address** is a static address allocation and is not subject to the lease terms.

Per the DHCP standard, [RFC 2131](#), a DHCP client does not wait for its lease to expire, because it risks getting a new address assigned to it. Instead, when a DHCP client reaches the halfway point of its lease period, it attempts to extend its lease so that it retains the same IP address. Thus, the lease duration is like a sliding window.

Typically if an IP address was assigned to a device, the device was subsequently taken off the network and its lease was not extended, the DHCP server will let that lease run out. Because the client is gone from the network and no longer needs the address, the lease duration in the server is reached and the lease is in “Expired” state.

The firewall has a hold timer that prevents the expired IP address from being reassigned immediately. This behavior temporarily reserves the address for the device in case it comes back onto the network. But if the address pool runs out of addresses, the server re-allocates this expired address before the hold timer expires. Expired addresses are cleared automatically as the system needs more addresses or when the hold timer releases them.

In the CLI, use the `show dhcp server lease` operational command to view lease information about the allocated IP addresses. If you do not want to wait for expired leases to be released automatically, you can use the `clear dhcp lease interface value expired-only` command to clear expired leases, making those addresses available in the pool again. You can use the `clear dhcp lease interface value ip ip` command to release a particular IP address. Use the `clear dhcp lease interface value mac mac_address` command to release a particular MAC address.

## DHCP Options

The history of DHCP and DHCP options traces back to the Bootstrap Protocol (BOOTP). BOOTP was used by a host to configure itself dynamically during its booting procedure. A host could receive an IP address and a file from which to download a boot program from a server, along with the server's address and the address of an Internet gateway.

Included in the BOOTP packet was a vendor information field, which could contain a number of tagged fields containing various types of information, such as the subnet mask, the BOOTP file size, and many other values. [RFC 1497](#) describes the [BOOTP Vendor Information Extensions](#). DHCP replaces BOOTP; BOOTP is not supported on the firewall.

These extensions eventually expanded with the use of DHCP and DHCP host configuration parameters, also known as options. Similar to vendor extensions, DHCP options are tagged data items that provide information to a DHCP client. The options are sent in a variable-length field at the end of a DHCP message. For example, the DHCP Message Type is option 53, and a value of 1 indicates the DHCPDISCOVER message. DHCP options are defined in [RFC 2132](#), [DHCP Options](#) and [BOOTP Vendor Extensions](#).

A DHCP client can negotiate with the server, limiting the server to send only those options that the client requests.

- ▲ [Predefined DHCP Options](#)
- ▲ [Multiple Values for a DHCP Option](#)
- ▲ [DHCP Options 43, 55, and 60 and Other Customized Options](#)

### Predefined DHCP Options

Palo Alto Networks firewalls support user-defined and predefined DHCP options in the DHCP server implementation. Such options are configured on the DHCP server and sent to the clients that sent a DHCPREQUEST to the server. The clients are said to *inherit* and implement the options that they are programmed to accept.

The firewall supports the following predefined options on its DHCP servers, shown in the order in which they appear on the **DHCP Server** configuration screen:

DHCP Option	DHCP Option Name
51	Lease duration
3	Gateway
1	IP Pool Subnet (mask)
6	Domain Name System (DNS) server address (primary and secondary)
44	Windows Internet Name Service (WINS) server address (primary and secondary)
41	Network Information Service (NIS) server address (primary and secondary)
42	Network Time Protocol (NTP) server address (primary and secondary)
70	Post Office Protocol Version 3 (POP3) server address

DHCP Option	DHCP Option Name
69	Simple Mail Transfer Protocol (SMTP) server address
15	DNS suffix

As mentioned, you can also configure vendor-specific and customized options, which support a wide variety of office equipment, such as IP phones and wireless infrastructure devices. Each option code supports multiple values, which can be IP address, ASCII, or hexadecimal format. With the firewall enhanced DHCP option support, branch offices do not need to purchase and manage their own DHCP servers in order to provide vendor-specific and customized options to DHCP clients.

## Multiple Values for a DHCP Option

You can enter multiple option values for an **Option Code** with the same **Option Name**, but all values for a particular code and name combination must be the same type (IP address, ASCII, or hexadecimal). If one type is inherited or entered, and later a different type is entered for the same code and name combination, the second type will overwrite the first type.

You can enter an **Option Code** more than once by using a different **Option Name**. In this case, the **Option Type** for the Option Code can differ among the multiple option names. For example, if option Coastal Server (option code 6) is configured with IP address type, option Server XYZ (option code 6) with ASCII type is also allowed.

The firewall sends multiple values for an option (strung together) to a client in order from top to bottom. Therefore, when entering multiple values for an option, enter the values in the order of preference, or else move the options to achieve your preferred order in the list. The order of options in the firewall configuration determines the order that the options appear in DHCPOFFER and DHCPACK messages.

You can enter an option code that already exists as a predefined option code, and the customized option code will override the predefined DHCP option; the firewall issues a warning.

## DHCP Options 43, 55, and 60 and Other Customized Options

The following table describes the option behavior for several options described in [RFC 2132](#).

Option Code	Option Name	Option Description/Behavior
43	Vendor Specific Information	<p>Sent from server to client. Vendor-specific information that the DHCP server has been configured to offer to the client. The information is sent to the client only if the server has a Vendor Class Identifier (VCI) in its table that matches the VCI in the client's DHCPREQUEST.</p> <p>An Option 43 packet can contain multiple vendor-specific pieces of information. It can also include encapsulated, vendor-specific extensions of data.</p>
55	Parameter Request List	<p>Sent from client to server. List of configuration parameters (option codes) that a DHCP client is requesting, possibly in order of the client's preference. The server tries to respond with options in the same order.</p>

Option Code	Option Name	Option Description/Behavior
60	Vendor Class Identifier (VCI)	Sent from client to server. Vendor type and configuration of a DHCP client. The DHCP client sends option code 60 in a DHCPREQUEST to the DHCP server. When the server receives option 60, it sees the VCI, finds the matching VCI in its own table, and then it returns option 43 with the value (that corresponds to the VCI), thereby relaying vendor-specific information to the correct client. Both the client and server have knowledge of the VCI.

You can send custom, vendor-specific option codes that are not defined in RFC 2132. The option codes can be in the range 1-254 and of fixed or variable length.



Custom DHCP options are not validated by the DHCP Server; you must ensure that you enter correct values for the options you create.

For ASCII and hexadecimal DHCP option types, the option value can be a maximum of 255 octets.

## Firewall as a DHCP Server and Client

The firewall can function as a DHCP server and as a DHCP client. The firewall DHCP server operates in the following manner:

- When the DHCP server receives a DHCPDISCOVER message from a client, the server replies with a DHCPOFFER message containing all of the predefined and user-defined options in the order they appear in the configuration. The client selects the options it needs and responds with a DHCPREQUEST message.
- When the server receives a DHCPREQUEST message from a client, the server replies with its DHCPACK message containing only the options specified in the request.
- [Dynamic Host Configuration Protocol, RFC 2131](#), is designed to support IPv4 and IPv6 addresses. The Palo Alto Networks implementation of DHCP server supports IPv4 addresses only.

The firewall [DHCP Client](#) operates in the following manner:

- When the DHCP client receives a DHCPOFFER from the server, the client automatically caches all of the options offered for future use, regardless of which options it had sent in its DHCPREQUEST.
- By default and to save memory consumption, the client caches only the first value of each option code if it receives multiple values for a code.
- There is no maximum length for DHCP messages unless the DHCP client specifies a maximum in option 57 in its DHCPDISCOVER or DHCPREQUEST messages.

## Configure an Interface as a DHCP Server

The prerequisites for this task are:

- Configure a Layer 3 Ethernet or Layer 3 VLAN interface.
- Assign the interface to a virtual router and a zone.
- Determine a valid pool of IP addresses from your network plan that you can designate to be assigned by your DHCP server to clients.
- Collect the DHCP options, values, and Vendor Class Identifiers you plan to configure.

Perform the following task to configure an interface on the firewall to act as a DHCP server. You can configure multiple DHCP servers.

### Configure an Interface as a DHCP Server

**Step 1** Select an interface to be a DHCP Server.

1. Select **Network > DHCP > DHCP Server** and click **Add**.
2. Enter an **Interface** name or select one from the drop-down.
3. For **Mode**, select **enabled** or **auto** mode. Auto mode enables the server and disables it if another DHCP server is detected on the network. The **disabled** setting disables the server.
4. (Optional) Click the **Ping IP when allocating new IP** check box if you want the server to ping the IP address before it assigns that address to its client.



If the ping receives a response, that means a different device already has that address, so it is not available. The server assigns the next address from the pool instead. This behavior is similar to [Optimistic Duplicate Address Detection \(DAD\) for IPv6, RFC 4429](#).



After you set options and return to the DHCP server tab, the **Probe IP** column for the interface indicates if this check box was checked.

## Configure an Interface as a DHCP Server (Continued)

<p><b>Step 2</b> Configure the predefined <a href="#">DHCP Options</a> that the server sends to its clients.</p>	<ul style="list-style-type: none"><li>In the Options section, select a <b>Lease</b> type:<ul style="list-style-type: none"><li><b>Unlimited</b> causes the server to dynamically choose IP addresses from the <b>IP Pools</b> and assign them permanently to clients.</li><li><b>Timeout</b> determines how long the lease will last. Enter the number of <b>Days</b> and <b>Hours</b>, and optionally the number of <b>Minutes</b>.</li></ul></li><li><b>Inheritance Source</b>—Leave <b>None</b> or select a source DHCP client interface or PPPoE client interface to propagate various server settings into the DHCP server. If you specify an <b>Inheritance Source</b>, select one or more options below that you want <b>inherited</b> from this source.<p>Specifying an inheritance source allows the firewall to quickly add DHCP options from the upstream server received by the DHCP client. It also keeps the client options updated if the source changes an option. For example, if the source replaces its NTP server (which had been identified as the <b>Primary NTP</b> server), the client will automatically inherit the new address as its <b>Primary NTP</b> server.</p><p> When inheriting DHCP option(s) that contain multiple IP addresses, the firewall uses only the first IP address contained in the option to conserve cache memory. If you require multiple IP addresses for a single option, configure the DHCP options directly on that firewall rather than configure inheritance.</p><ul style="list-style-type: none"><li><b>Check inheritance source status</b>—If you selected an <b>Inheritance Source</b>, clicking this link opens the <b>Dynamic IP Interface Status</b> window, which displays the options that were inherited from the DHCP client.</li><li><b>Gateway</b>—IP address of the network gateway (an interface on the firewall) that is used to reach any device not on the same LAN as this DHCP server.</li><li><b>Subnet Mask</b>—Network mask used with the addresses in the <b>IP Pools</b>.</li></ul></li></ul>
--	---

**Configure an Interface as a DHCP Server (Continued)**

For the following fields, click the down arrow and select **None**, or **inherited**, or enter a remote server's IP address that your DHCP server will send to clients for accessing that service. If you select **inherited**, the DHCP server inherits the values from the source DHCP client specified as the **Inheritance Source**.

- **Primary DNS, Secondary DNS**—IP address of the preferred and alternate Domain Name System (DNS) servers.
- **Primary WINS, Secondary WINS**—IP address of the preferred and alternate Windows Internet Naming Service (WINS) servers.
- **Primary NIS, Secondary NIS**—IP address of the preferred and alternate Network Information Service (NIS) servers.
- **Primary NTP, Secondary NTP**—IP address of the available Network Time Protocol servers.
- **POP3 Server**—IP address of a Post Office Protocol (POP3) server.
- **SMTP Server**—IP address of a Simple Mail Transfer Protocol (SMTP) server.
- **DNS Suffix**—Suffix for the client to use locally when an unqualified hostname is entered that it cannot resolve.

### Configure an Interface as a DHCP Server (Continued)

<p><b>Step 3</b> (Optional) Configure a vendor-specific or custom DHCP option that the DHCP server sends to its clients.</p>	<ol style="list-style-type: none"> <li>1. In the Custom DHCP Options section, click <b>Add</b> and enter a descriptive <b>Name</b> to identify the DHCP option.</li> <li>2. Enter the <b>Option Code</b> you want to configure the server to offer (range is 1-254). (See <a href="#">RFC 2132</a> for option codes.)</li> <li>3. If the <b>Option Code</b> is 43, the <b>Vendor Class Identifier</b> field appears. Enter a VCI, which is a string or hexadecimal value (with 0x prefix) used as a match against a value that comes from the client Request containing option 60. The server looks up the incoming VCI in its table, finds it, and returns Option 43 and the corresponding option value.</li> <li>4. <b>Inherit from DHCP server inheritance source</b>—Select this check box only if you specified an <b>Inheritance Source</b> for the DHCP Server predefined options and you want the vendor-specific and custom options also to be <b>inherited</b> from this source.</li> <li>5. <b>Check inheritance source status</b>—If you selected an <b>Inheritance Source</b>, clicking this link opens <b>Dynamic IP Interface Status</b>, which displays the options that were inherited from the DHCP client.</li> <li>6. If you did not select the <b>Inherit from DHCP server inheritance source</b> check box, select an <b>Option Type: IP Address, ASCII, or Hexadecimal</b>. Hexadecimal values must start with the 0x prefix.</li> <li>7. Enter the <b>Option Value</b> you want the DHCP server to offer for that <b>Option Code</b>. You can enter multiple values on separate lines.</li> <li>8. Click <b>OK</b>.</li> </ol>
<p><b>Step 4</b> (Optional) Add another vendor-specific or custom DHCP option.</p>	<ol style="list-style-type: none"> <li>1. Repeat <a href="#">Step 3</a> to enter another custom DHCP Option. <ul style="list-style-type: none"> <li>• You can enter multiple option values for an <b>Option Code</b> with the same <b>Option Name</b>, but all values for an <b>Option Code</b> must be the same type (<b>IP Address, ASCII, or Hexadecimal</b>). If one type is inherited or entered and a different type is entered for the same <b>Option Code</b> and the same <b>Option Name</b>, the second type will overwrite the first type. When entering multiple values for an option, enter the values in the order of preference, or else move the Custom DHCP Options to achieve the preferred order in the list. Select an option and click <b>Move Up</b> or <b>Move Down</b>.</li> <li>• You can enter an <b>Option Code</b> more than once by using a different <b>Option Name</b>. In this case, the <b>Option Type</b> for the Option Code can differ among the multiple option names.</li> </ul> </li> <li>2. Click <b>OK</b>.</li> </ol>

**Configure an Interface as a DHCP Server (Continued)**

<p><b>Step 5</b> Identify the stateful pool of IP addresses from which the DHCP server chooses an address and assigns it to a DHCP client.</p> <p> If you are not the network administrator for your network, ask the network administrator for a valid pool of IP addresses from the network plan that can be designated to be assigned by your DHCP server.</p>	<ol style="list-style-type: none"><li>1. In the <b>IP Pools</b> field, click <b>Add</b> and enter the range of IP addresses from which this server assigns an address to a client. Enter an IP subnet and subnet mask (for example, 192.168.1.0/24) or a range of IP addresses (for example, 192.168.1.10-192.168.1.20). At least one IP pool is required.</li><li>2. Optionally repeat to specify another IP address pool.</li></ol>
<p><b>Step 6</b> (Optional) Specify an IP address from the IP pools that will not be assigned dynamically. If you also specify a <b>MAC Address</b>, the <b>Reserved Address</b> is assigned to that device when the device requests an IP address through DHCP.</p> <p> See the <a href="#">DHCP Addressing</a> section for an explanation of allocation of a <b>Reserved Address</b>.</p>	<ol style="list-style-type: none"><li>1. In the <b>Reserved Address</b> field, click <b>Add</b>.</li><li>2. Enter an IP address from the <b>IP Pools</b> (format x.x.x.x) that you do not want to be assigned dynamically by the DHCP server.</li><li>3. (Optional) Specify the <b>MAC Address</b> (format xx:xx:xx:xx:xx:xx) of the device to which you want to permanently assign the IP address specified in Step 2.</li><li>4. (Optional) Repeat Steps 2-3 to reserve another address.</li></ol>
<p><b>Step 7</b> Save the configuration.</p>	<p>Click <b>OK</b> and <b>Commit</b> the change.</p>

## Configure an Interface as a DHCP Client

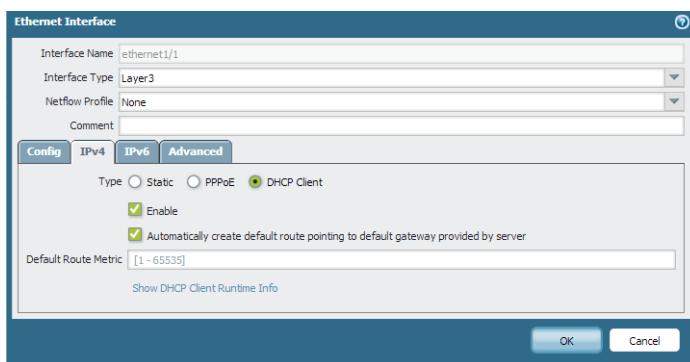
Before configuring a firewall interface as a **DHCP Client**, make sure you have configured a Layer 3 Ethernet or Layer 3 VLAN interface, and the interface is assigned to a virtual router and a zone. Perform this task if you need to use DHCP to request an IPv4 address for an interface on your firewall.

### Configure an Interface as a DHCP Client

**Step 1** Configure an interface as a DHCP client.

1. Select **Network > Interfaces**.
2. On the **Ethernet** tab or the **VLAN** tab, click **Add** and enter an interface, or click a configured interface, that you want to be a DHCP client.

The following shows the **Ethernet Interface** screen:



3. Click the **IPv4** tab; for **Type**, select **DHCP Client**.
4. Select the **Enable** check box.
5. Optionally select the **Automatically create default route pointing to default gateway provided by server** check box. This causes the firewall to create a static route to a default gateway that will be useful when clients are trying to access many destinations that do not need to have routes maintained in a routing table on the firewall.
6. Optionally enter a **Default Route Metric** (priority level) for the route between the firewall and the DHCP server (range is 1-65535; there is no default metric). A route with a lower number has higher priority during route selection. For example, a route with a metric of 10 is used before a route with a metric of 100.
7. Optionally click **Show DHCP Client Runtime Info** to see all of the settings the client has inherited from its DHCP server.

**Step 2** Save the configuration.

Click **OK** and **Commit** the change.

Now the Ethernet interface indicates **Dynamic-DHCP Client** in its **IP Address** field on the **Ethernet** tab.

**Configure an Interface as a DHCP Client**

**Step 3** (Optional) See which interfaces on the firewall are configured as DHCP clients.

1. Select **Network > Interfaces > Ethernet** and look in the **IP Address** field to see which interfaces indicate DHCP Client.
2. Select **Network > Interfaces > VLAN** and look in the **IP Address** field to see which interfaces indicate DHCP Client.

## Configure an Interface as a DHCP Relay Agent

Before configuring a firewall interface as a DHCP relay agent, make sure you have configured a Layer 3 Ethernet or Layer 3 VLAN interface, and the interface is assigned to a virtual router and a zone. You want that interface be able to pass DHCP messages between clients and servers. The interface can forward messages to a maximum of four external DHCP servers. A client DHCPDISCOVER message is sent to all configured servers, and the DHCPOFFER message of the first server that responds is relayed back to the requesting client.

Perform the following task to configure an interface on the firewall to act as a DHCP relay agent:

<b>Configure an Interface as a DHCP Relay Agent</b>	
<b>Step 1</b> Select DHCP Relay.	Select <b>Network &gt; DHCP &gt; DHCP Relay</b> .
<b>Step 2</b> Specify the IP address of each DHCP server with which the DHCP relay agent will communicate.	<ol style="list-style-type: none"><li>1. In the <b>Interface</b> field, select from the drop-down the interface you want to be the DHCP relay agent.</li><li>2. Check either the <b>IPv4</b> or <b>IPv6</b> check box, indicating the type of DHCP server address you will specify.</li><li>3. If you checked <b>IPv4</b>, in the <b>DHCP Server IP Address</b> field, click <b>Add</b>. Enter the address of the DHCP server to and from which you will relay DHCP messages.</li><li>4. If you checked <b>IPv6</b>, in the <b>DHCP Server IPv6 Address</b> field, click <b>Add</b>. Enter the address of the DHCP server to and from which you will relay DHCP messages. If you specify a <i>multicast</i> address, also specify an outgoing <b>Interface</b>.</li><li>5. Optionally repeat Steps 2-4 to enter a maximum of four DHCP server addresses.</li></ol>
<b>Step 3</b> Save the configuration.	Click <b>OK</b> and <b>Commit</b> the change.

## Monitor and Troubleshoot DHCP

You can view the status of dynamic address leases that your DHCP server has assigned or that your DHCP client has been assigned by issuing commands from the [CLI](#). You can also clear leases before they time out and are released automatically.

- ▲ [View DHCP Server Information](#)
- ▲ [Clear Leases Before They Expire Automatically](#)
- ▲ [View DHCP Client Information](#)
- ▲ [Gather Debug Output about DHCP](#)

### [View DHCP Server Information](#)

To view DHCP pool statistics, IP addresses the server has assigned, the corresponding MAC address, state and duration of the lease, and time the lease began, use the following command. If the address was configured as a **Reserved Address**, the **state** column indicates reserved and there is no duration or **lease\_time**. If the lease was configured as **Unlimited**, the duration column displays a value of 0.

```
admin@PA-200> show dhcp server lease all
interface: "ethernet1/2"
Allocated IPs: 1, Total number of IPs in pool: 5. 20.0000% used
ip           mac           state      duration    lease_time
192.168.3.11  f0:2f:af:42:70:cf  committed   0          Wed Jul  2 08:10:56 2014
admin@PA-200>
```

To view the options that a DHCP server has assigned to clients, use the following command:

```
admin@PA-200> show dhcp server settings all
Interface     GW        DNS1        DNS2        DNS-Suffix  Inherit source
-----
ethernet1/2    192.168.3.1  10.43.2.10  10.44.2.10          ethernet1/3
admin@PA-200>
```

### [Clear Leases Before They Expire Automatically](#)

The following example shows how to release expired **DHCP Leases** of an interface (server) before the hold timer releases them automatically. Those addresses will be available in the IP pool again.

```
admin@PA-200> clear dhcp lease interface ethernet1/2 expired-only
```

The following example shows how to release the lease of a particular IP address:

```
admin@PA-200> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

The following example shows how to release the lease of a particular MAC address:

```
admin@PA-200> clear dhcp lease interface ethernet1/2 mac f0:2c:ae:29:71:34
```

## View DHCP Client Information

To view the status of IP address leases sent to the firewall when it is acting as a DHCP client, use the `show dhcp client state interface_name` command or the following command:

```
admin@PA-200> show dhcp client state all
Interface      State       IP           Gateway      Leased-until
-----
ethernet1/1    Bound      10.43.14.80  10.43.14.1   70315
admin@PA-200>
```

## Gather Debug Output about DHCP

To gather debug output about DHCP, use one of the following commands:

```
admin@PA-200> debug dhcpcd
admin@PA-200> debug management-server dhcpcd
```

## NAT

This section describes Network Address Translation (NAT) and how to configure NAT rules and features. NAT was introduced to solve the problem of an organization not having enough public, globally-routable IPv4 addresses assigned to it by the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry. NAT translates private, non-routable IPv4 addresses to one or more globally-routable IPv4 addresses, thereby conserving an organization's routable IP addresses.

Since its origination, the use of NAT has expanded. For example, NAT is used as a way to not disclose the real IP addresses of hosts that need access to public addresses. It is also used to manage traffic by performing port forwarding. NAT can be used to solve network design challenges, enabling networks with identical IP subnets to communicate with each other.

The [NAT64](#) option translates between IPv6 and IPv4 addresses, providing connectivity between networks using disparate IP addressing schemes, and therefore a migration path to IPv6 addressing. IPv6-to-IPv6 Network Prefix Translation ([NPTv6](#)) translates one IPv6 prefix to another IPv6 prefix. PAN-OS supports all of these functions.

If you use private IP addresses within your internal networks, you must use NAT to translate the private addresses to public addresses that can be routed on external networks. In PAN-OS, you create NAT policy rules that instruct the firewall which packet addresses need translation and what the translated addresses are.

- ▲ [NAT Policy Rules](#)
- ▲ [Source NAT and Destination NAT](#)
- ▲ [NAT Rule Capacities](#)
- ▲ [Dynamic IP and Port NAT Oversubscription](#)
- ▲ [Dataplane NAT Memory Statistics](#)
- ▲ [Configure NAT](#)
- ▲ [NAT Configuration Examples](#)

## NAT Policy Rules

- ▲ NAT Policy Rule Functionality
- ▲ NAT Address Pools Identified as Address Objects
- ▲ Proxy ARP for NAT Address Pools

### NAT Policy Rule Functionality

You configure a NAT rule to match a packet's source zone and destination zone, at a minimum. In addition to zones, you can configure matching criteria based on the packet's destination interface, source and destination address, and service. You can configure multiple NAT rules. The firewall evaluates the rules in order from the top down. Once a packet matches the criteria of a single NAT rule, the packet is not subjected to additional NAT rules. Therefore, your list of NAT rules should be in order from most specific to least specific so that packets are subjected to the most specific rule you created for them.

Static NAT rules do not have precedence over other forms of NAT. Therefore, for static NAT to work, the static NAT rules must be above all other NAT rules in the list on the firewall.

NAT rules provide address translation, and are different from security policy rules, which allow or deny packets. It is important to understand the firewall's flow logic when it applies NAT rules and security policy rules so that you can determine what rules you need, based on the zones you have defined.

Upon ingress, the firewall inspects the packet and does a route lookup to determine the egress interface and zone. Then the firewall determines if the packet matches one of the NAT rules that have been defined, based on source and/or destination zone. It then evaluates and applies any security policies that match the packet based on the original (pre-NAT) source and destination addresses, but the post-NAT zones. Finally, upon egress, for a matching NAT rule, the firewall translates the source and/or destination address and port numbers.

Keep in mind that the translation of the IP address and port do not occur until the packet leaves the firewall. The NAT rules and security policies apply to the original IP address (the pre-NAT address). A NAT rule is configured based on the zone associated with a pre-NAT IP address.

Security policies differ from NAT rules because security policies examine post-NAT zones to determine whether the packet is allowed or not. Because the very nature of NAT is to modify source or destination IP addresses, which can result in modifying the packet's outgoing interface and zone, security policies are enforced on the post-NAT zone.

You can verify the NAT rules processed by using the CLI `test nat-policy-match` command in operational mode. For example:

```
user@device1> test nat-policy-match ?  
+ destination      Destination IP address  
+ destination-port Destination port  
+ from            From zone  
+ ha-device-id    HA Active/Active device ID  
+ protocol        IP protocol value  
+ source          Source IP address  
+ source-port     Source port  
+ to              To Zone  
+ to-interface    Egress interface to use  
|                 Pipe through a command
```

<Enter> Finish input

```
user@device1> test nat-policy-match from 13-untrust source 10.1.1.1 destination
66.151.149.20 destination-port 443 protocol 6
```

Destination-NAT: Rule matched: CA2-DEMO  
66.151.149.20:443 => 192.168.100.15:443

## NAT Address Pools Identified as Address Objects

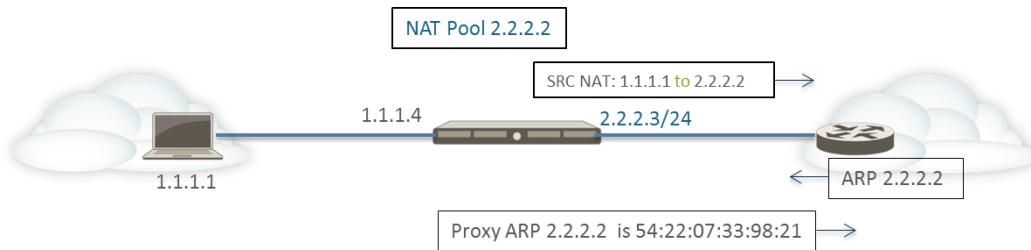
When configuring a **Dynamic IP** or **Dynamic IP and Port** NAT address pool in a NAT policy rule, it is typical to configure the pool of translated addresses with address objects. Each address object can be a host IP address, IP address range, or IP subnet.



Because both NAT rules and security policy rules use address objects, it is a best practice to distinguish between them by naming an address object used for NAT with a prefix, such as "NAT-name."

## Proxy ARP for NAT Address Pools

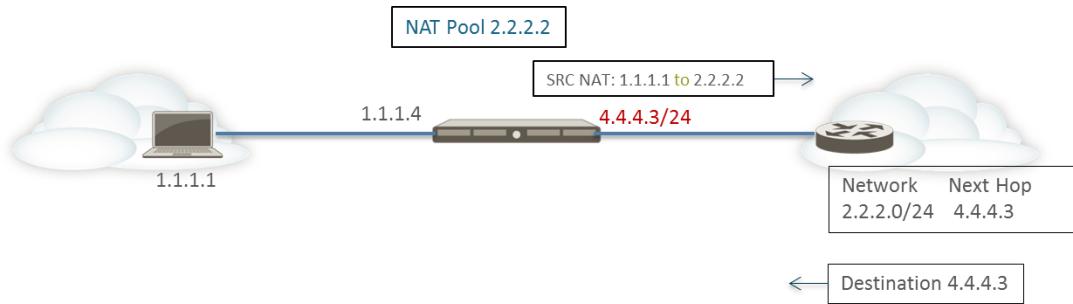
NAT address pools are not bound to any interfaces. The following figure illustrates the behavior of the firewall when it is performing proxy ARP for an address in a NAT address pool.



The firewall performs source NAT for a client, translating the source address 1.1.1.1 to the address in the NAT pool, 2.2.2.2. The translated packet is sent on to a router.

For the return traffic, the router does not know how to reach 2.2.2.2 (because the IP address 2.2.2.2 is just an address in the NAT address pool), so it sends an ARP request packet to the firewall.

- If the address pool (2.2.2.2) is in the same subnet as the egress/ingress interface IP address (2.2.2.3/24), the firewall can send a proxy ARP reply to the router, indicating the Layer 2 MAC address of the IP address, as shown in the figure above.
- If the address pool (2.2.2.2) is not a subnet of an interface on the firewall, the firewall will not send a proxy ARP reply to the router. This means that the router must be configured with the necessary route to know where to send packets destined for 2.2.2.2, in order to ensure the return traffic is routed back to the firewall, as shown in the figure below.



## Source NAT and Destination NAT

The firewall supports both source address and/or port translation and destination address and/or port translation.

### Source NAT

Source NAT is typically used by internal users to access the Internet; the source address is translated and thereby kept private. There are three types of source NAT:

- **Dynamic IP and Port (DIPP)**—Allows multiple hosts to have their source IP addresses translated to the same public IP address with different port numbers. The dynamic translation is to the next available address in the NAT address pool, which you configure as a **Translated Address** pool to be an IP address, range of addresses, a subnet, or a combination of these.

As an alternative to using the next address in the NAT address pool, DIPP allows you to specify the address of the **Interface** itself. The advantage of specifying the interface in the NAT rule is that the NAT rule will be automatically updated to use any address subsequently acquired by the interface. DIPP is sometimes referred to as interface-based NAT or network address port translation (NAPT).

DIPP has a default NAT oversubscription rate, which is the number of times that the same translated IP address and port pair can be used concurrently. For more information, see [Dynamic IP and Port NAT Oversubscription](#) and [Modify the Oversubscription Rate for DIPP NAT](#).

- **Dynamic IP**—Allows the one-to-one, dynamic translation of a source IP address only (no port number) to the next available address in the NAT address pool. The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use **Advanced (Dynamic IP/Port Fallback)** to enable use of DIPP addresses when necessary. In either event, as sessions terminate and the addresses in the pool become available, they can be allocated to translate new connections.

Dynamic IP NAT supports the option for you to [Reserve Dynamic IP NAT Addresses](#).

- **Static IP**—Allows the 1-to-1, static translation of a source IP address, but leaves the source port unchanged. A common scenario for a static IP translation is an internal server that must be available to the Internet.

### Destination NAT

Destination NAT is performed on incoming packets, when the firewall translates a public destination address to a private address. Destination NAT does not use address pools or ranges. It is a 1-to-1, static translation with the option to perform port forwarding or port translation.

- **Static IP**—Allows the 1-to-1, static translation of a destination IP address and optionally the port number. One common use of destination NAT is to configure several NAT rules that map a single public destination address to several private destination host addresses assigned to servers or services. In this case, the destination port numbers are used to identify the destination hosts. For example:

- **Port Forwarding**—Can translate a public destination address and port number to a private destination address, but keeps the same port number.
- **Port Translation**—Can translate a public destination address and port number to a private destination address and a different port number, thus keeping the real port number private. It is configured by entering a **Translated Port** on the **Translated Packet** tab in the NAT policy rule. See the [Destination NAT with Port Translation Example](#).

## NAT Rule Capacities

The number of NAT rules allowed is based on the firewall platform. Individual rule limits are set for static, Dynamic IP (DIP), and Dynamic IP and Port (DIPP) NAT. The sum of the number of rules used for these NAT types cannot exceed the total NAT rule capacity. For DIPP, the rule limit is based on the device's oversubscription setting (8, 4, 2, or 1) and the assumption of one translated IP address per rule. To see platform-specific NAT rule limits and translated IP address limits, use the [Compare Firewalls](#) tool.

Consider the following when working with NAT rules:

- If you run out of pool resources, you cannot create more NAT rules, even if the platform's maximum rule count has not been reached.
- If you consolidate NAT rules, the logging and reporting will also be consolidated. The statistics are provided per the rule, not per all of the addresses within the rule. If you need granular logging and reporting, do not combine the rules.

## Dynamic IP and Port NAT Oversubscription

Dynamic IP and Port (DIPP) NAT allows you to use each translated IP address and port pair multiple times (8, 4, or 2 times) in concurrent sessions. This reusability of an IP address and port (known as oversubscription) provides scalability for customers who have too few public IP addresses. The design is based on the assumption that hosts are connecting to different destinations, therefore sessions can be uniquely identified and collisions are unlikely. The oversubscription rate in effect multiplies the original size of the address/port pool to 8, 4, or 2 times the size. For example, the default limit of 64K concurrent sessions allowed, when multiplied by an oversubscription rate of 8, results in 512K concurrent sessions allowed.

The oversubscription rates that are allowed vary based on the platform. The oversubscription rate is global; it applies to the device. This oversubscription rate is set by default and consumes memory, even if you have enough public IP addresses available to make oversubscription unnecessary. You can reduce the rate from the default setting to a lower setting or even 1 (which means no oversubscription). By configuring a reduced rate, you decrease the number of source device translations possible, but increase the DIP and DIPP NAT rule capacities. To change the default rate, see [Modify the Oversubscription Rate for DIPP NAT](#).

If you select **Platform Default**, your explicit configuration of oversubscription is turned off and the default oversubscription rate for the platform applies, as shown in the table below. The **Platform Default** setting allows for an upgrade or downgrade of a software release.

The following table lists the default (highest) oversubscription rate for each platform.

Platform	Default Oversubscription Rate
PA-200	2
PA-500	2
PA-2020	2
PA-2050	2
PA-3020	2
PA-3050	2
PA-3060	2
PA-4020	4
PA-4050	8
PA-4060	8
PA-5020	4
PA-5050	8
PA-5060	8
PA-7050	8
PA-7080	8
VM-100	1

Platform	Default Oversubscription Rate
VM-200	1
VM-300	2
VM-1000-HV	2

The firewall supports a maximum of 256 translated IP addresses per NAT rule, and each platform supports a maximum number of translated IP addresses (for all NAT rules combined). If oversubscription causes the maximum translated addresses per rule (256) to be exceeded, the firewall will automatically reduce the oversubscription ratio in an effort to have the commit succeed. However, if your NAT rules result in translations that exceed the maximum translated addresses for the platform, the commit will fail.

## Dataplane NAT Memory Statistics

The `show running global-ippool` command displays statistics related to NAT memory consumption for a pool. The Size column displays the number of bytes of memory that the resource pool is using. The Ratio column displays the oversubscription ratio (for DIPP pools only). The lines of pool and memory statistics are explained in the following sample output:

```
admin@PA-7050-HA-0 (active-primary)>show running global-ippool
  
```

Idx	Type	From	To	Num	Ref.Cnt	Size	Ratio
1	DynamicIP	201.0.0.0-201.0.255.255	210.0.0.0	4096	2	657072	N/A
2	DynamicIP	202.0.0.0-202.0.0.255	220.0.0.0	256	1	41232	N/A
3	DynamicIP/Port	200.0.2.100-200.0.2.100	200.0.3.11	1	1	68720	8

Usable NAT DIP/DIPP shared memory size: 58490064      ← Total physical NAT memory (bytes)  
 Used NAT DIP/DIPP shared memory size: 767024 (1.3%)      ← Bytes and % of usable NAT memory  
 DynamicIP NAT Pool: 2 (1.19%)      ← Number of DIP pools in use and % of total usable memory that all DIP pools use  
 DynamicIP/Port NAT Pool: 1 (0.12%)      ← Number of DIPP pools in use and % of total usable memory that all DIPP pools use

For NAT pool statistics for a virtual system, the `show running ippool` command has columns indicating the memory size used per NAT rule and the oversubscription ratio used (for DIPP rules). The following is sample output for the command.

```
admin@PA-7050-HA-0 vsys1 (active-primary)> show running ippool
  
```

VSYS 1 has 4 NAT rules, DIP and DIPP rules:					
Rule	Type	Used	Available	Mem Size	Ratio
nat1	DynamicIP	0	4096	788144	0
nat2	DynamicIP	0	256	49424	0
nat3	DynamicIP/Port	0	638976	100976	4
nat11	DynamicIP	0	4096	788144	0

A field in the output of the `show running nat-rule-ippool rule` command shows the memory (bytes) used per NAT rule. The following is sample output for the command, with the memory usage for the rule encircled.

```
admin@PA-7050-HA-0 (active-primary)>show running nat-rule-ippool rule nat1
  
```

VSYS1 Rule nat1:  
 Rule:nat1, Pool index:1, memory usage: 788144

Reserve IP: no  
 201.0.0.0-201.0.255.255 =>  
 210.0.0.0-210.0.15.255

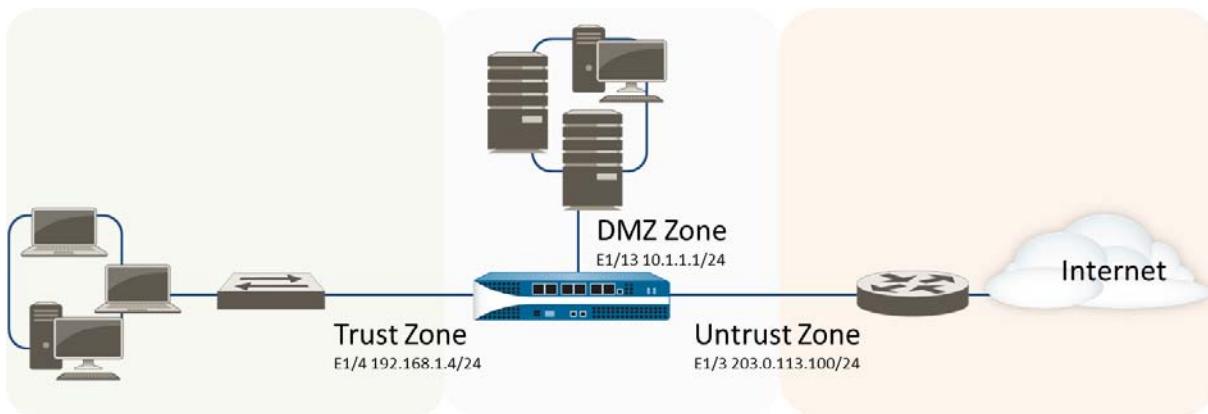
Source	Xlat-Source	Ref.Cnt (F)	TTL(s)
Total IPs in use: 0			
Total entries in time-reserve cache: 0			
Total freelist left: 4096			

## Configure NAT

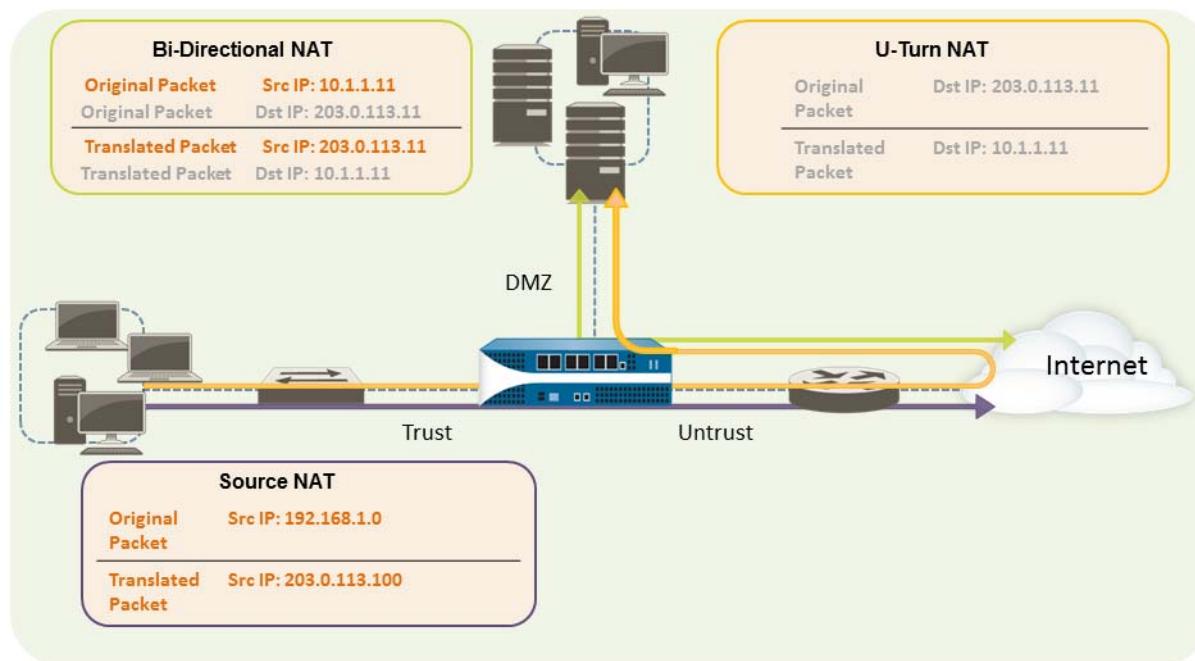
Perform the following tasks to configure various aspects of NAT. In addition to the examples below, there are examples in the section [NAT Configuration Examples](#).

- ▲ Translate Internal Client IP Addresses to Your Public IP Address (Source DIPP NAT)
- ▲ Enable Clients on the Internal Network to Access your Public Servers (Destination U-Turn NAT)
- ▲ Enable Bi-Directional Address Translation for Your Public-Facing Servers (Static Source NAT)
- ▲ Modify the Oversubscription Rate for DIPP NAT
- ▲ Disable NAT for a Specific Host or Interface
- ▲ Reserve Dynamic IP NAT Addresses

The NAT example in this section is based on the following topology, which was also used in [Getting Started](#) for setting up interfaces and zones:



Based on the topology initially used in [Getting Started](#) to create the interfaces and zones, there are three NAT policies we need to create as follows:



- To enable the clients on the internal network to access resources on the Internet, the internal 192.168.1.0 addresses will need to be translated to publicly routable addresses. In this case, we will configure source NAT (the purple enclosure and arrow above), using the egress interface address, 203.0.113.100, as the source address in all packets that leave the firewall from the internal zone. See [Translate Internal Client IP Addresses to Your Public IP Address \(Source DIPP NAT\)](#) for instructions.
- To enable clients on the internal network to access the public web server in the DMZ zone, we must configure a NAT rule that redirects the packet from the external network, where the original routing table lookup will determine it should go based on the destination address of 203.0.113.11 within the packet, to the actual address of the web server on the DMZ network of 10.1.1.11. To do this you must create a NAT rule from the trust zone (where the source address in the packet is) to the untrust zone (where the original destination address is) to translate the destination address to an address in the DMZ zone. This type of destination NAT is called *U-Turn NAT* (the yellow enclosure and arrow above). See [Enable Clients on the Internal Network to Access your Public Servers \(Destination U-Turn NAT\)](#) for instructions.
- To enable the web server—which has both a private IP address on the DMZ network and a public-facing address for access by external users—to both send and receive requests, the firewall must translate the incoming packets from the public IP address to the private IP address and the outgoing packets from the private IP address to the public IP address. On the firewall, you can accomplish this with a single bi-directional static source NAT policy (the green enclosure and arrow above). See [Enable Bi-Directional Address Translation for Your Public-Facing Servers \(Static Source NAT\)](#).

## Translate Internal Client IP Addresses to Your Public IP Address (Source DIPP NAT)

When a client on your internal network sends a request, the source address in the packet contains the IP address for the client on your internal network. If you use private IP address ranges internally, the packets from the client will not be able to be routed on the Internet unless you translate the source IP address in the packets leaving the network into a publicly routable address.

On the firewall you can do this by configuring a source NAT policy that translates the source address (and optionally the port) into a public address. One way to do this is to translate the source address for all packets to the egress interface on your firewall, as shown in the following procedure.

### Configure Source NAT

**Step 1** Create an address object for the external IP address you plan to use.

1. Select **Objects > Addresses** and then click **Add**.
2. Enter a **Name** and optionally a **Description** for the object.
3. Select **IP Netmask** from the **Type** drop-down and then enter the IP address of the external interface on the firewall, 203.0.113.100 in this example.

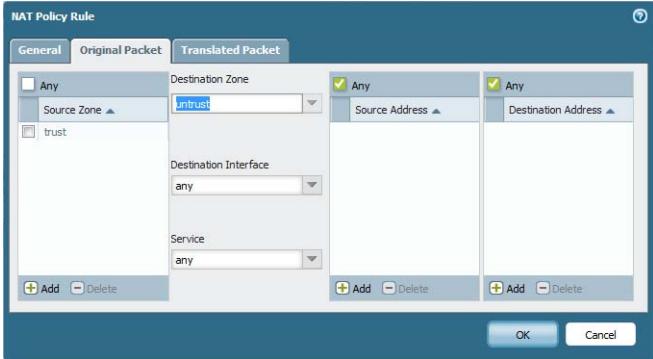
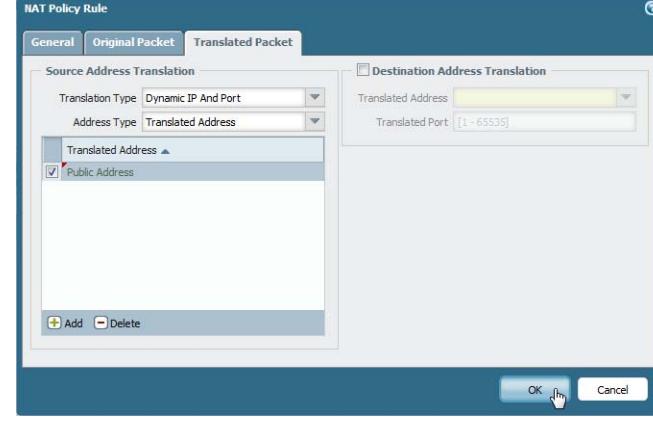


4. To save the address object, click **OK**.



Although you do not have to use address objects in your policies, it is a best practice because it simplifies administration by allowing you to make updates in one place rather than having to update every policy where the address is referenced.

### Configure Source NAT (Continued)

<p><b>Step 2</b> Create the NAT policy.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; NAT</b> and click <b>Add</b>.</li> <li>2. On the <b>General</b> tab, enter a descriptive <b>Name</b> for the policy.</li> <li>3. (Optional) Enter a tag, which is a keyword or phrase that allows you to sort or filter policies.</li> <li>4. For <b>NAT Type</b>, select <b>ipv4</b> (default).</li> <li>5. On the <b>Original Packet</b> tab, select the zone you created for your internal network in the <b>Source Zone</b> section (click <b>Add</b> and then select the zone) and the zone you created for the external network from the <b>Destination Zone</b> drop-down.</li> </ol>  <ol style="list-style-type: none"> <li>6. On the <b>Translated Packet</b> tab, select <b>Dynamic IP And Port</b> from the <b>Translation Type</b> drop-down in the Source Address Translation section of the screen.</li> <li>7. For <b>Address Type</b>, there are two choices. You could select <b>Translated Address</b> and then click <b>Add</b>. Select the address object you just created.</li> </ol>  <p>An alternative <b>Address Type</b> is <b>Interface Address</b>, in which case the translated address will be the IP address of the interface. For this choice, you would select an <b>Interface</b> and optionally an <b>IP Address</b> if the interface has more than one IP address.</p> <ol style="list-style-type: none"> <li>8. Click <b>OK</b> to save the NAT policy.</li> </ol>
<p><b>Step 3</b> Save the configuration.</p>	<p>Click <b>Commit</b>.</p>

### Configure Source NAT (Continued)

**Step 4** (Optional) Access the CLI to verify the translation.

1. Use the `show session all` command to view the session table, where you can verify the source IP address and port and the corresponding translated IP address and port.
2. Use the `show session id <id_number>` to view more details about a session.
3. If you configured Dynamic IP NAT, use the `show counter global filter aspect session severity drop | match nat` command to see if any sessions failed due to NAT IP allocation. If all of the addresses in the Dynamic IP NAT pool are allocated when a new connection is supposed to be translated, the packet will be dropped.

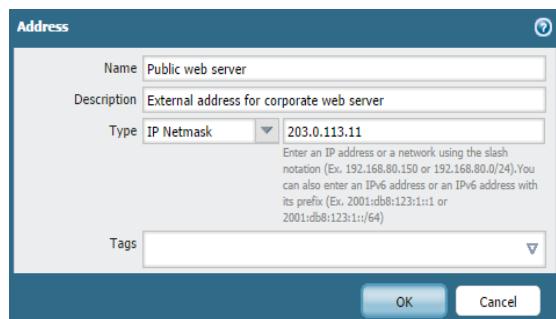
## Enable Clients on the Internal Network to Access your Public Servers (Destination U-Turn NAT)

When a user on the internal network sends a request for access to the corporate web server in the DMZ, the DNS server will resolve it to the public IP address. When processing the request, the firewall will use the original destination in the packet (the public IP address) and route the packet to the egress interface for the untrust zone. In order for the firewall to know that it must translate the public IP address of the web server to an address on the DMZ network when it receives requests from users on the trust zone, you must create a destination NAT rule that will enable the firewall to send the request to the egress interface for the DMZ zone as follows.

### Configure U-Turn NAT

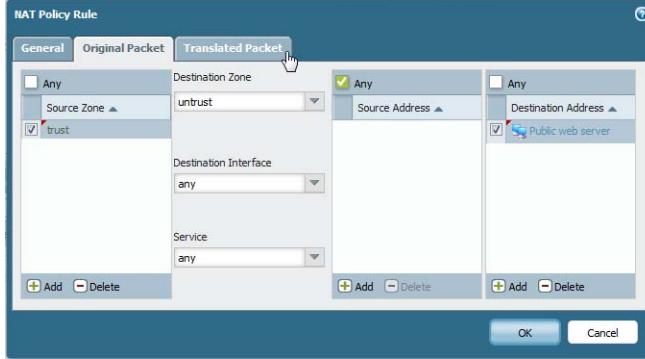
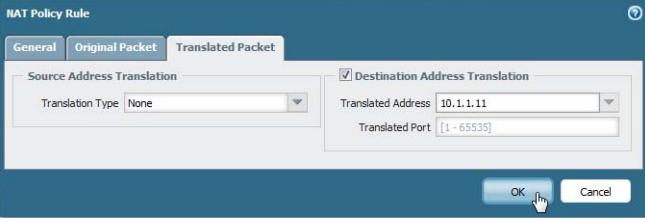
**Step 1** Create an address object for the web server.

1. Select **Objects > Addresses** and click **Add**.
2. Enter a **Name** and optionally a **Description** for the object.
3. Select **IP Netmask** from the **Type** drop-down and enter the public IP address of the web server, 203.0.113.11 in this example.



4. Click **OK**.

### Configure U-Turn NAT (Continued)

<p><b>Step 1</b> Create the NAT policy.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; NAT</b> and click <b>Add</b>.</li> <li>2. On the <b>General</b> tab, enter a descriptive <b>Name</b> for the NAT rule.</li> <li>3. On the <b>Original Packet</b> tab, select the zone you created for your internal network in the <b>Source Zone</b> section (click <b>Add</b> and then select the zone) and the zone you created for the external network from the <b>Destination Zone</b> drop-down.</li> <li>4. In the <b>Destination Address</b> section, click <b>Add</b> and select the address object you created for your public web server.</li> </ol>  <p>5. On the <b>Translated Packet</b> tab, select the <b>Destination Address Translation</b> check box and then enter the IP address that is assigned to the web server interface on the DMZ network, 10.1.1.11 in this example.</p>  <p>6. Click <b>OK</b> to save the NAT policy.</p>
<p><b>Step 2</b> Save the configuration.</p>	<p>Click <b>Commit</b>.</p>

### Enable Bi-Directional Address Translation for Your Public-Facing Servers (Static Source NAT)

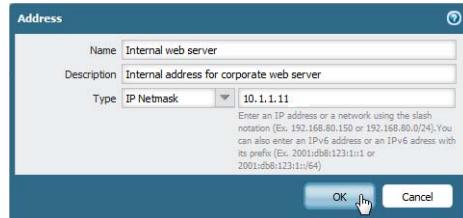
When your public-facing servers have private IP addresses assigned on the network segment where they are physically located, you need a source NAT rule to translate the source address of the server to the external address upon egress. You create a static NAT rule to translate the internal source address, 10.1.1.11, to the external web server address, 203.0.113.11 in our example.

However, a public-facing server must be able to both send and receive packets. You need a reciprocal policy that translates the public address (the destination IP address in incoming packets from Internet users) into the private address so that the firewall can route the packet to your DMZ network. You create a bi-directional static NAT rule, as described in the following procedure. Bi-directional translation is an option for static NAT only.

## Configure Bi-Directional NAT

**Step 1** Create an address object for the web server's internal IP address.

1. Select **Objects > Addresses** and click **Add**.
2. Enter a **Name** and optionally a **Description** for the object.
3. Select **IP Netmask** from the **Type** drop-down and enter the IP address of the web server on the DMZ network, 10.1.1.11 in this example.

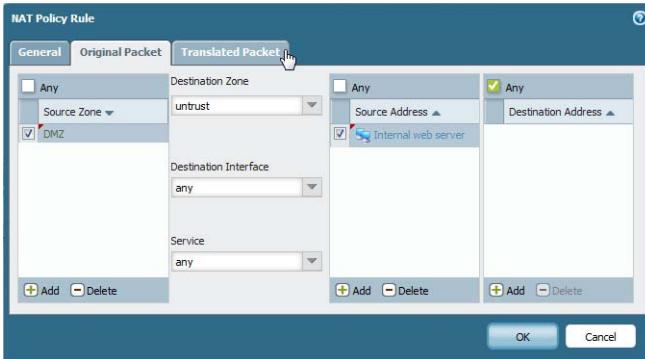
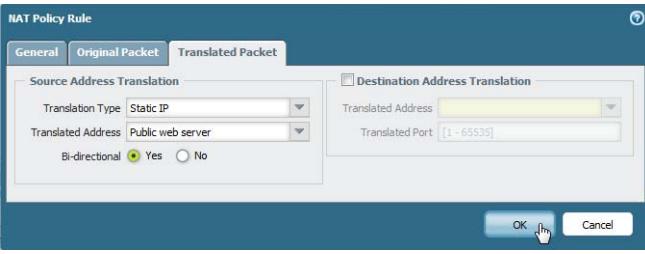


4. Click **OK**.



If you did not already create an address object for the *public* address of your web server, you should create that object now.

### Configure Bi-Directional NAT (Continued)

<p><b>Step 2</b> Create the NAT policy.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; NAT</b> and click <b>Add</b>.</li> <li>2. On the <b>General</b> tab, enter a descriptive <b>Name</b> for the NAT rule.</li> <li>3. On the <b>Original Packet</b> tab, select the zone you created for your DMZ in the <b>Source Zone</b> section (click <b>Add</b> and then select the zone) and the zone you created for the external network from the <b>Destination Zone</b> drop-down.</li> <li>4. In the <b>Source Address</b> section, click <b>Add</b> and select the address object you created for your internal web server address.</li> </ol>  <ol style="list-style-type: none"> <li>5. On the <b>Translated Packet</b> tab, select <b>Static IP</b> from the <b>Translation Type</b> drop-down in the <b>Source Address Translation</b> section and then select the address object you created for your external web server address from the <b>Translated Address</b> drop-down.</li> <li>6. In the <b>Bi-directional</b> field, select <b>Yes</b>.</li> </ol>  <ol style="list-style-type: none"> <li>7. Click <b>OK</b> to save the NAT policy.</li> </ol>
<p><b>Step 3</b> Save the configuration.</p>	Click <b>Commit</b> .

## Modify the Oversubscription Rate for DIPP NAT

If you have enough public IP addresses that you do not need to use DIPP NAT oversubscription, you can reduce the oversubscription rate and thereby gain more DIP and DIPP NAT rules allowed.

<b>Set NAT Oversubscription</b>	
<b>Step 1</b> View the DIPP NAT oversubscription rate.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Setup &gt; Session &gt; Session Settings</b>. View the <b>NAT Oversubscription Rate</b> setting.</li> </ol>
<b>Step 2</b> Set the DIPP NAT oversubscription rate.	<ol style="list-style-type: none"> <li>Click the Edit icon in the Session Settings section.</li> <li>In the <b>NAT Oversubscription Rate</b> drop-down, select <b>1x</b>, <b>2x</b>, <b>4x</b>, or <b>8x</b>, depending on which ratio you want.</li> </ol> <p> The <b>Platform Default</b> setting applies the default oversubscription setting for the platform. If you want no oversubscription, select <b>1x</b>.</p> <ol style="list-style-type: none"> <li>Click <b>OK</b> and <b>Commit</b> the change.</li> </ol>

## Disable NAT for a Specific Host or Interface

Both source NAT and destination NAT rules can be configured to disable address translation. You may have exceptions where you do not want NAT to occur for a certain host in a subnet or for traffic exiting a specific interface. The following procedure shows how to disable source NAT for a host.

<b>Create a Source NAT Exemption</b>	
<b>Step 1</b> Create the NAT policy.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; NAT</b> and click <b>Add</b>.</li> <li>Enter a descriptive <b>Name</b> for the policy.</li> <li>On the <b>Original Packet</b> tab, select the zone you created for your internal network in the <b>Source Zone</b> section (click <b>Add</b> and then select the zone) and the zone you created for the external network from the <b>Destination Zone</b> drop-down.</li> <li>For <b>Source Address</b>, click <b>Add</b> and enter the host address. Click <b>OK</b>.</li> <li>On the <b>Translated Packet</b> tab, select <b>None</b> from the <b>Translation Type</b> drop-down in the Source Address Translation section of the screen.</li> <li>Click <b>OK</b> to save the NAT policy.</li> </ol>
<b>Step 2</b> Save the configuration.	Click <b>Commit</b> .



NAT rules are processed in order from the top to the bottom, so place the NAT exemption policy before other NAT policies to ensure it is processed before an address translation occurs for the sources you want to exempt.

## Reserve Dynamic IP NAT Addresses

You can reserve Dynamic IP NAT addresses (for a configurable period of time) to prevent them from being allocated as translated addresses to a different source IP address that needs translation. When configured, the reservation applies to all of the translated Dynamic IP addresses in progress and any new translations.

For both translations in progress and new translations, when a source IP address is translated to an available translated IP address, that pairing is retained even after all sessions related to that specific source IP are expired. The reservation timer for each source IP address begins after all sessions that use that source IP address translation expire. Dynamic IP NAT is a one-to-one translation; one source IP address translates to one translated IP address that is chosen dynamically from those addresses available in the configured pool. Therefore, a translated IP address that is reserved is not available for any other source IP address until the reservation expires because a new session has not started. The timer is reset each time a new session for a source IP/translated IP mapping begins, after a period when no sessions were active.

By default, no addresses are reserved. You can reserve Dynamic IP NAT addresses for the firewall or for a virtual system.

### Reserve Dynamic IP NAT Addresses for a Firewall

```
Step 1 user@device1# set setting nat reserve-ip yes
```

```
Step 2 user@device1# set setting nat reserve-time <1-604800 secs>
```

### Reserve Dynamic IP NAT Addresses for a Virtual System

```
Step 1 user@device1# set vsys <vsysid> setting nat reserve-ip yes
```

```
Step 2 user@device1# set vsys <vsysid> setting nat reserve-time <1-604800 secs>
```

For example, suppose there is a Dynamic IP NAT pool of 30 addresses and there are 20 translations in progress when the `nat reserve-time` is set to 28800 seconds (8 hours). Those 20 translations are now reserved, so that when the last session (of any application) that uses each source IP/translated IP mapping expires, the translated IP address is reserved for only that source IP address for 8 hours, in case that source IP address needs translation again. Additionally, as the 10 remaining translated addresses are allocated, they each are reserved for their source IP address, each with a timer that begins when the last session for that source IP address expires.

In this manner, each source IP address can be repeatedly translated to its same NAT address from the pool; another host will not be assigned a reserved translated IP address from the pool, even if there are no active sessions for that translated address.

Suppose a source IP/translated IP mapping has all of its sessions expire, and the reservation timer of 8 hours begins. After a new session for that translation begins, the timer stops, and the sessions continue until they all end, at which point the reservation timer starts again, reserving the translated address.

The reservation timer remain in effect on the Dynamic IP NAT pool until you disable it by entering the `set setting nat reserve-ip no` command or you change the `nat reserve-time` to a different value.

The CLI commands for reservations do not affect Dynamic IP and Port (DIPP) or Static IP NAT pools.

## NAT Configuration Examples

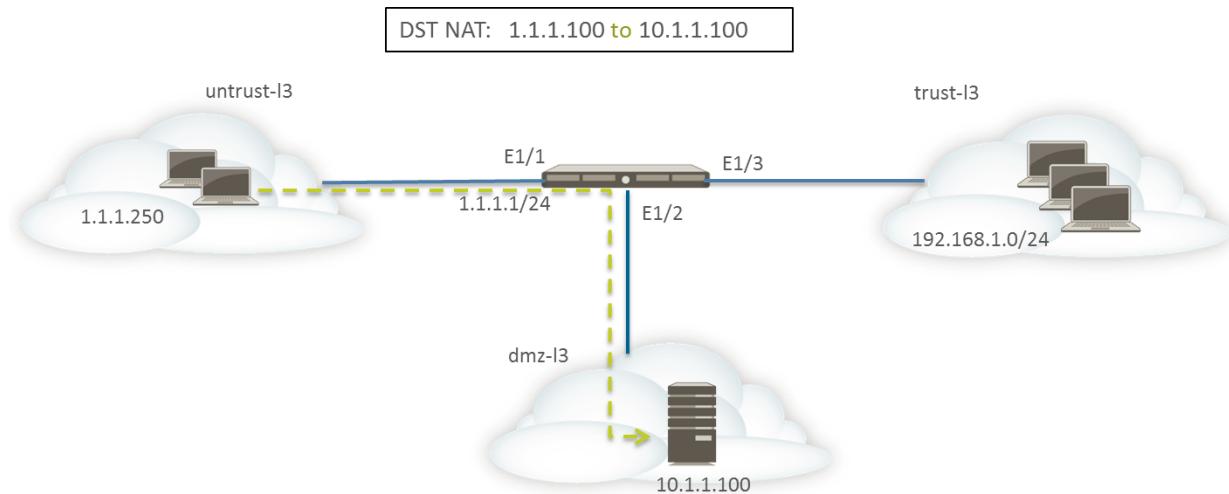
- ▲ Destination NAT Example—One-to-One Mapping
- ▲ Destination NAT with Port Translation Example
- ▲ Destination NAT Example—One-to-Many Mapping
- ▲ Source and Destination NAT Example
- ▲ Virtual Wire Source NAT Example
- ▲ Virtual Wire Static NAT Example
- ▲ Virtual Wire Destination NAT Example

### Destination NAT Example—One-to-One Mapping

The most common mistakes when configuring NAT and security rules are the references to the zones and address objects. The addresses used in destination NAT rules always refer to the original IP address in the packet (that is, the pre-translated address). The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address).

The addresses in the security policy also refer to the IP address in the original packet (that is, the pre-NAT address). However, the destination zone is the zone where the end host is physically connected. In other words, the destination zone in the security rule is determined after the route lookup of the post-NAT destination IP address.

In the following example of a one-to-one destination NAT mapping, users from the zone named untrust-l3 access the server 10.1.1.100 in the zone named dmz-l3 using the IP address 1.1.1.100.



Before configuring the NAT rules, consider the sequence of events for this scenario.

- Host 1.1.1.250 sends an ARP request for the address 1.1.1.100 (the public address of the destination server).

- The firewall receives the ARP request packet for destination 1.1.1.100 on the Ethernet1/1 interface and processes the request. The firewall responds to the ARP request with its own MAC address because of the destination NAT rule configured.
- The NAT rules are evaluated for a match. For the destination IP address to be translated, a destination NAT rule from zone untrust-l3 to zone untrust-l3 must be created to translate the destination IP of 1.1.1.100 to 10.1.1.100.
- After determining the translated address, the firewall performs a route lookup for destination 10.1.1.100 to determine the egress interface. In this example, the egress interface is Ethernet1/2 in zone dmz-l3.
- The firewall performs a security policy lookup to see if the traffic is permitted from zone untrust-l3 to dmz-l3.

The direction of the policy matches the ingress zone and the zone where the server is physically located.



The security policy refers to the IP address in the original packet, which has a destination address of 1.1.1.100.



- The firewall forwards the packet to the server out egress interface Ethernet1/2. The destination address is changed to 10.1.1.100 as the packet leaves the firewall.

For this example, the following address objects are configured:

Name	Location	Type	Address	Tags
webserver-private		IP Netmask	10.1.1.100	
Webserver-public		IP Netmask	1.1.1.100	

The configured NAT rule would look like this:

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Dst NAT-webser	untrust-l3	untrust-l3	none	any	Webserver-public	any	none	address: webserver-private

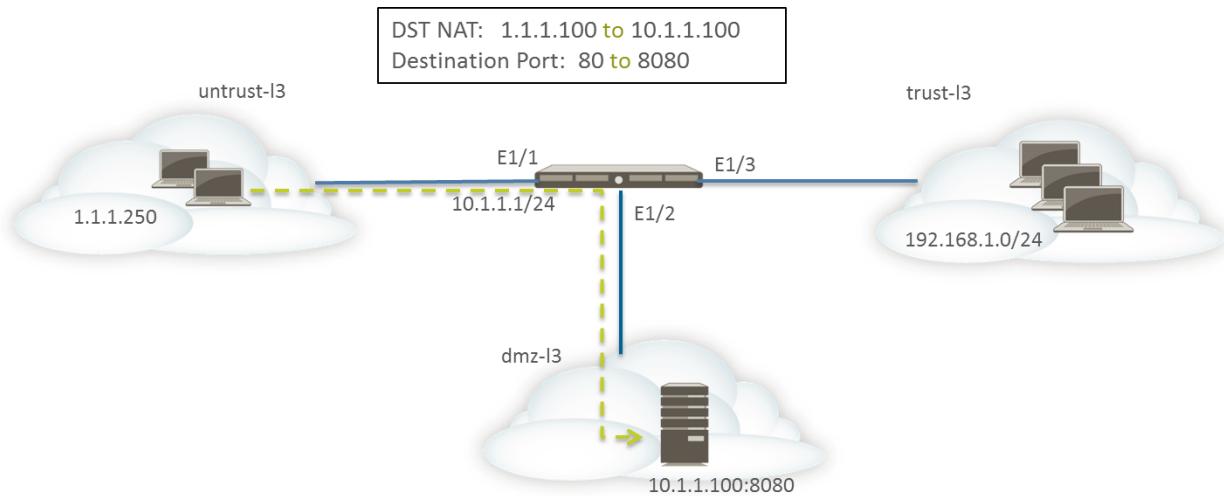
The direction of the NAT rules is based on the result of route lookup.

The configured security policy to provide access to the server from the untrust-l3 zone would look like this:

Name	Source		Destination			Application	Service	Action	Profile	Options
	Zone	Address	Zone	Address	Application					
Webserver acces	untrust-l3	any	dmz-l3	Webserver-pub	web-browsing	any		✓	none	

## Destination NAT with Port Translation Example

In this example, the web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 and TCP Port 80. The destination NAT rule is configured to translate both IP address and port to 10.1.1.100 and TCP port 8080.



The following NAT and security rules must be configured on the firewall:

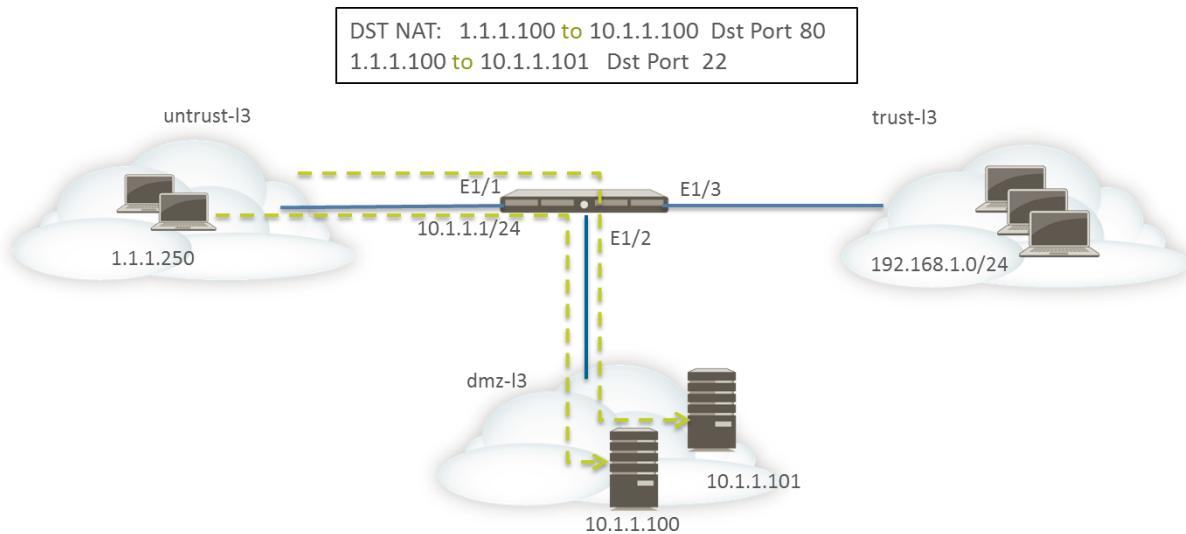
Name	Original Packet							Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
Dst NAT-webserv	untrust-I3	untrust-I3	none	any	Servers-public	service-http	none	address: webserver-private port: 8080	

Name	Source		Destination			Application	Service
	Zone	Address	Zone	Address	Application		
Webserver access	untrust-I3	any	dmz-I3	Servers-public	web-browsing	any	

Use the `show session all` CLI command to verify the translation.

## Destination NAT Example—One-to-Many Mapping

In this example, one IP address maps to two different internal hosts. The firewall uses the application to identify the internal host to which the firewall forwards the traffic.



All HTTP traffic is sent to host 10.1.1.100 and SSH traffic is sent to server 10.1.1.101. The following address objects are required:

- Address object for the one pre-translated IP address of the server
- Address object for the real IP address of the SSH server
- Address object for the real IP address of the web server

The configured address objects would look like this:

	Name	Type	Address
■	Servers-public	IP Netmask	1.1.1.100
■	SSH-server	IP Netmask	10.1.1.101
■	webserver-private	IP Netmask	10.1.1.100

The NAT rules would look like this:

Name	Original Packet						Translated Packet	
	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
Dst NAT-webserv	untrust-I3	untrust-I3	none	any	Servers-public	service-http	none	address: webserver-private
Dst NAT-SSH	untrust-I3	untrust-I3	none	any	Servers-public	custom-ssh	none	address: SSH-server

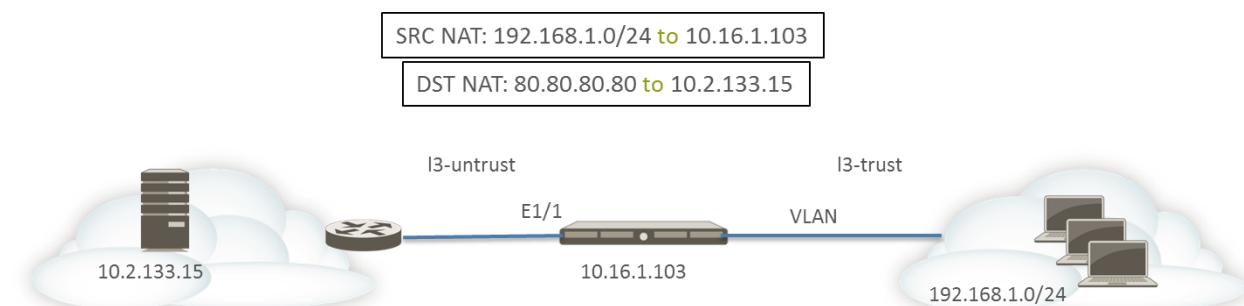
The security rules would look like this:

Name	Source		Destination		Application	Service	Action
	Zone	Address	Zone	Address			
Webserver access	untrust-I3	any	dmz-I3	Servers-public	web-browsing	application-default	✓
SSH access	untrust-I3	any	dmz-I3	Servers-public	ssh	application-default	✓

## Source and Destination NAT Example

In this example, NAT rules translate both the source and destination IP address of packets between the clients and the server.

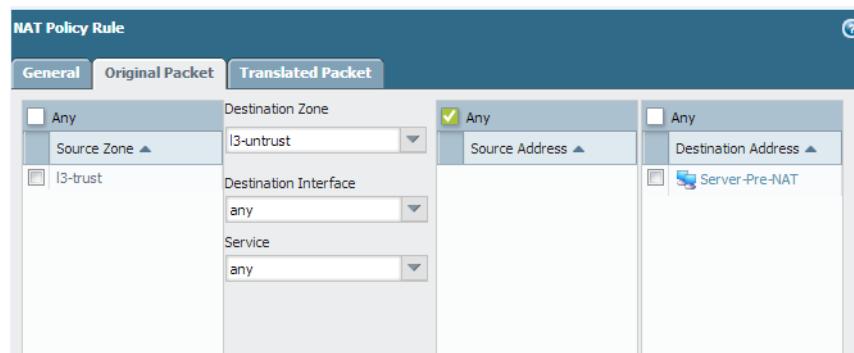
- Source NAT—The source addresses in the packets from the clients in the I3-trust zone to the server in the I3-untrust zone are translated from the private addresses in the network 192.168.1.0/24 to the IP address of the egress interface on the firewall (10.16.1.103). Dynamic IP and Port translation causes the port numbers to be translated also.
- Destination NAT—The destination addresses in the packets from the clients to the server are translated from the server's public address (80.80.80.80) to the server's private address (10.2.133.15).

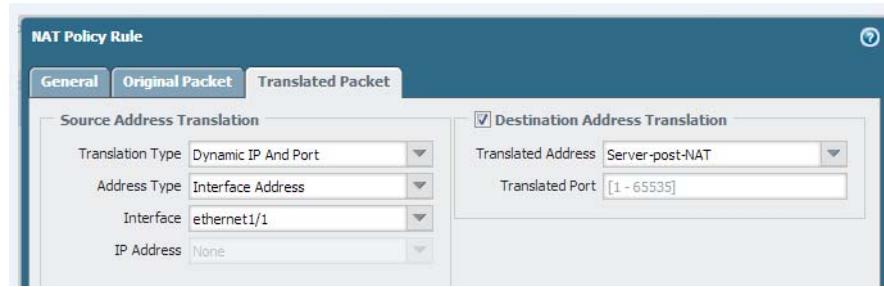


The following address objects are created for destination NAT.

- Server-Pre-NAT: 80.80.80.80
- Server-post-NAT: 10.2.133.15

The following screen shots illustrate how to configure the source and destination NAT policies for the example.





To verify the translations, use the CLI command `show session all filter destination 80.80.80.80`. Note that a client address 192.168.1.11 and its port number are translated to 10.16.1.103 and a port number. The destination address 80.80.80.80 is translated to 10.2.133.15.

## Virtual Wire Source NAT Example

Virtual wire deployment of a Palo Alto Networks firewall includes the benefit of providing security transparently to the end devices. It is possible to configure NAT for interfaces configured in a virtual wire. All of the NAT types are allowed: source NAT (Dynamic IP, Dynamic IP and Port, static) and destination NAT.

Because interfaces in a virtual wire do not have an IP address assigned, it is not possible to translate an IP address to an interface IP address. You must configure an IP address pool.

The firewall will not proxy ARP for NAT addresses. Ensure that routes are configured on the upstream and downstream devices. See [Proxy ARP for NAT Address Pools](#) for more explanation about proxy ARP.

Proper routing must be configured on the upstream and downstream routers in order for the packets to be translated in virtual wire mode.

In the source NAT and static NAT examples below, security policies (not shown) are configured from the virtual wire zone named `vw-trust` to the zone named `vw-untrust`.

In the following topology, two routers are configured to provide connectivity between subnets 1.1.1.0/24 and 3.1.1.0/24. The link between the routers is configured in subnet 2.1.1.0/30. Static routing is configured on both routers to establish connectivity between the networks. Before the firewall is deployed in the environment, the topology and the routing table for each router look like this:



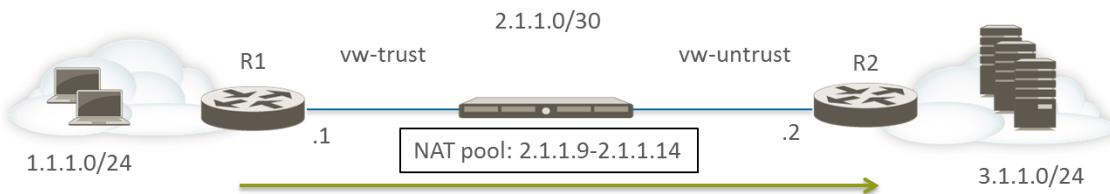
Route on R1:

Destination	Next Hop
3.1.1.0/24	2.1.1.2

Route on R2:

Destination	Next Hop
1.1.1.0/24	2.1.1.1

Now the firewall is deployed in virtual wire mode between the two Layer 3 devices. All communications from clients in network 1.1.1.0/24 accessing servers in network 3.1.1.0/24 are translated to an IP address in the range 2.1.1.9-2.1.1.14. A NAT IP address pool with range 2.1.1.9-2.1.1.14 is configured on the firewall.



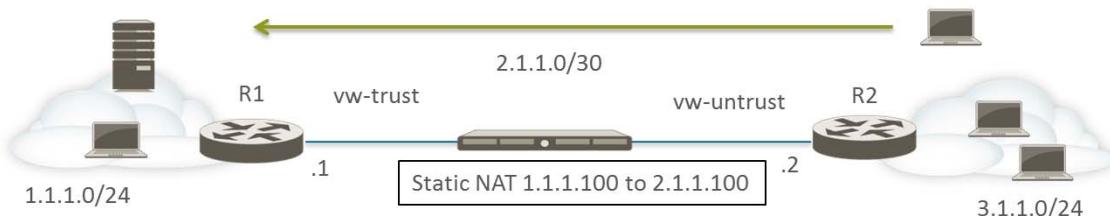
All connections from the clients in subnet 1.1.1.0/24 will arrive at router R2 with a translated source address in the range 2.1.1.9-2.1.1.14. The response from servers will be directed to these addresses. In order for source NAT to work, you must configure proper routing on router R2, so that packets destined for other addresses are not dropped. The routing table below shows the modified routing table on router R2. The route ensures the traffic to the destinations 2.1.1.9-2.1.1.14 (that is, hosts on subnet 2.1.1.8/29) will be sent back through the firewall to router R1.

Route on R2:

Destination	Next Hop
2.1.1.8/29	2.1.1.1

## Virtual Wire Static NAT Example

In this example, security policies are configured from the virtual wire zone named vw-trust to vw-untrust. Host 1.1.1.100 is statically translated to address 2.1.1.100. With the **Bi-directional** option enabled, the firewall generates a NAT policy from the vw-untrust zone to the vw-trust zone. Clients on the vw-untrust zone access the server using the IP address 2.1.1.100, which the firewall translates to 1.1.1.100. Any connections initiated by the server at 1.1.1.100 are translated to source IP address 2.1.1.100.



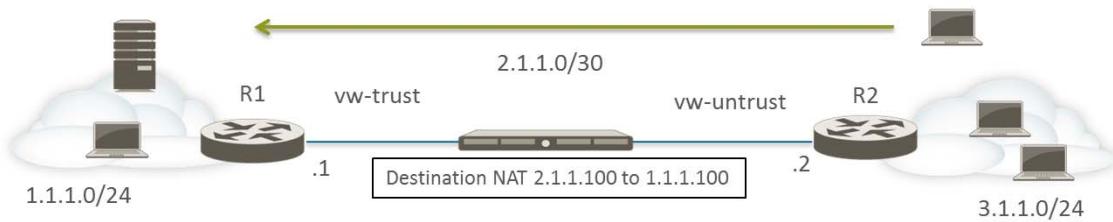
Route on R2:

Destination	Next Hop
2.1.1.100/32	2.1.1.1

Original Packet										Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
1	Static NAT	none	vw-trust	vw-untrust	any	webserver priv...	any	any	static-ip webserver public bi-directional: yes	none	

## Virtual Wire Destination NAT Example

Clients in the vw-untrust zone access the server using the IP address 2.1.1.100, which the firewall translates to 1.1.1.100. Both the NAT and security policies must be configured from the vw-untrust zone to the vw-trust zone.



Route on R2:

Destination	Next Hop
2.1.1.100/32	2.1.1.1

Original Packet										Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
1	DST NAT	none	vw-untrust	vw-trust	any	any	webserver public	any	none	address: webserver private	

## NPTv6

IPv6-to-IPv6 Network Prefix Translation (NPTv6) performs a stateless, static translation of one IPv6 prefix to another IPv6 prefix (port numbers are not changed). There are four primary benefits of NPTv6:

- You can prevent the asymmetrical routing problems that result from Provider Independent addresses being advertised from multiple datacenters.
- NPTv6 allows more specific routes to be advertised so that return traffic arrives at the same firewall that transmitted the traffic.
- Private and public addresses are independent; you can change one without affecting the other.
- You have the ability to translate [Unique Local Addresses](#) to globally routable addresses.

This topic builds on a basic understanding of NAT. You should be sure you are familiar with [NAT](#) concepts before configuring NPTv6.

- ▲ [NPTv6 Overview](#)
- ▲ [How NPTv6 Works](#)
- ▲ [NDP Proxy](#)
- ▲ [NPTv6 and NDP Proxy Example](#)
- ▲ [Create an NPTv6 Policy](#)

## NPTv6 Overview

This section describes [IPv6-to-IPv6 Network Prefix Translation](#) (NPTv6) and how to configure it. NPTv6 is defined in [RFC 6296](#). Palo Alto Networks does not implement all functionality defined in the RFC, but is compliant with the RFC in the functionality it has implemented.

NPTv6 performs stateless translation of one IPv6 prefix to another IPv6 prefix. It is stateless, meaning that it does not keep track of ports or sessions on the addresses translated. NPTv6 differs from NAT66, which is stateful. Palo Alto Networks supports [NPTv6 RFC 6296](#) prefix translation; it does not support NAT66.

With the limited addresses in the IPv4 space, [NAT](#) was required to translate private, non-routable IPv4 addresses to one or more globally-routable IPv4 addresses.

For organizations using IPv6 addressing, there is no need to translate IPv6 addresses to IPv6 addresses due to the abundance of IPv6 addresses. However, there are [Reasons to Use NPTv6](#) to translate IPv6 prefixes at the firewall.

NPTv6 translates the prefix portion of an IPv6 address but not the host portion or the application port numbers. The host portion is simply copied, and therefore remains the same on either side of the firewall. The host portion also remains visible within the packet header.

- ▲ [NPTv6 Does Not Provide Security](#)
- ▲ [Platform Support for NPTv6](#)
- ▲ [Unique Local Addresses](#)
- ▲ [Reasons to Use NPTv6](#)

### [NPTv6 Does Not Provide Security](#)

It is important to understand that NPTv6 does not provide security. In general, stateless network address translation does not provide any security; it provides an address translation function. NPTv6 does not hide or translate port numbers. You must set up firewall security policies correctly in each direction to ensure that traffic is controlled as you intended.

### [Platform Support for NPTv6](#)

NPTv6 is supported on the following platforms (NPTv6 with hardware lookup but packets go through the CPU): PA-7000 Series, PA-5000 Series, PA-4000 Series, PA-3060 firewall, PA-3050 firewall, and PA-2000 Series. Platforms supported with no ability to have hardware perform a session look-up: PA-3020 firewall, PA 500 firewall, PA-200 firewall, and VM-Series.

### [Unique Local Addresses](#)

[RFC 4193, Unique Local IPv6 Unicast Addresses](#), defines unique local addresses (ULAs), which are IPv6 unicast addresses. They can be considered IPv6 equivalents of the private IPv4 addresses identified in [RFC 1918, Address Allocation for Private Internets](#), which cannot be routed globally.

A ULA is globally unique, but not expected to be globally routable. It is intended for local communications and to be routable in a limited area such as a site or among a small number of sites. Palo Alto Networks does not recommend that you assign ULAs, but a firewall configured with NPTv6 will translate prefixes sent to it, including ULAs.

## Reasons to Use NPTv6

Although there is no shortage of public, globally routable IPv6 addresses, there are reasons you might want to translate IPv6 addresses. NPTv6:

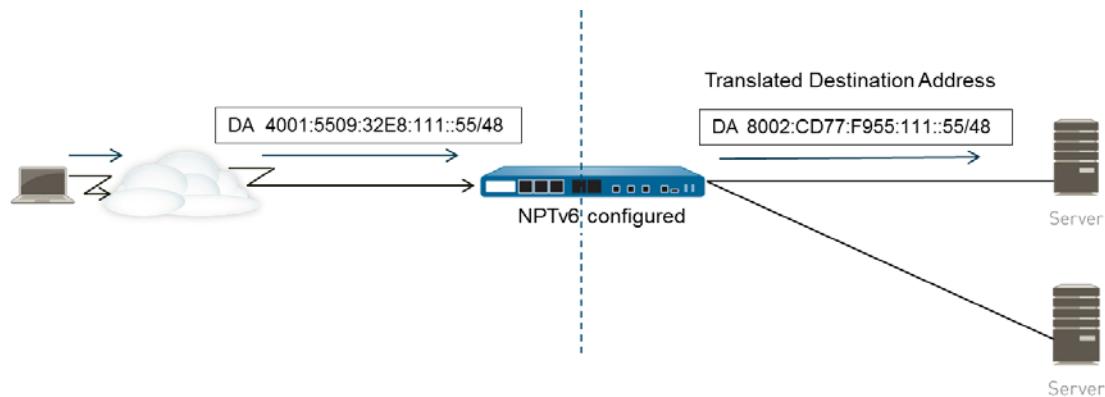
- **Prevents asymmetrical routing**—Asymmetric routing can occur if a Provider Independent address space (/48, for example) is advertised by multiple data centers to the global Internet. By using NPTv6, you can advertise more specific routes from regional firewalls, and the return traffic will arrive at the same firewall where the source IP address was translated by the translator.
- **Provides address independence**—You need not change the IPv6 prefixes used inside your local network if the global prefixes are changed (for example, by an ISP or as a result of merging organizations). Conversely, you can change the inside addresses at will without disrupting the addresses that are used to access services in the private network from the Internet. In either case, you update a NAT rule rather than reassign network addresses.
- **Translates ULAs for routing**—You can have [Unique Local Addresses](#) assigned within your private network, and have the firewall translate them to globally routable addresses. Thus, you have the convenience of private addressing and the functionality of translated, routable addresses.
- **Reduces exposure to IPv6 prefixes**—IPv6 prefixes are less exposed than if you didn't translate network prefixes, however, NPTv6 is not a security measure. The interface identifier portion of each IPv6 address is not translated; it remains the same on each side of the firewall and visible to anyone who can see the packet header. Additionally, the prefixes are not secure; they can be determined by others.

## How NPTv6 Works

When you configure a policy for NPTv6, the Palo Alto Networks firewall performs a static, one-to-one IPv6 translation in both directions. The translation is based on the algorithm described in [RFC 6296](#).

In one use case, the firewall performing NPTv6 is located between an internal network and an external network (such as the Internet) that uses globally routable prefixes. When datagrams are going in the outbound direction, the internal source prefix is replaced with the external prefix; this is known as source translation.

In another use case, when datagrams are going in the inbound direction, the destination prefix is replaced with the internal prefix (known as destination translation). The figure below illustrates destination translation and a characteristic of NPTv6: only the prefix portion of an IPv6 address is translated. The host portion of the address is not translated and remains the same on either side of the firewall. In the figure below, the host identifier is 111::55 on both sides of the firewall.



It is important to understand that NPTv6 does not provide security. While you are planning your NPTv6 NAT policies, remember also to configure security policies in each direction.

A NAT or NPTv6 policy rule cannot have both the Source Address and the Translated Address set to Any.

In an environment where you want IPv6 prefix translation, three firewall features work together: NPTv6 NAT policies, security policies, and [NDP Proxy](#).

The firewall does not translate the following:

- Addresses that the firewall has in its Neighbor Discovery (ND) cache.
- The subnet 0xFFFF (in accordance with [RFC 6296](#), Appendix B).
- IP multicast addresses.
- IPv6 addresses with a prefix length of /31 or shorter.
- Link-local addresses. If the firewall is operating in virtual wire mode, there are no IP addresses to translate, and the firewall does not translate link-local addresses.
- Addresses for TCP sessions that authenticate peers using the TCP Authentication Option (RFC 5925).

When using NPTv6, performance for fast path traffic is impacted because NPTv6 is performed in the slow path.

NPTv6 will work with IPSec IPv6 only if the firewall is originating and terminating the tunnel. Transit IPSec traffic would fail because the source and/or destination IPv6 address would be modified. A NAT traversal technique that encapsulates the packet would allow IPSec IPv6 to work with NPTv6.

- ▲ [Checksum-Neutral Mapping](#)
- ▲ [Bi-Directional Translation](#)
- ▲ [NPTv6 Applied to a Specific Service](#)

## Checksum-Neutral Mapping

The NPTv6 mapping translations that the firewall performs are checksum-neutral, meaning that “... they result in IP headers that will generate the same IPv6 pseudo-header checksum when the checksum is calculated using the standard Internet checksum algorithm [RFC 1071].” See [RFC 6296](#), Section 2.6, for more information about checksum-neutral mapping.

If you are using NPTv6 to perform destination NAT, you can provide the internal IPv6 address and the external prefix/prefix length of the firewall interface in the syntax of the `test nptv6` CLI command. The CLI responds with the checksum-neutral, public IPv6 address to use in your NPTv6 configuration to reach that destination.

## Bi-Directional Translation

When you [Create an NPTv6 Policy](#), the **Bi-directional** check box in the **Translated Packet** tab provides a convenient way for you to have the firewall create a corresponding NAT or NPTv6 translation in the opposite direction of the translation you configured. By default, **Bi-directional** translation is disabled.



If you enable **Bi-directional** translation, it is very important to make sure you have security policies in place to control the traffic in both directions. Without such policies, the **Bi-directional** feature will allow packets to be automatically translated in both directions, which you might not want.

## NPTv6 Applied to a Specific Service

The Palo Alto Networks implementation of NPTv6 offers the ability to filter packets to limit which packets are subject to translation. Keep in mind that NPTv6 does not perform port translation. There is no concept of Dynamic IP and Port (DIPP) translation because NPTv6 translates IPv6 prefixes only. However, you can specify that only packets for a certain service port undergo NPTv6 translation. To do so, [Create an NPTv6 Policy](#) that specifies a **Service** in the Original Packet.

## NDP Proxy

Neighbor Discovery Protocol (NDP) for IPv6 performs functions similar to those provided by Address Resolution Protocol (ARP) for IPv4. [RFC 4861](#) defines [Neighbor Discovery for IP version 6 \(IPv6\)](#). Hosts, routers, and firewalls use NDP to determine the link-layer addresses of neighbors on connected links, to keep track of which neighbors are reachable, and to update neighbors' link-layer addresses that have changed. Peers advertise their own MAC address and IPv6 address, and they also solicit addresses from peers.

NDP also supports the concept of *proxy*, when a node has a neighboring device that is able to forward packets on behalf of the node. The device (firewall) performs the role of NDP Proxy.

Palo Alto Networks firewalls support NDP and NDP Proxy on their interfaces. When you configure the firewall to act as an NDP Proxy for addresses, it allows the firewall to send Neighbor Discovery (ND) advertisements and respond to ND solicitations from peers that are asking for MAC addresses of IPv6 prefixes assigned to devices behind the firewall. You can also configure addresses for which the firewall will not respond to proxy requests (negated addresses).

In fact, NDP is enabled by default, and you need to configure NDP Proxy when you configure NPTv6, for the following reasons:

- The stateless nature of NPTv6 requires a way to instruct the firewall to respond to ND packets sent to specified NDP Proxy addresses, and to not respond to negated NDP Proxy addresses.



It is recommended that you negate your neighbors' addresses in the NDP Proxy configuration, because NDP Proxy indicates the firewall will reach those addresses behind the firewall, but the neighbors are not behind the firewall.

- NDP causes the firewall to save the MAC addresses and IPv6 addresses of neighbors in its ND cache. (Refer to the figure in [NPTv6 and NDP Proxy Example](#).) The firewall does not perform NPTv6 translation for addresses that it finds in its ND cache because doing so could introduce a conflict. If the host portion of an address in the cache happens to overlap with the host portion of a neighbor's address, and the prefix in the cache is translated to the same prefix as that of the neighbor (because the egress interface on the firewall belongs to the same subnet as the neighbor), then you would have a translated address that is exactly the same as the legitimate IPv6 address of the neighbor, and a conflict occurs. (If an attempt to perform NPTv6 translation occurs on an address in the ND cache, an informational syslog message logs the event: **NPTv6 Translation Failed**.)

When an interface with NDP Proxy enabled receives an ND solicitation requesting a MAC address for an IPv6 address, the following sequence occurs:

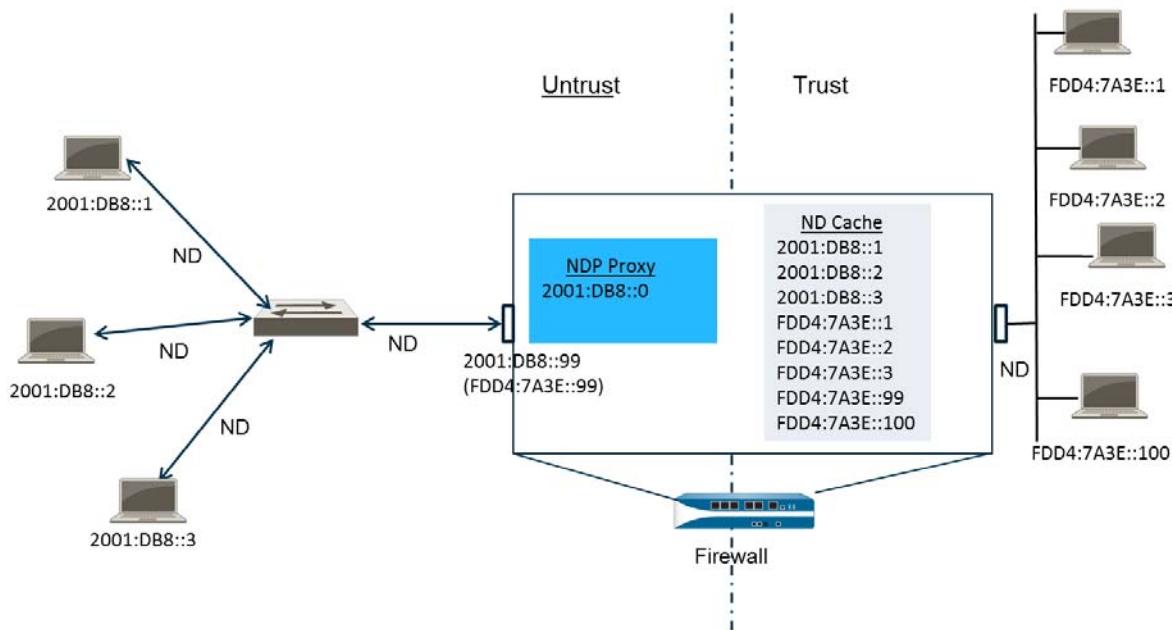
- The firewall searches the ND cache to ensure the IPv6 address from the solicitation is not there. If the address is there, the firewall ignores the ND solicitation.
- If the source IPv6 address is 0, that means the packet is a Duplicate Address Detection packet, and the firewall ignores the ND solicitation.
- The firewall does a Longest Prefix Match search of the NDP Proxy addresses and finds the best match to the address in the solicitation. If the Negate field for the match is checked (in the NDP Proxy list), the firewall drops the ND solicitation.
- Only if the Longest Prefix Match search matches, and that matched address is not negated, will the NDP Proxy respond to the ND solicitation. The firewall responds with an ND packet, providing its own MAC address as the MAC address of the next hop toward the queried destination.

In order to successfully support NDP, the firewall does not perform NDP Proxy for the following:

- Duplicate Address Detection (DAD).
- Addresses in the ND cache (because such addresses do not belong to the firewall; they belong to discovered neighbors).

## NPTv6 and NDP Proxy Example

The following figure and text illustrate how NPTv6 and NDP Proxy function together.



### The ND Cache in NPTv6 Example

In the above example, multiple peers connect to the firewall through a switch, with ND occurring between the peers and the switch, between the switch and the firewall, and between the firewall and the devices on the trust side.

As the firewall learns of peers, it saves their addresses to its ND cache. Trusted peers FDDA:7A3E::1, FDDA:7A3E::2, and FDDA:7A3E::3 are connected to the firewall on the trust side. FDDA:7A3E::99 is the untranslated address of the firewall itself; its public-facing address is 2001:DB8::99. The addresses of the peers on the untrust side have been discovered and appear in the ND cache: 2001:DB8::1, 2001:DB8::2, and 2001:DB8::3.

### The NDP Proxy in NPTv6 Example

In our scenario, we want the firewall to act as NDP Proxy for the prefixes on devices behind the firewall. When the firewall is NDP Proxy for a specified set of addresses/ranges/prefixes, and it sees an address from this range in an ND solicitation or advertisement, the firewall will respond as long as a device with that specific address doesn't respond first, the address is not negated in the NDP proxy configuration, and the address is not in the ND cache. The firewall does the prefix translation (described below) and sends the packet to the trust side, where that address might or might not be assigned to a device.

In this example, the ND Proxy table contains the network address 2001:DB8::0. When the interface sees an ND for 2001:DB8::100, no other devices on the L2 switch claim the packet, so the proxy range causes the firewall to claim it, and after translation to FDD4:7A3E::100, the firewall sends it out to the trust side.

## The NPTv6 Translation in NPTv6 Example

In this example, the **Original Packet** is configured with a **Source Address** of FDD4:7A3E::0 and a **Destination of Any**. The **Translated Packet** is configured with the **Translated Address** of 2001:DB8::0.

Therefore, outgoing packets with a source of FDD4:7A3E::0 are translated to 2001:DB8::0. Incoming packets with a destination prefix in the network 2001:DB8::0 are translated to FDD4:7A3E::0.

## Neighbors in the ND Cache are Not Translated

In our example, there are hosts behind the firewall with host identifiers :1, :2, and :3. If the prefixes of those hosts are translated to a prefix that exists beyond the firewall, and if those devices also have host identifiers :1, :2, and :3, because the host identifier portion of the address remains unchanged, the resulting translated address would belong to the existing device, and an addressing conflict would result. In order to avoid a conflict with overlapping host identifiers, NPTv6 does not translate addresses that it finds in its ND cache.

## Create an NPTv6 Policy

Perform this task when you want to configure a NAT NPTv6 policy to translate one IPv6 prefix to another IPv6 prefix. The prerequisites for this task are:

- Enable IPv6. Select **Device > Setup > Session**. Click **Edit** and select **IPv6 Firewalling**.
- Configure a Layer 3 Ethernet interface with a valid IPv6 address and with IPv6 enabled. Select **Network > Interfaces > Ethernet**, select an interface, and on the **IPv6** tab, select **Enable IPv6 on the interface**.
- Create network security policies, because NPTv6 does not provide security.
- Decide whether you want source translation, destination translation, or both.
- Identify the zones to which you want to apply the NPTv6 policy.
- Identify your original and translated IPv6 prefixes.

Configure an NPTv6 Policy	
<b>Step 1</b> Create a new NPTv6 policy.	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; NAT</b> and click <b>Add</b>.</li> <li>2. On the <b>General</b> tab, enter a descriptive <b>Name</b> for the NPTv6 policy rule.</li> <li>3. (Optional) Enter a <b>Description</b> and <b>Tag</b>.</li> <li>4. For <b>NAT Type</b>, select <b>NPTv6</b>.</li> </ol>
<b>Step 2</b> Specify the match criteria for incoming packets; packets that match all of the criteria are subject to the NPTv6 translation.  Zones are required for both types of translation.	<ol style="list-style-type: none"> <li>1. On the <b>Original Packet</b> tab, for <b>Source Zone</b>, leave <b>Any</b> or click <b>Add</b> to enter the source zone to which the policy applies.</li> <li>2. Enter the <b>Destination Zone</b> to which the policy applies.</li> <li>3. (Optional) Select a <b>Destination Interface</b>.</li> <li>4. (Optional) Select a <b>Service</b> to restrict what type of packets are translated.</li> <li>5. If you are doing source translation, enter a <b>Source Address</b> or select <b>Any</b>. The address could be an address object. The following constraints apply to <b>Source Address</b> and <b>Destination Address</b>: <ul style="list-style-type: none"> <li>• Prefixes of <b>Source Address</b> and <b>Destination Address</b> for the <b>Original Packet</b> and <b>Translated Packet</b> must be in the format xxxx:xxxx::/yy, although leading zeros in the prefix can be dropped.</li> <li>• The IPv6 address cannot have an interface identifier (host) portion defined.</li> <li>• The range of supported prefix lengths is /32 to /64.</li> <li>• The <b>Source Address</b> and <b>Destination Address</b> cannot both be set to <b>Any</b>.</li> </ul> </li> <li>6. If you are doing source translation, you can optionally enter a <b>Destination Address</b>. If you are doing destination translation, the <b>Destination Address</b> is required. See the constraints listed in the prior step.</li> </ol>

### Configure an NPTv6 Policy (Continued)

<p><b>Step 3</b> Specify the translated packet.</p>	<ol style="list-style-type: none"> <li>1. On the <b>Translated Packet</b> tab, if you want to do source translation, in the Source Address Translation section, for <b>Translation Type</b>, select <b>Static IP</b>. If you do not want to do source translation, select <b>None</b>.</li> <li>2. If you chose <b>Static IP</b>, the <b>Translated Address</b> field appears. Enter the translated IPv6 prefix or address object. See the constraints listed in <a href="#">Step 5</a>.       <p> It is a best practice to configure your <b>Translated Address</b> to be the prefix of the untrust interface address of your firewall. For example, if your untrust interface has the address 2001:1a:1b:1:99/64, make your <b>Translated Address</b> 2001:1a:1b:1::0/64.</p> </li> <li>3. (Optional) Select <b>Bi-directional</b> if you want the firewall to create a corresponding NPTv6 translation in the opposite direction of the translation you configured.       <p> If you enable <b>Bi-directional</b> translation, it is very important to make sure you have security policies in place to control the traffic in both directions. Without such policies, the <b>Bi-directional</b> feature will allow packets to be automatically translated in both directions, which you might not want.</p> </li> <li>4. If you want to do destination translation, select <b>Destination Address Translation</b>. In the <b>Translated Address</b> field, choose an address object from the drop-down or enter your internal destination address.</li> <li>5. Click <b>OK</b>.</li> </ol>
<p><b>Step 4</b> Configure NDP Proxy.</p> <p>When you configure the firewall to act as an NDP Proxy for addresses, it allows the firewall to send Neighbor Discovery (ND) advertisements and respond to ND solicitations from peers that are asking for MAC addresses of IPv6 prefixes assigned to devices behind the firewall.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and select an interface.</li> <li>2. On the <b>Advanced &gt; NDP Proxy</b> tab, select <b>Enable NDP Proxy</b> and click <b>Add</b>.</li> <li>3. Enter the <b>IP Address(es)</b> for which NDP Proxy is enabled. It can be an address, a range of addresses, or a prefix and prefix length. The order of IP addresses does not matter. These addresses are ideally the same as the Translated Addresses that you configured in an NPTv6 policy.       <p> If the address is a subnet, the NDP Proxy will respond to all addresses in the subnet, so you should list the neighbors in that subnet with <b>Negate</b> selected, as described in the next step.</p> </li> <li>4. (Optional) Enter one or more addresses for which you do not want NDP Proxy enabled, and select <b>Negate</b>. For example, from an IP address range or prefix range configured in the prior step, you could negate a smaller subset of addresses. It is recommended that you negate the addresses of the neighbors of the firewall.</li> </ol>
<p><b>Step 5</b> Save the configuration.</p>	<p>Click <b>OK</b> and <b>Commit</b>.</p>

# LACP

The firewall can now use Link Aggregation Control Protocol (LACP) to detect the physical interfaces between itself and a connected device (peer) and manage those interfaces as a single virtual interface (aggregate group). An aggregate group increases the bandwidth between peers. Enabling LACP provides redundancy within the group: the protocol automatically detects interface failures and performs failover to standby interfaces. Without LACP, you must manually identify interface failures occurring at layers above the physical or occurring between peers that are not directly connected.

The following Palo Alto Networks firewalls support LACP: PA-500, PA-3000 Series, PA-4000 Series, PA-5000 Series, and PA-7000 Series. The firewalls support LACP for HA3 (only on the PA-500, PA-3000 Series, PA-4000 Series, and PA-5000 Series), Layer 2, and Layer 3 interfaces.

The following topics describe LACP and how to configure it for aggregate groups:

- ▲ [LACP Settings](#)
- ▲ [Configure LACP](#)

## LACP Settings

To implement LACP, you must configure an aggregate group on each LACP peer that will use the protocol. Before you [Configure LACP](#), determine the optimal settings for each peer, as described in the following topics:

- ▲ [Mode](#)
- ▲ [Transmission Rate](#)
- ▲ [Fast Failover](#)
- ▲ [Port Priority and System Priority](#)

### Mode

In LACP active mode, a device actively searches the network for peers and queries their status (available or unresponsive). In passive mode, a device only responds to queries from an active peer. Between any two peers, it is recommended that one be active and the other passive. LACP cannot function if both peers are passive.

### Transmission Rate

You can configure a device to detect the state (available or unresponsive) of peers and individual interfaces at fast (every second) or slow (every 30 seconds) intervals. When the device does not receive an LACP update from the peer within a period that is three times the transmission rate (3 seconds or 90 seconds), it flags the peer as unresponsive. Therefore, set the transmission rate according to how much LACP processing your network can support and how quickly a device should detect and resolve interface failures.

For example, in a network where peers have many redundant links, a single interface failure would not disrupt traffic. In this case, a slow rate would suffice for detecting failures and would avoid the extra processing associated with the fast rate. If the network can support the extra processing and requires high availability (for example, datacenters supporting critical business operations), a fast transmission rate would enable the firewall to substitute failed interfaces quicker.



If devices have different transmission rates, each uses the rate of its peer.

## Fast Failover

When an interface goes down, it fails over to a standby interface. The IEEE 802.1ax standard that defines LACP specifies a failover process that takes at least three seconds. For networks that require quicker failover, the firewall provides an option that performs fast failover within one second. This option is recommended for deployments in which critical data might be lost during the standard failover interval. For example, if the amount of traffic between peers is close to the maximum that the active interfaces can support and one interface fails, the risk of data being lost while a standby interface becomes active is significantly less for fast failover than for standard failover.



Because both peers perform failover when an interface goes down, it is recommended that you configure fast failover on both so that they complete the process within the same time frame.

## Port Priority and System Priority

When you configure an aggregate group, the **Max Ports** parameter determines how many interfaces can be active at any given time. If the number of interfaces you assign to the group exceeds the **Max Ports**, the remaining interfaces are in standby mode. If an active interface fails, a standby interface becomes active. LACP uses the **LACP Port Priority** assigned to each interface to determine which interfaces are initially active and to determine the order in which standby interfaces become active upon failover. (You set port priorities when configuring individual interfaces, not when configuring the aggregate group.)

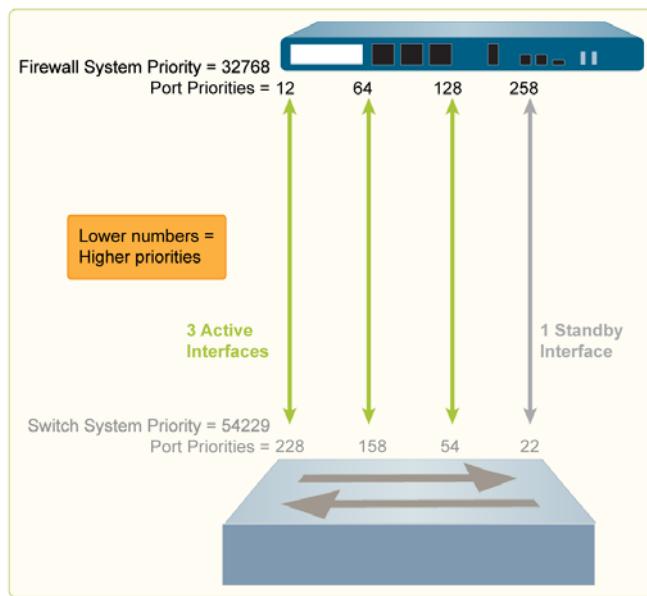


It is recommended that you assign a unique priority number to each interface in an aggregate group. However, if multiple interfaces have the same priority number, the interface with the lowest port number has the highest priority.

To enable LACP between two peers, each requires an aggregate group configuration. If the port priority values for the member interfaces differ in each peer, the values of the peer with the higher **System Priority** will override the other peer in determining active and standby interfaces.

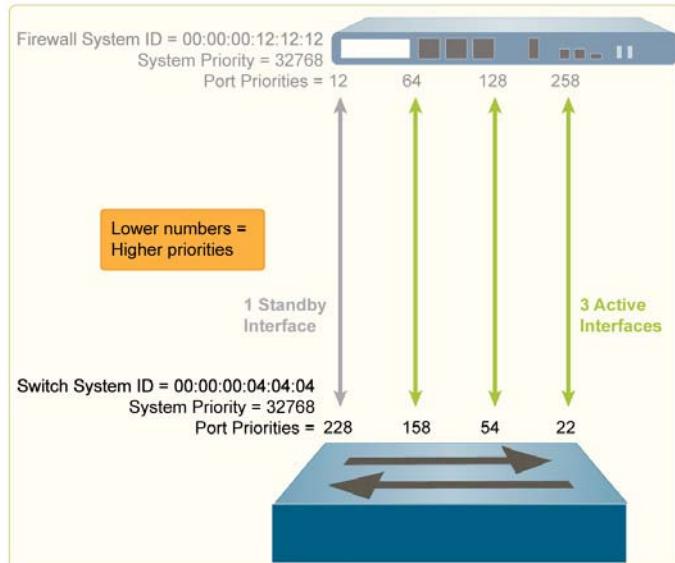
For port and system priorities, the priority level is the inverse of its numerical value: a priority of 1 designates the highest priority level; a value of 65535 designates the lowest priority level. The default is 32768.

The following figure shows an aggregate group instance configured on a firewall and on a switch. The group has four interfaces and the **Max Ports** parameter is set to three. That means three interfaces are active and one is standby. The firewall administrator assigned port priorities 12, 64, 128, and 258 to the interfaces. The switch administrator assigned port priorities 22, 54, 158, and 228 to the interfaces. LACP uses the port priorities of the firewall instance because the **System Priority** of the firewall is higher than that of the switch.

**Figure: LACP System Priority**

It is a best practice to assign a unique system priority to each peer. However, in some cases, peers might have the same value. This could happen if a different administrator configured the aggregate group on each peer. In such cases, the peer for which the *system ID* is a lower numerical value will override the other peer with respect to port priorities. LACP automatically derives the system ID from the system priority and system MAC address. A numerically lower MAC address produces a numerically lower system ID.

The following figure shows the same peers as in [Figure: LACP System Priority](#) but with identical system priorities. In this case, LACP uses the system IDs to determine port prioritization: the switch overrides the firewall.

**Figure: LACP System ID**

Firewalls in a high availability (HA) pair have the same system priority value. However, in an active/passive deployment, the system ID for each can be the same or different, depending on whether you assign the same MAC address. (Firewalls in an active/active deployment require unique MAC addresses so PAN-OS automatically assigns them.) When the LACP peers (also in HA mode) are virtualized (appearing to the network as a single device), selecting the **Same System MAC Address for Active-Passive HA** option for the firewalls is a best practice to minimize latency during failover. When the LACP peers are not virtualized, using the unique MAC address of each firewall is the best practice to minimize failover latency. In the latter case, if the HA firewall pair and the LACP peer devices all have the same system priority but each firewall in the HA pair has a unique system ID, one firewall might have a lower system ID than the LACP peers while the other firewall has a higher system ID than the LACP peers. In this case, when failover occurs on the firewalls, port prioritization switches between the LACP peers and the firewall that becomes active.

## Configure LACP

Before starting this procedure:

- Determine which physical interfaces connect the LACP peers. This procedure assumes the cabling is complete.
- Determine the optimal [LACP Settings](#) for the peers.



This procedure only covers the configuration steps for an LACP peer that is a Palo Alto Networks firewall. Other devices have proprietary methods for configuring LACP.

Perform the following steps to configure LACP on a firewall. In a high availability deployment, configure the primary (for active/active) or active (for active/passive) firewall; the secondary or passive firewall automatically synchronizes with it.

## Configure LACP

<p><b>Step 1</b> Add an aggregate group with LACP enabled.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and click <b>Add Aggregate Group</b>.</li><li>2. In the field adjacent to the read-only <b>Interface Name</b>, enter a number (1-8) to identify the group.</li><li>3. For the <b>Interface Type</b>, select <b>HA</b>, <b>Layer 2</b>, or <b>Layer 3</b>.  Only select <b>HA</b> if the interface is an HA3 link between two firewalls in an active/active deployment.</li><li>4. On the <b>LACP</b> tab, select <b>Enable LACP</b>.</li><li>5. For the <b>LACP Mode</b>, select whether the firewall is <b>Passive</b> (default) or <b>Active</b>.</li><li>6. For the <b>Transmission Rate</b>, select <b>Fast</b> or <b>Slow</b>.</li><li>7. If desired, select <b>Fast Failover</b> (under one second) for when interfaces go down. Otherwise, the standard failover (at least three seconds) applies.</li><li>8. Enter a <b>System Priority</b> number (1-65535, default 32768) that determines whether the firewall or peer overrides the other with respect to port priorities. Note that the lower the number, the higher the priority.</li><li>9. For the <b>Max Ports</b>, enter the number of interfaces (1-8) that are active. The value cannot exceed the number of interfaces you assign to the group. If the number of assigned interfaces exceeds the number of active interfaces, the remaining interfaces will be in standby mode.</li><li>10. By default, each firewall in an HA pair has a unique MAC address. A <b>Same System MAC Address for Active-Passive HA</b> configuration is recommended only when the LACP peers are virtualized (appearing to the network as a single device). In such cases, select the check box and select the system-generated <b>MAC Address</b>, or enter your own. You must verify the address is globally unique.  If the firewalls are not in active/passive HA mode, PAN-OS ignores your selections for these fields. Firewalls in an active/active deployment require unique MAC addresses so PAN-OS automatically assigns them. If the <b>Interface Type</b> is <b>HA</b>, these fields do not appear.</li><li>11. Click <b>OK</b>.</li></ol>
--	---

## Configure LACP (Continued)

<p><b>Step 2</b> Assign interfaces to the aggregate group.</p>	<p>Perform the following steps for each physical interface (1-8) that will belong to the aggregate group.</p> <p> During normal operations, assign more than one interface. You would only assign a single interface if a troubleshooting procedure requires it.</p> <ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces</b> and select the interface name. It must be the same type (HA, Layer 2, or Layer 3) as the aggregate group.</li> <li>2. Change the <b>Interface Type</b> to <b>Aggregate Ethernet</b>.</li> <li>3. Select the <b>Aggregate Group</b> you just defined.</li> <li>4. Select the <b>Link Speed</b>, <b>Link Duplex</b>, and <b>Link State</b>. It is a best practice to set the same link speed and duplex values for every interface in the group. For non-matching values, the commit operation displays a warning and PAN-OS defaults to the higher speed and full duplex.</li> <li>5. Enter an <b>LACP Port Priority</b> (1-65535, default 32768). If the number of interfaces you assign exceeds the <b>Max Ports</b> value you configured for the group, the port priorities determine which interfaces are active or standby. The lower the numeric value, the higher the priority.</li> <li>6. Click <b>OK</b> and <b>Commit</b>.</li> </ol>
<p><b>Step 3</b> Verify the status of the aggregate group.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b>.</li> <li>2. Verify that the Features column displays an LACP enabled icon for the aggregate group.</li> <li>3. Verify that the Link State column displays a green icon for the aggregate group, indicating that all member interfaces are up. If the icon is yellow, at least one member is down but not all. If the icon is red, all members are down.</li> <li>4. If the Link State icon for the aggregate group is yellow or red, select <b>Monitor &gt; Logs &gt; System</b> and review the logs for the LACP subtype to investigate the causes of the interface failures.</li> </ol>
<p><b>Step 4</b> (Optional) If you selected <b>HA</b> as the <b>Interface Type</b> for the aggregate group, enable forwarding of packets over the HA3 link.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; High Availability &gt; Active/Active Config</b> and edit the Packet Forwarding section.</li> <li>2. For the <b>HA3 Interface</b>, select the aggregate group you configured.</li> <li>3. Click <b>OK</b> and <b>Commit</b>.</li> </ol>

## ECMP

Equal Cost Multiple Path (ECMP) processing is a networking feature that enables the firewall to use up to four equal-cost routes to the same destination. Without this feature, if there are multiple equal-cost routes to the same destination, the virtual router chooses one of those routes from the routing table and adds it to its forwarding table; it will not use any of the other routes unless there is an outage in the chosen route.

Enabling ECMP functionality on a virtual router allows the firewall to have up to four equal-cost paths to a destination in its forwarding table, allowing the firewall to:

- Load balance flows (sessions) to the same destination over multiple equal-cost links.
- Efficiently use all available bandwidth on links to the same destination rather than leave some links unused.
- Dynamically shift traffic to another ECMP member to the same destination if a link fails, rather than having to wait for the routing protocol or RIB table to elect an alternative path/route. This can help reduce downtime when links fail.

The following sections describe ECMP and how to configure it.

- ▲ [ECMP Load-Balancing Algorithms](#)
- ▲ [ECMP Platform, Interface, and IP Routing Support](#)
- ▲ [HA Active/Active Failover Behavior with ECMP](#)
- ▲ [Configure ECMP on a Virtual Router](#)
- ▲ [Enable ECMP for Multiple BGP Autonomous Systems](#)
- ▲ [Verify ECMP](#)

## ECMP Load-Balancing Algorithms

Let's suppose the Routing Information Base (RIB) of the firewall has multiple equal-cost paths to a single destination. The maximum number of equal-cost paths defaults to 2. ECMP chooses the best two equal-cost paths from the RIB to copy to the Forwarding Information Base (FIB). ECMP then determines, based on the load-balancing method, which of the two paths in the FIB that the firewall will use for the destination during this session.

ECMP load balancing is done at the session level, not at the packet level—the start of a new session is when the firewall (ECMP) chooses an equal-cost path. The equal-cost paths to a single destination are considered ECMP path members or ECMP group members. ECMP determines which one of the multiple paths to a destination in the FIB to use for an ECMP flow, based on which load-balancing algorithm you set. A virtual router can use only one load-balancing algorithm.

Enabling, disabling, or changing ECMP on an existing virtual router causes the system to restart the virtual router, which might cause existing sessions to be terminated.



The four algorithm choices emphasize different priorities, as follows:

- **Hash-based algorithms prioritize session stickiness**—The **IP Modulo** and **IP Hash** algorithms use hashes based on information in the packet header, such as source and destination address. Because the header of each flow in a given session contains the same source and destination information, these options prioritize session *stickiness*. If you choose the **IP Hash** algorithm, you can optionally set a **Hash Seed** value to further randomize load balancing if you have a large number of sessions to the same destination and they're not being distributed evenly over the ECMP links.
- **Balanced algorithm prioritizes load balancing**—The **Balanced Round Robin** algorithm distributes incoming sessions equally across the links, favoring load balancing over session stickiness. (Round robin indicates a sequence in which the least recently chosen item is chosen.) In addition, if new routes are added or removed from an ECMP group (for example if a path in the group goes down), the virtual router will re-balance the sessions across links in the group. Additionally, if the flows in a session have to switch routes due to an outage, when the original route associated with the session becomes available again, the flows in the session will revert to the original route when the virtual router once again re-balances the load.
- **Weighted algorithm prioritizes link capacity and/or speed**—As an extension to the ECMP protocol standard, the Palo Alto Networks implementation provides for a **Weighted Round Robin** load-balancing option that takes into account differing link capacities and speeds on the egress interfaces of the firewall. With this option, you can assign **ECMP Weights** (range is 1-255; default is 100) to the interfaces based on link performance using factors such as link capacity, speed, and latency to ensure that loads are balanced to fully leverage the available links.

For example, suppose the firewall has redundant links to an ISP: ethernet1/1 (100 Mbps) and ethernet1/8 (200 Mbps). Although these are equal-cost paths, the link via ethernet1/8 provides greater bandwidth and therefore can handle a greater load than the ethernet1/1 link. Therefore, to ensure that the load-balancing functionality takes into account link capacity and speed, you might assign ethernet1/8 a weight of 200 and ethernet1/1 a weight of 100. The 2:1 weight ratio causes the virtual router to send twice as many sessions to ethernet1/8 as it sends to ethernet1/1. However, because the ECMP protocol is inherently session-based, when using the **Weighted Round Robin** algorithm, the firewall will be able to load balance across the ECMP links only on a best-effort basis.



Assign lower-speed or lower-capacity links with a lower weight. Assign higher-speed or higher-capacity links with a higher weight. In this manner, the firewall can distribute sessions based on these ratios, rather than overdrive a low-capacity link that is one of the equal-cost paths.

Keep in mind that ECMP weights are assigned to interfaces to determine load balancing (to influence which *equal-cost* path is chosen), not for route selection (a route choice from routes that could have different costs).

## ECMP Platform, Interface, and IP Routing Support

ECMP is supported on all Palo Alto Networks firewall platforms, with hardware forwarding support on the PA-7000 Series, PA-5000 Series, PA-3060 firewalls, and PA-3050 firewalls. PA-3020 firewalls, PA-500 firewalls, PA-200 firewalls, and VM-Series firewalls support ECMP through software only. Performance is affected for sessions that cannot be hardware offloaded.

ECMP is supported on Layer 3, Layer 3 subinterface, VLAN, tunnel, and Aggregated Ethernet interfaces.

ECMP can be configured for static routes and any of the dynamic routing protocols the firewall supports.

ECMP affects the route table capacity because the capacity is based on the number of paths, so an ECMP route with four paths will consume four entries of route table capacity. ECMP implementation might slightly decrease the route table capacity because more memory is being used by session-based tags to map traffic flows to particular interfaces.

ECMP has the following restrictions:

- PA-2000 Series firewalls and PA-4000 Series firewalls with ECMP enabled might not be able to offload sessions to hardware for forwarding. Packets matching ECMP routes will be sent to software, while packets matching non-ECMP routes can still be forwarded by hardware.
- For the PA-4000 Series firewalls, packets to be forwarded by ECMP routes will be sent to software for route lookup and forwarding, even though the session is in offloaded state.
- Virtual router-to-virtual router routing using static routes does not support ECMP.

## HA Active/Active Failover Behavior with ECMP

In the event of a failover in a high availability (HA) active/active configuration, the sessions on the failed peer are transferred to the HA peer. When this happens, the new active primary device tries to use the same egress interface that the former failed active/active device was using. If such interface is found among the ECMP paths, the transferred sessions will take the same egress interface and path. This behavior takes place regardless of the ECMP algorithm in use; using the same interface is desirable.

Only if no ECMP path matches the original egress interface will the active-primary select a new ECMP path.

In an HA active/active configuration, if you did not configure the same interfaces on both peers, when a failover occurs, the active-primary will select the next best path from the FIB table. In this scenario, the existing sessions might not be distributed according to the ECMP algorithm.

## Configure ECMP on a Virtual Router

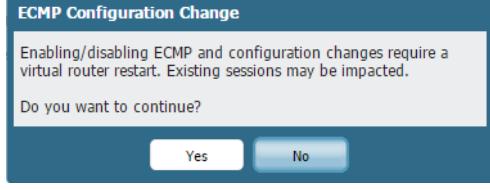
Use the following procedure to enable ECMP on a virtual router. The prerequisites are to:

- Specify the interfaces that belong to a virtual router (**Network > Virtual Routers > Router Settings > General**).
- Specify the IP routing protocol.

Enabling, disabling, or changing ECMP for an existing virtual router causes the system to restart the virtual router, which might cause sessions to be terminated.

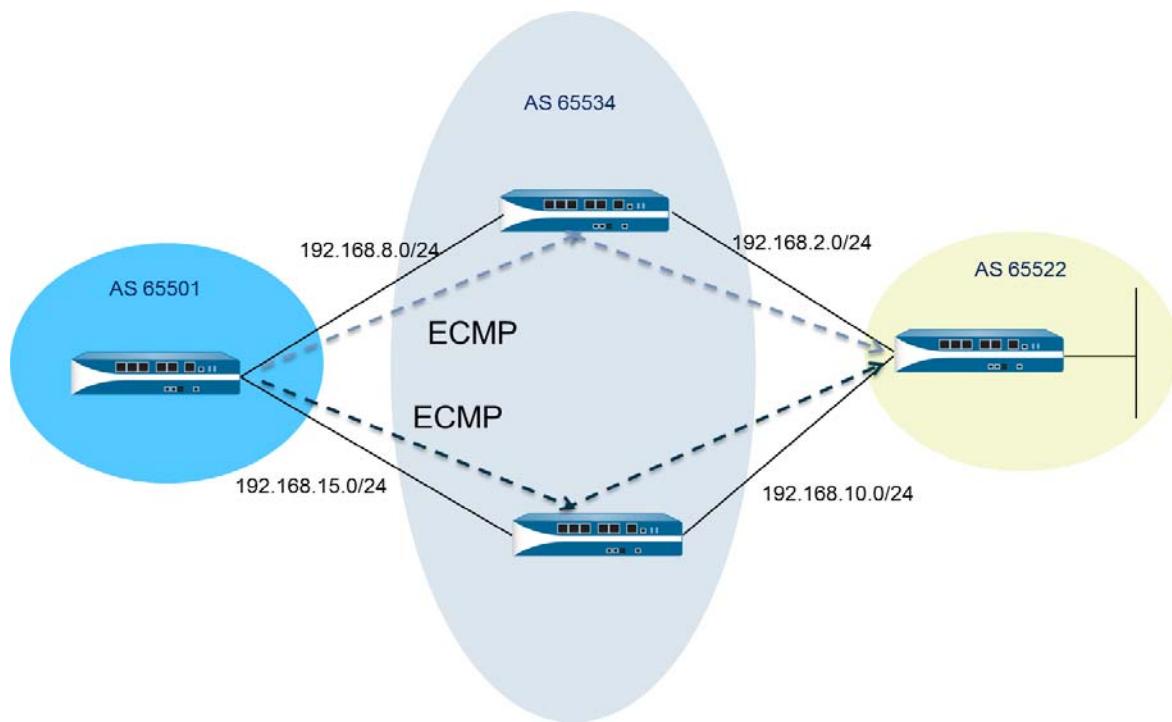
<b>Configure ECMP on a Virtual Router</b>	
<b>Step 1</b> Enable ECMP for a virtual router.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Virtual Routers</b> and select the virtual router on which to enable ECMP.</li><li>2. Select <b>Router Settings &gt; ECMP</b> and select the <b>Enable</b> check box.</li></ol>
<b>Step 2</b> (Optional) Enable symmetric return of packets from server to client.	(Optional) Select the <b>Symmetric Return</b> check box to cause return packets to egress out the same interface on which the associated ingress packets arrived. That is, the firewall will use the ingress interface on which to send return packets, rather than use the ECMP interface. The <b>Symmetric Return</b> setting overrides load balancing. This behavior occurs only for traffic flows from the server to the client.
<b>Step 3</b> Specify the maximum number of equal-cost paths (to a destination network) that can be copied from the Routing Information Base (RIB) to the Forwarding Information Base (FIB).	For <b>Max Path</b> allowed, enter <b>2</b> , <b>3</b> , or <b>4</b> . Default: 2.
<b>Step 4</b> Select the load-balancing algorithm for the virtual router. For more information on load-balancing methods and how they differ, see <a href="#">ECMP Load-Balancing Algorithms</a> .	For <b>Load Balance</b> , select one of the following options from the <b>Method</b> drop-down: <ul style="list-style-type: none"><li>• <b>IP Modulo</b> (default)—Uses a hash of the source and destination IP addresses in the packet header to determine which ECMP route to use.</li><li>• <b>IP Hash</b>—Uses a hash of the source and destination IP addresses and optionally the source and destination port numbers in the packet header to determine which ECMP route to use. Specify options in <a href="#">Step 5</a> below.</li><li>• <b>Balanced Round Robin</b>—Uses round robin among the ECMP paths and re-balances paths when the number of paths changes.</li><li>• <b>Weighted Round Robin</b>—Uses round robin and a relative weight to select from among ECMP paths. Specify the weights in <a href="#">Step 6</a> below.</li></ul>

### Configure ECMP on a Virtual Router (Continued)

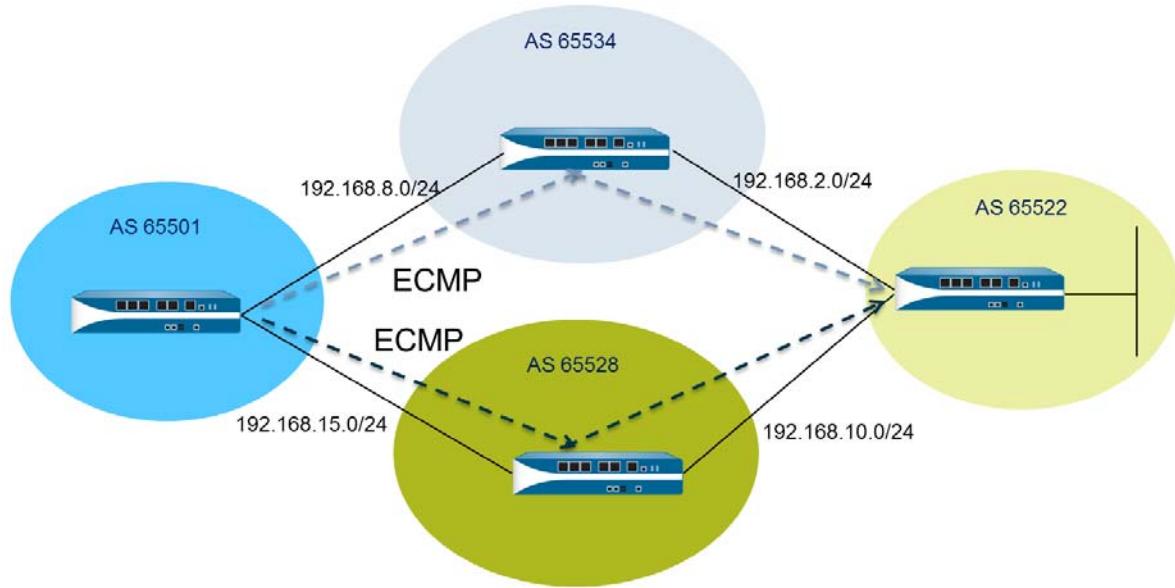
<p><b>Step 5</b> (Optional) (IP Hash only) Configure IP Hash options.</p>	<p>If you selected <b>IP Hash</b> as the <b>Method</b>:</p> <ol style="list-style-type: none"> <li>Check the <b>Use Source/Destination Ports</b> check box if you want to use source or destination port numbers in the <b>IP Hash</b> calculation.</li> <li>Enter a <b>Hash Seed</b> value (an integer with a maximum of 9 digits). Specify a <b>Hash Seed</b> value to further randomize load balancing. Specifying a hash seed value is useful if you have a large number of sessions with the same tuple information.</li> </ol>
<p><b>Step 6</b> (Weighted Round Robin only) Define a weight for each interface in the ECMP group.</p>	<p>If you selected <b>Weighted Round Robin</b> as the <b>Method</b>, define a weight for each of the interfaces that are the egress points for traffic to be routed to the same destinations (that is, interfaces that are part of an ECMP group, such as the interfaces that provide redundant links to your ISP or interfaces to the core business applications on your corporate network).</p> <p>The higher the weight, the more often that equal-cost path will be selected for a new session.</p> <p> A higher speed link should be given a higher weight than a slower link so that more of the ECMP traffic goes over the faster link.</p> <ol style="list-style-type: none"> <li>Create an ECMP group by clicking <b>Add</b> and selecting an <b>Interface</b> from the drop-down.</li> <li><b>Add</b> the other interfaces in the ECMP group.</li> <li>Click on <b>Weight</b> and specify the relative weight for each interface (range is 1-255; default is 100).</li> </ol>
<p><b>Step 7</b> Save the configuration.</p>	<ol style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Yes</b> to restart the virtual router. Restarting the virtual router might cause existing sessions to be terminated.</li> </ol>
	<p> This message displays only if you are modifying an existing virtual router with ECMP.</p>
<p><b>Step 8</b> Save the configuration.</p>	<p><b>Commit</b> the configuration.</p>

## Enable ECMP for Multiple BGP Autonomous Systems

Perform the following task if you have BGP configured, and you want to enable ECMP over multiple autonomous systems. This task presumes that BGP is already configured. In the following figure, two ECMP paths to a destination go through two firewalls belonging to a single ISP in a single BGP autonomous system.



In the following figure, two ECMP paths to a destination go through two firewalls belonging to two different ISPs in different BGP autonomous systems.



#### Enable ECMP for BGP Autonomous Systems

Step 1	Configure ECMP.	See <a href="#">Configure ECMP on a Virtual Router</a> .
Step 2	For BGP routing, enable ECMP over multiple autonomous systems.	<ol style="list-style-type: none"><li>Select <b>Network &gt; Virtual Routers</b> and select the virtual router on which to enable ECMP for multiple BGP autonomous systems.</li><li>Select <b>BGP &gt; Advanced</b> and select the <b>ECMP Multiple AS Support</b> check box.</li></ol>
Step 3	Save the configuration.	Click <b>OK</b> and <b>Commit</b> the configuration.

## Verify ECMP

A virtual router configured for ECMP indicates in the Forwarding Information Base (FIB) table which routes are ECMP routes. An ECMP flag (E) for a route indicates that it is participating in ECMP for the egress interface to the next hop for that route.

### Confirm That Routes Are Equal-Cost Multiple Paths

Look at the FIB and confirm that some routes are equal-cost multiple paths.

1. Select **Network > Virtual Routers**.
2. In the row of the virtual router for which you enabled ECMP, click **More Runtime Stats**.
3. Select **Routing > Forwarding Table** to see the FIB. In the table, note that multiple routes to the same Destination (out a different Interface) have the “E” flag.  
An asterisk “\*” denotes the preferred path for the ECMP group.

## LLDP

Palo Alto Networks firewalls support Link Layer Discovery Protocol (LLDP), which functions at the link layer to discover neighboring devices and their capabilities. LLDP allows the firewall and other network devices to send and receive LLDP data units (LLDPDUs) to and from neighbors. The receiving device stores the information in a MIB, which the Simple Network Management Protocol (SNMP) can access. LLDP makes troubleshooting easier, especially for virtual wire deployments where the firewall would typically go undetected by a ping or traceroute.

- ▲ [LLDP Overview](#)
- ▲ [Supported TLVs in LLDP](#)
- ▲ [LLDP Syslog Messages and SNMP Traps](#)
- ▲ [Configure LLDP](#)
- ▲ [View LLDP Settings and Status](#)
- ▲ [Clear LLDP Statistics](#)

## LLDP Overview

LLDP operates at Layer 2 of the OSI model, using MAC addresses. An LLDPDU is a sequence of type-length-value (TLV) elements encapsulated in an Ethernet frame. The IEEE 802.1AB standard defines three MAC addresses for LLDPDUs: 01-80-C2-00-00-0E, 01-80-C2-00-00-03, and 01-80-C2-00-00-00.

The Palo Alto Networks firewall supports only one MAC address for transmitting and receiving LLDP data units: 01-80-C2-00-00-0E. When transmitting, the firewall uses 01-80-C2-00-00-0E as the destination MAC address. When receiving, the firewall processes datagrams with 01-80-C2-00-00-0E as the destination MAC address. If the firewall receives either of the other two MAC addresses for LLDPDUs on its interfaces, the firewall takes the same forwarding action it took prior to this feature, as follows:

- If the interface type is vwire, the firewall forwards the datagram to the other port.
- If the interface type is L2, the firewall floods the datagram to the rest of the VLAN.
- If the interface type is L3, the firewall drops the datagrams.

The PA-2000 Series platform is not supported due to the hardware limitation of how Aggregated Ethernet interfaces function. Panorama, the GlobalProtect Mobile Security Manager, and the WildFire appliance are also not supported.

Interface types that do not support LLDP are TAP, high availability (HA), Decrypt Mirror, virtual wire/vlan/L3 subinterfaces, and PA-7000 Series Log Processing Card (LPC) interfaces.

An LLDP Ethernet frame has the following format:

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

Within the LLDP Ethernet frame, the TLV structure has the following format:

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

## Supported TLVs in LLDP

LLDPDUs include mandatory and optional TLVs. The following table lists the mandatory TLVs that the firewall supports:

### Mandatory TLVs in an LLDPDU Message

Mandatory TLVs	TLV Type	Description
Chassis ID TLV	1	Identifies the firewall chassis. Each firewall must have exactly one unique Chassis ID. The Chassis ID subtype is 4 (MAC address) on Palo Alto Networks platforms will use the MAC address of Eth0 to ensure uniqueness.
Port ID TLV	2	Identifies the port from which the LLDPDU is sent. Each firewall uses one Port ID for each LLDPDU message transmitted. The Port ID subtype is 5 (interface name) and uniquely identifies the transmitting port. The firewall uses the interface's ifname as the Port ID.
Time-to-live (TTL) TLV	3	Specifies how long (in seconds) LLDPDU information received from the peer is retained as valid in the local firewall (range is 0-65535). The value is a multiple of the LLDP Hold Time Multiplier. When the TTL value is 0, the information associated with the device is no longer valid and the firewall removes that entry from the MIB.
End of LLDPDU TLV	0	Indicates the end of the TLVs in the LLDP Ethernet frame.

The following table lists the optional TLVs that the Palo Alto Networks firewall supports:

### Optional TLVs in an LLDPDU Message

Optional TLVs	TLV Type	Purpose and Notes Regarding Firewall Implementation
Port Description TLV	4	Describes the port of the firewall in alpha-numeric format. The ifAlias object is used.
System Name TLV	5	Configured name of the firewall in alpha-numeric format. The sysName object is used.
System Description TLV	6	Describes the firewall in alpha-numeric format. The sysDescr object is used.
System Capabilities	7	Describes the deployment mode of the interface, as follows: <ul style="list-style-type: none"> <li>• An L3 interface is advertised with router (bit 6) capability and the “other” bit (bit 1).</li> <li>• An L2 interface is advertised with MAC Bridge (bit 3) capability and the “other” bit (bit 1).</li> <li>• A virtual wire interface is advertised with Repeater (bit 2) capability and the “other” bit (bit 1).</li> </ul>

**Optional TLVs in an LLDPDU Message (Continued)**

Optional TLVs	TLV Type	Purpose and Notes Regarding Firewall Implementation
Management Address	8	<p>One or more IP addresses used for the management of the device, as follows:</p> <ul style="list-style-type: none"> <li>• IP address of the management (MGT) interface</li> <li>• IPv4 and/or IPv6 address of the interface</li> <li>• Loopback address</li> <li>• User-defined address entered in the management address field</li> </ul> <p>If no management IP address is provided, the default is the MAC address of the transmitting interface.</p> <p>Included is the interface number of the management address specified. Also included is the OID of the hardware interface with the management address specified (if applicable).</p> <p>If more than one management address is specified, they will be sent in the order they are specified, starting at the top of the list. A maximum of four Management Addresses are supported.</p> <p>This is an optional parameter and can be left disabled.</p>

## LLDP Syslog Messages and SNMP Traps

The firewall stores LLDP information in MIBs, which an SNMP Manager can monitor. If you want the firewall to send SNMP trap notifications and syslog messages about LLDP events, you must enable **SNMP Syslog Notification** in an LLDP profile.

Per [RFC 5424, The Syslog Protocol](#), and [RFC 1157, A Simple Network Management Protocol](#), LLDP sends syslog and SNMP trap messages when MIB changes occur. These messages are rate-limited by the **Notification Interval**, an LLDP global setting that defaults to 5 seconds and is configurable.

Because the LLDP syslog and SNMP trap messages are rate-limited, some LLDP information provided to those processes might not match the current LLDP statistics seen when you [View the LLDP status information](#). This is normal, expected behavior.

A maximum of 5 MIBs can be received per interface (Ethernet or AE). Each different source has one MIB. If this limit is exceeded, the error message `tooManyNeighbors` is triggered.

## Configure LLDP

To configure LLDP, and create an LLDP profile, you must be a superuser or device administrator (deviceadmin). A firewall interface supports a maximum of five LLDP peers.

Configure LLDP	
Step 1	Enable LLDP on the firewall.
Step 2	(Optional) Change LLDP global settings.

- Select **Network > LLDP** and edit the LLDP General section; select the **Enable** check box.
1. For **Transmit Interval (sec)**, specify the interval (in seconds) at which LLDPDUs are transmitted. Default: 30 seconds. Range: 1-3600 seconds.
  2. For **Transmit Delay (sec)**, specify the delay time (in seconds) between LLDP transmissions sent after a change is made in a TLV element. The delay helps to prevent flooding the segment with LLDPDUs if many network changes spike the number of LLDP changes, or if the interface flaps. The **Transmit Delay** must be less than the **Transmit Interval**. Default: 2 seconds. Range: 1-600 seconds.
  3. For **Hold Time Multiple**, specify a value that is multiplied by the **Transmit Interval** to determine the total TTL Hold Time. Default: 4. Range: 1-100. The maximum TTL Hold Time is 65535 seconds, regardless of the multiplier value.
  4. For **Notification Interval**, specify the interval (in seconds) at which **LLDP Syslog Messages and SNMP Traps** are transmitted when MIB changes occur. Default: 5 seconds. Range: 1-3600 seconds.
  5. Click **OK**.

<b>Configure LLDP</b>	
<p><b>Step 3</b> Create an LLDP profile.</p> <p>For descriptions of the optional TLVs, see <a href="#">Supported TLVs in LLDP</a>.</p>	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Network Profiles &gt; LLDP Profile</b> and click <b>Add</b>.</li> <li>Enter a <b>Name</b> for the LLDP profile.</li> <li>For <b>Mode</b>, select <b>transmit-receive</b> (default), <b>transmit-only</b>, or <b>receive-only</b>.</li> <li>Click the <b>SNMP Syslog Notification</b> check box to enable SNMP notifications and syslog messages. If enabled, the global <b>Notification Interval</b> is used. The firewall will send both an SNMP trap and a syslog event as configured in the <b>Device &gt; Log Settings &gt; System &gt; SNMP Trap Profile</b> and <b>Syslog Profile</b>.</li> <li>For <a href="#">Optional TLVs</a>, select the TLVs you want transmitted: <ul style="list-style-type: none"> <li>• <b>Port Description</b></li> <li>• <b>System Name</b></li> <li>• <b>System Description</b></li> <li>• <b>System Capabilities</b></li> </ul> </li> <li>Specifying a <b>Management Address</b> is optional. To add one or more, select the check box and <b>Add a Name</b>.</li> <li>Select the <b>Interface</b> from which to obtain the management address. At least one management address is required if <b>Management Address</b> TLV is enabled. If no management IP address is configured, the system uses the MAC address of the transmitting interface as the management address TLV.</li> <li>Select <b>IPv4</b> or <b>IPv6</b>, and in the adjacent field, select an IP address from the drop-down (which lists the addresses configured on the selected interface), or enter an address.</li> <li>Click <b>OK</b>.</li> <li>Up to four management addresses are allowed. If you specify more than one <b>Management Address</b>, they will be sent in the order they are specified, starting at the top of the list. To change the order of the addresses, select an address and use the <b>Move Up</b> or <b>Move Down</b> buttons.</li> <li>Click <b>OK</b>.</li> </ol>
<p><b>Step 4</b> Assign an LLDP profile to an interface.</p>	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Interfaces</b> and select the interface where you will assign an LLDP profile.</li> <li>Select <b>Advanced &gt; LLDP</b>.</li> <li>Select the <b>Enable LLDP</b> check box to assign an LLDP profile to the interface.</li> <li>For <b>Profile</b>, select the profile you created. Selecting <b>None</b> enables LLDP with basic functionality: sends the three mandatory TLVs and enables <b>transmit-receive</b> mode. If you want to create a new profile, click <b>LLDP Profile</b> and follow the instructions in <a href="#">Step 4</a>.</li> <li>Click <b>OK</b>.</li> </ol>
<p><b>Step 5</b> Save the configuration.</p>	Click <b>Commit</b> .

## View LLDP Settings and Status

Perform the following procedure to view LLDP settings and status.

### View LLDP Settings and Status

Step 1 View LLDP global settings.	<p>1. Select <b>Network &gt; LLDP</b>.</p> <ul style="list-style-type: none"><li>• On the LLDP General screen, the <b>Enable</b> check box indicates whether LLDP is enabled or not.<ul style="list-style-type: none"><li>– If LLDP is enabled, the configured global settings (Transmit Interval, Transmit Delay, Hold Time Multiple, and Notification Interval) are displayed.</li><li>– If LLDP is not enabled, the default values of the global settings are displayed.</li></ul></li></ul> <p>For descriptions of these values, see <a href="#">(Optional) Change LLDP global settings</a>.</p>
-----------------------------------	--

**View LLDP Settings and Status (Continued)**

<p><b>Step 2</b> View the LLDP status information.</p>	<ol style="list-style-type: none"><li>1. Select the <b>Status</b> tab.</li><li>2. (Optional) Enter a filter to restrict the information that is displayed.</li></ol> <p><b>Interface Information:</b></p> <ul style="list-style-type: none"><li>• <b>Interface</b>—Name of the interfaces that have LLDP profiles assigned to them.</li><li>• <b>LLDP</b>—LLDP status: enabled or disabled.</li><li>• <b>Mode</b>—LLDP mode of the interface: Tx/Rx, Tx Only, or Rx Only.</li><li>• <b>Profile</b>—Name of the profile assigned to the interface.</li></ul> <p><b>Transmission Information:</b></p> <ul style="list-style-type: none"><li>• <b>Total Transmitted</b>—Count of LLDPDUs transmitted out the interface.</li><li>• <b>Dropped Transmit</b>—Count of LLDPDUs that were not transmitted out the interface because of an error. For example, a length error when the system is constructing an LLDPDU for transmission.</li></ul> <p><b>Received Information:</b></p> <ul style="list-style-type: none"><li>• <b>Total Received</b>—Count of LLDP frames received on the interface.</li><li>• <b>Dropped TLV</b>—Count of LLDP frames discarded upon receipt.</li><li>• <b>Errors</b>—Count of TLVs that were received on the interface and contained errors. Types of TLV errors include: one or more mandatory TLVs missing, out of order, containing out-of-range information, or length error.</li><li>• <b>Unrecognized</b>—Count of TLVs received on the interface that are not recognized by the LLDP local agent. For example, the TLV type is in the reserved TLV range.</li><li>• <b>Aged Out</b>—Count of items deleted from the Receive MIB due to proper TTL expiration.</li></ul>
--	--

**View LLDP Settings and Status (Continued)**

**Step 3** View summary LLDP information for each neighbor seen on an interface.

1. Select the **Peers** tab.
2. Optionally enter a filter to restrict the information being displayed.
  - Local Interface—Interface on the firewall that detected the neighboring device.
  - Remote Chassis ID—Chassis ID of the peer. The MAC address will be used.
  - Port ID—Port ID of the peer.
  - Name—Name of peer.
  - More info—Provides the following remote peer details, which are based on the Mandatory and Optional TLVs:
    - Chassis Type: MAC address.
    - MAC Address: MAC address of the peer.
    - System Name: Name of the peer.
    - System Description: Description of the peer.
    - Port Description: Port description of the peer.
    - Port Type: Interface name.
    - Port ID: The firewall uses the interface's ifname.
    - System Capabilities: Capabilities of the system. O=Other, P=Repeater, B=Bridge, W=Wireless-LAN, R=Router, T=Telephone
    - Enabled Capabilities: Capabilities enabled on the peer.
    - Management Address: Management address of the peer.

## Clear LLDP Statistics

You can clear LLDP statistics for specific interfaces.

Clear LLDP Statistics	
<p><b>Step 1</b> Clear LLDP statistics for specific interfaces.</p>	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; LLDP &gt; Status</b> and in the left hand column, select one or more interfaces for which you want to clear LLDP statistics.</li><li>2. Click <b>Clear LLDP Statistics</b> at the bottom of the screen.</li></ol>



# Policy

---

Policies allow you to enforce rules and take action. The different types of policy rules that you can create on the firewall are: Security, NAT, Quality of Service (QoS), Policy Based Forwarding (PBF), Decryption, Application Override, Captive Portal, Denial of Service (DoS), and Zone protection policies. All these different policies work together to allow, deny, prioritize, forward, encrypt, decrypt, make exceptions, authenticate access, and reset connections as needed to help secure your network. The following topics describe how to work with policy:

- ▲ [Policy Types](#)
- ▲ [Security Policy](#)
- ▲ [Policy Objects](#)
- ▲ [Security Profiles](#)
- ▲ [Enumeration of Rules Within a Rulebase](#)
- ▲ [Move or Clone a Policy Rule or Object to a Different Virtual System](#)
- ▲ [Use Tags to Group and Visually Distinguish Objects](#)
- ▲ [Use a Dynamic Block List in Policy](#)
- ▲ [Register IP Addresses and Tags Dynamically](#)
- ▲ [Monitor Changes in the Virtual Environment](#)
- ▲ [CLI Commands for Dynamic IP Addresses and Tags](#)
- ▲ [Identify Users Connected through a Proxy Server](#)
- ▲ [Policy-Based Forwarding](#)
- ▲ [DoS Protection Against Flooding of New Sessions](#)

## Policy Types

The Palo Alto Networks next-generation firewall supports a variety of policy types that work together to safely enable applications on your network.

Policy Type	Description
Security	Determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service. For more details, see <a href="#">Security Policy</a> .
NAT	Instruct the firewall which packets need translation and how to do the translation. The firewall supports both source address and/or port translation and destination address and/or port translation. For more details, see <a href="#">NAT</a> .
QoS	Identify traffic requiring QoS treatment (either preferential treatment or bandwidth-limiting) using a defined parameter or multiple parameters and assign it a class. For more details, see <a href="#">Quality of Service</a> .
Policy Based Forwarding	Identify traffic that should use a different egress interface than the one that would normally be used based on the routing table. For details, see <a href="#">Policy-Based Forwarding</a> .
Decryption	Identify encrypted traffic that you want to inspect for visibility, control, and granular security. For more details, see <a href="#">Decryption</a> .
Application Override	Identify sessions that you do not want processed by the App-ID engine, which is a Layer-7 inspection. Traffic matching an application override policy forces the firewall to handle the session as a regular stateful inspection firewall at Layer-4. For more details, see <a href="#">Manage Custom or Unknown Applications</a> .
Captive Portal	Identify traffic that requires the user to be known. The captive portal policy is only triggered if other User-ID mechanisms did not identify a user to associate with the source IP address. For more details, see <a href="#">Captive Portal</a> .
DoS Protection	Identify potential denial-of-service (DoS) attacks and take protective action in response to rule matches. <a href="#">DoS Protection Profiles</a> .

## Security Policy

Security policies protect network assets from threats and disruptions and aid in optimally allocating network resources for enhancing productivity and efficiency in business processes. On the Palo Alto Networks firewall, security policies determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

All traffic passing through the firewall is matched against a session and each session is matched against a security policy. When a session match occurs, the security policy is applied to bi-directional traffic (client to server and server to client) in that session. For traffic that doesn't match any defined rules, the default rules apply. The default rules—displayed at the bottom of the security rulebase—are predefined to allow all intrazone (within the zone) traffic and deny all interzone (between zones) traffic. Although these rules are part of the pre-defined configuration and are read-only by default, you can override them and change a limited number of settings, including the tags, action (allow or block), log settings, and security profiles.

Security policies are evaluated left to right and from top to bottom. A packet is matched against the first rule that meets the defined criteria; after a match is triggered the subsequent rules are not evaluated. Therefore, the more specific rules must precede more generic ones in order to enforce the best match criteria. Traffic that matches a rule generates a log entry at the end of the session in the traffic log, if logging is enabled for that rule. The logging options are configurable for each rule, and can for example be configured to log at the start of a session instead of, or in addition to, logging at the end of a session.

- ▲ Components of a Security Policy Rule
- ▲ Security Policy Best Practices

## Components of a Security Policy Rule

The security policy rule construct permits a combination of the required and optional fields as detailed in the following tables:

- ▲ Required Fields
- ▲ Optional Fields

### Required Fields

Required Field	Description
<b>Name</b>	A label that supports up to 31 characters, used to identify the rule.
<b>Rule Type</b>	<p>Specifies whether the rule applies to traffic within a zone, between zones, or both:</p> <ul style="list-style-type: none"> <li>• <b>universal</b> (default)—Applies the rule to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if you create a universal role with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, and all traffic from zone A to zone B and all traffic from zone B to zone A.</li> <li>• <b>intrazone</b>—Applies the rule to all matching traffic within the specified source zones (you cannot specify a destination zone for intrazone rules). For example, if you set the source zone to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.</li> <li>• <b>interzone</b>—Applies the rule to all matching traffic between the specified source and destination zones. For example, if you set the source zone to A, B, and C and the destination zone to A and B, the rule would apply to traffic from zone A to zone B, from zone B to zone A, from zone C to zone A, and from zone C to zone B, but not traffic within zones A, B, or C.</li> </ul>
<b>Source Zone</b>	The zone from which the traffic originates.
<b>Destination Zone</b>	The zone at which the traffic terminates. If you use NAT, make sure to always reference the post-NAT zone.
<b>Application</b>	The application which you wish to control. The firewall uses App-ID, the traffic classification technology, to identify traffic on your network. App-ID provides application control and visibility in creating security policies that block unknown applications, while enabling, inspecting, and shaping those that are allowed.

Required Field	Description (Continued)
<b>Action</b>	<p>Specifies an <i>Allow</i> or <i>Block</i> action for the traffic based on the criteria you define in the rule. When you configure the firewall to block traffic, it either resets the connection or silently drops packets. To provide a better user experience, you can configure granular options to block traffic instead of silently dropping packets, which can cause some applications to break and appear unresponsive to the user.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>—(default action) Allows the traffic.</li> <li>• <b>Deny</b>—Blocks traffic, and enforces the default <i>Deny Action</i> defined for the application that is being denied. To view the deny action defined by default for an application, view the application details in <b>Objects &gt; Applications</b> or check the application details in <b>Applipedia</b>.</li> <li>• <b>Drop</b>—Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset is not sent to the host/application.</li> </ul> <p>For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: <b>Drop</b> and enable the <b>Send ICMP Unreachable</b> checkbox. When enabled, the firewall sends the ICMP code for <i>communication with the destination is administratively prohibited</i>—ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.</p> <ul style="list-style-type: none"> <li>• Reset—Resets a connection in one of the following ways. <ul style="list-style-type: none"> <li>• <b>Reset client</b>—Sends a TCP reset to the client-side device.</li> <li>• <b>Reset server</b>—Sends a TCP reset to the server-side device.</li> <li>• <b>Reset both</b>—Sends a TCP reset to both the client-side and server-side devices.</li> </ul> </li> </ul> <p>A reset is sent only after a session is formed. If the session is blocked before a 3-way handshake is completed, the firewall does not send a reset. For a TCP session with a reset action, the firewall does not send an ICMP Unreachable response. For a UDP session with a drop or reset action, if the <b>ICMP Unreachable</b> checkbox is selected, the firewall sends an ICMP message to the client.</p>

## Optional Fields

Optional Field	Description
<b>Tag</b>	A keyword or phrase that allows you to filter security rules. This is handy when you have defined many rules and wish to then review those that are tagged with a keyword such as <i>IT-sanctioned applications</i> or <i>High-risk applications</i> .
<b>Description</b>	A text field, up to 255 characters, used to describe the rule.
<b>Source IP Address</b>	Define host IP or FQDN, subnet, named groups, or country-based enforcement. If you use NAT, make sure to always refer to the original IP addresses in the packet (i.e. the pre-NAT IP address).
<b>Destination IP Address</b>	The location or destination for the traffic. If you use NAT, make sure to always refer to the original IP addresses in the packet (i.e. the pre-NAT IP address).
<b>User</b>	The user or group of users for whom the policy applies. You must have User-ID enabled on the zone. To enable User-ID, see <a href="#">User-ID Overview</a> .

Optional Field	Description (Continued)
<b>URL Category</b>	<p>Using the URL Category as match criteria allows you to customize security profiles (antivirus, anti-spyware, vulnerability, file-blocking, Data Filtering, and DoS) on a per-URL-category basis. For example, you can prevent.exe file download/upload for URL categories that represent higher risk while allowing them for other categories. This functionality also allows you to attach schedules to specific URL categories (allow social-media websites during lunch &amp; after-hours), mark certain URL categories with QoS (financial, medical, and business), and select different log forwarding profiles on a per-URL-category-basis.</p> <p>Although you can manually configure URL categories on your device, to take advantage of the dynamic URL categorization updates available on the Palo Alto Networks firewalls, you must purchase a URL filtering license.</p>  To block or allow traffic based on URL category, you must apply a URL Filtering profile to the security policy rules. Define the URL Category as <i>Any</i> and attach a URL Filtering profile to the security policy. See <a href="#">Define Basic Security Rules</a> for information on using the default profiles in your security policy and see <a href="#">Control Access to Web Content</a> for more details.
<b>Service</b>	<p>Allows you to select a Layer 4 (TCP or UDP) port for the application. You can choose <i>any</i>, specify a port, or use <i>application-default</i> to permit use of the standards-based port for the application. For example, for applications with well-known port numbers such as DNS, the <i>application-default</i> option will match against DNS traffic only on TCP port 53. You can also add a custom application and define the ports that the application can use.</p>  For inbound allow rules (for example, from untrust to trust), using <i>application-default</i> prevents applications from running on unusual ports and protocols. Application-default is the default option; while the device still checks for all applications on all ports, with this configuration, applications are only allowed on their standard ports/protocols.
<b>Security Profiles</b>	<p>Provide additional protection from threats, vulnerabilities, and data leaks. Security profiles are only evaluated for rules that have an <i>allow</i> action.</p>
<b>HIP Profile (for GlobalProtect)</b>	<p>Allows you to identify clients with Host Information Profile (HIP) and then enforce access privileges.</p>
<b>Options</b>	<p>Allow you to define logging for the session, log forwarding settings, change Quality of Service (QoS) markings for packets that match the rule, and schedule when (day and time) the security rule should be in effect.</p>

## Security Policy Best Practices

The task of safely enabling Internet access and preventing misuse of web access privileges, and exposure to vulnerabilities and attacks is a continuous process. The key principle when defining policy on the Palo Alto Networks firewall is to use a positive enforcement approach. Positive enforcement implies that you selectively allow what is required for day-to-day business operations as opposed to a negative enforcement approach where you would selectively block everything that is not allowed. Consider the following suggestions when creating policy:

- If you have two or more zones with identical security requirements, combine them into one security rule.
- The ordering of rules is crucial to ensure the best match criteria. Because policy is evaluated top down, the more specific policy must precede the ones that are more general, so that the more specific rule is not *shadowed*. The term shadow refers to a rule that is not evaluated or is skipped because it is placed lower in the policy list. When the rule is placed lower, it is not evaluated because the match criteria was met by another rule that preceded it, thereby shadowing the rule from policy evaluation.
- To restrict and control access to inbound applications, in the security policy, explicitly define the port that the service/application will be listening on.
- Logging for broad allow rules—for example access to well known servers like DNS—can generate a lot of traffic. Hence it is not recommended unless absolutely necessary.
- By default, the firewall creates a log entry at the end of a session. However, you can modify this default behavior and configure the firewall to log at the start of the session. Because this significantly increases the log volume, logging at session start is recommended only when you are troubleshooting an issue. Another alternative for troubleshooting without enabling logging at session start is to use the session browser (**Monitor > Session Browser**) to view the sessions in real time.

## Policy Objects

A *policy object* is a single object or a collective unit that groups discrete identities such as IP addresses, URLs, applications, or users. With policy objects that are a collective unit, you can reference the object in security policy instead of manually selecting multiple objects one at a time. Typically, when creating a policy object, you group objects that require similar permissions in policy. For example, if your organization uses a set of server IP addresses for authenticating users, you can group the set of server IP addresses as an *address group* policy object and reference the address group in the security policy. By grouping objects, you can significantly reduce the administrative overhead in creating policies.

You can create the following policy objects on the firewall:

Policy Object	Description
Address/Address Group, Region	Allow you to group specific source or destination addresses that require the same policy enforcement. The address object can include an IPv4 or IPv6 address (single IP, range, subnet) or the FQDN. Alternatively, a region can be defined by the latitude and longitude coordinates or you can select a country and define an IP address or IP range. You can then group a collection of address objects to create an <i>address group</i> object. You can also use <a href="#">dynamic address groups</a> to dynamically update IP addresses in environments where host IP addresses change frequently.
User/User Group	Allow you to create a list of users from the local database or an external database and group them.
Application Group and Application Filter	An <i>Application Filter</i> allows you to filter applications dynamically. It allows you to filter, and save a group of applications using the attributes defined in the application database on the firewall. For example, you can <a href="#">Create an Application Filter</a> by one or more attributes—category, sub-category, technology, risk, characteristics. With an application filter, when a content update occurs, any new applications that match your filter criteria are automatically added to your saved application filter. An <i>Application Group</i> allows you to create a static group of specific applications that you want to group together for a group of users or for a particular service, or to achieve a particular policy goal. See <a href="#">Create an Application Group</a> .
Service/Service Groups	Allows you to specify the source and destination ports and protocol that a service can use. The firewall includes two pre-defined services—service-http and service-https—that use TCP ports 80 and 8080 for HTTP, and TCP port 443 for HTTPS. You can however, create any custom service on any TCP/UDP port of your choice to restrict application usage to specific ports on your network (in other words, you can define the default port for the application).
	 To view the standard ports used by an application, in <b>Objects &gt; Applications</b> search for the application and click the link. A succinct description displays.

## Security Profiles

While security policies enable you to allow or block traffic on your network, security profiles help you define an *allow but scan* rule, which scan allowed applications for threats, such as viruses, malware, spyware, and DDOS attacks. When traffic matches the allow rule defined in the security policy, the security profile(s) that are attached to the rule are applied for further content inspection rules such as antivirus checks and data filtering.



Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.

The firewall provides default security profiles that you can use out of the box to begin protecting your network from threats. See [Set Up Basic Security Policies](#) for information on using the default profiles in your security policy. As you get a better understanding about the security needs on your network, you can create custom profiles. See [Scan Traffic for Threats](#) for more information.

You can add security profiles that are commonly applied together to a security profile group; this set of profiles can be treated as a unit and added to security policies in one step (or included in security policies by default, if you choose to set up a default security profile group).

The following topics provide more detailed information about each type of security profile and how to set up a security profile group:

- ▲ [Antivirus Profiles](#)
- ▲ [Anti-Spyware Profiles](#)
- ▲ [Vulnerability Protection Profiles](#)
- ▲ [URL Filtering Profiles](#)
- ▲ [Data Filtering Profiles](#)
- ▲ [File Blocking Profiles](#)
- ▲ [WildFire Analysis Profiles](#)
- ▲ [DoS Protection Profiles](#)
- ▲ [Zone Protection Profiles](#)
- ▲ [Security Profile Group](#)

## Antivirus Profiles

Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto Networks antivirus solution can provide protection for clients without significantly impacting the performance of the firewall. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. If you have enabled [Decryption](#) on the firewall, the profile also enables scanning of decrypted content.

The default profile inspects all of the listed protocol decoders for viruses, and generates alerts for SMTP, IMAP, and POP3 protocols while blocking for FTP, HTTP, and SMB protocols. You can configure the action for a decoder or antivirus signature and specify how the firewall responds to a threat event:

- **Default**—For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. Typically, the default action is an alert or a reset-both. The default action is displayed in parenthesis, for example default (alert) in the threat or Antivirus signature.
- **Allow**—Permits the application traffic
- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop**—Drops the application traffic.
- **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
- **Reset Server**—For TCP, resets the server-side connection. For UDP, drops the connection.
- **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.

Customized profiles can be used to minimize antivirus inspection for traffic between trusted security zones, and to maximize the inspection of traffic received from untrusted zones, such as the Internet, as well as the traffic sent to highly sensitive destinations, such as server farms.

The Palo Alto Networks WildFire system also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As threats are discovered by WildFire, signatures are quickly created and then integrated into the standard antivirus signatures that can be downloaded by Threat Prevention subscribers on a daily basis (sub-hourly for WildFire subscribers).

## Anti-Spyware Profiles

Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you may want to have custom Anti-Spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic received from an untrusted zone, such as Internet facing zones.

You can define your own custom Anti-Spyware profiles, or choose one of the following predefined profiles when applying anti-spyware to a security policy:

- **Default**—Uses the default action for every signature, as specified by Palo Alto Networks when the signature is created.
- **Strict**—Overrides the default action of critical, high, and medium severity threats to the block action, regardless of the action defined in the signature file. This profile still uses the default action for medium and informational severity signatures.

When the firewall detects a threat event, you can configure the following actions in an Anti-Spyware profile:

- **Default**—For each threat signature and anti-spyware signature that is defined by Palo Alto Networks, a default action is specified internally. Typically the default action is an alert or a reset-both. The default action is displayed in parenthesis, for example default (alert) in the threat or Antivirus signature.
- **Allow**—Permits the application traffic
- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop**—Drops the application traffic.
- **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
- **Reset Server**—For TCP, resets the server-side connection. For UDP, drops the connection.
- **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
- **Block IP**— This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

In addition, you can enable the [DNS Sinkholing](#) action in Anti-Spyware profiles to enable the firewall to forge a response to a DNS query for a known malicious domain, causing the malicious domain name to resolve to an IP address that you define. This feature helps to identify infected hosts on the protected network using DNS traffic. Infected hosts can then be easily identified in the traffic and threat logs because any host that attempts to connect to the sinkhole IP address are most likely infected with malware.

Anti-Spyware and Vulnerability Protection profiles are configured similarly.

## Vulnerability Protection Profiles

Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network. For example, Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection profile protects clients and servers from all known critical, high, and medium-severity threats. You can also create exceptions, which allow you to change the response to a specific signature.

To configure how the firewall responds to a threat, see [Anti-Spyware Profiles](#) for a list of supported actions.

## URL Filtering Profiles

[URL Filtering](#) profiles enable you to monitor and control how users access the web over HTTP and HTTPS. The firewall comes with a default profile that is configured to block websites such as known malware sites, phishing sites, and adult content sites. You can use the default profile in a security policy, clone it to be used as a starting point for new URL filtering profiles, or add a new URL profile that will have all categories set to allow for visibility into the traffic on your network. You can then customize the newly added URL profiles and add lists of specific websites that should always be blocked or allowed, which provides more granular control over URL categories.

## Data Filtering Profiles

Data filtering profiles prevent sensitive information such as credit card or social security numbers from leaving a protected network. The data filtering profile also allows you to filter on key words, such as a sensitive project name or the word confidential. It is important to focus your profile on the desired file types to reduce false positives. For example, you may only want to search Word documents or Excel spreadsheets. You may also only want to scan web-browsing traffic, or FTP.

You can use default profiles, or create custom data patterns. There are two default profiles:

- CC# (Credit Card)—Identifies credit card numbers using a hash algorithm. The content must match the hash algorithm in order for data to be detected as a credit card number. This method will reduce false positives.
- SSN# (Social Security Number)—Uses an algorithm to detect nine digit numbers, regardless of format. There are two fields: SSN# and SSN# (no dash).

### Weight and Threshold Values

It is important to understand how the weight of an object (SSN, CC#, pattern) is calculated in order to set the appropriate threshold for a condition you are trying to filter. Each occurrence multiplied by the weight value will be added together in order to reach an action threshold (alert or block).

### Example: Filter for Social Security Numbers Only

For simplicity, if you only want to filter files with Social Security Numbers (SSN) and you define a weight of 3 for SSN#, you would use the following formula: each instance of a SSN x weight = threshold increment. In this case, if a Word document has 10 social security numbers you multiply that by the weight of 3, so  $10 \times 3 = 30$ . In order to take action for a file that contains 10 social security numbers you would set the threshold to 30. You may want to set an alert at 30 and then block at 60. You may also want to set a weight in the field SSN# (no dash) for Social Security Numbers that do not contain dashes. If multiple settings are used, they will accumulate to reach a given threshold.

### Example: Filter for Social Security Numbers and a Custom Pattern

In this example, we will filter on files that contain Social Security Numbers and the custom pattern confidential. In other words, if a file has Social Security Numbers in addition to the word confidential and the combined instances of those items hit the threshold, the file will trigger an alert or block, depending on the action setting.

SSN# weight = 3

Custom Pattern confidential weight = 20

The custom pattern is case sensitive.

If the file contains 20 Social Security Numbers and a weight of 3 is configured, that is  $20 \times 3 = 60$ . If the file also contains one instance of the term confidential and a weight of 20 is configured, that is  $1 \times 20 = 20$  for a total of 80. If your threshold for block is set to 80, this scenario would block the file. The alert or block action will be triggered as soon as the threshold is hit.

## File Blocking Profiles

The firewall uses file blocking profiles to block specified file types over specified applications and in the specified session flow direction (inbound/outbound/both). You can set the profile to alert or block on upload and/or download and you can specify which applications will be subject to the file blocking profile. You can also configure custom block pages that will appear when a user attempts to download the specified file type. This allows the user to take a moment to consider whether or not they want to download a file.

Configure a file blocking profile with the following actions:

- **Alert**—When the specified file type is detected, a log is generated in the data filtering log.
- **Block**—When the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log is also generated in the data filtering log.
- **Continue**—When the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log is also generated in the data filtering log. Because this type of forwarding action requires user interaction, it is only applicable for web traffic.

## WildFire Analysis Profiles

Use a WildFire analysis profile to enable the firewall to [forward unknown files or email links for WildFire analysis](#). Specify files to be forwarded for analysis based on application, file type, and transmission direction (upload or download). Files or email links matched to the profile rule are forwarded either the WildFire public cloud or the WildFire private cloud (hosted with a WF-500 appliance), depending on the analysis location defined for the rule.

You can also use the WildFire analysis profiles to set up a [Wildfire hybrid cloud](#) deployment. If you are using a WildFire appliance to analyze sensitive files locally (such as PDFs), you can specify for less sensitive file types (such as PE files) or file types that are not supported for WildFire appliance analysis (such as APKs) to be analyzed by the WildFire public cloud. Using both the WildFire appliance and the WildFire cloud for analysis allows you to benefit from a prompt verdict for files that have already been processed by the cloud, and for files that are not supported for appliance analysis, and frees up the appliance capacity to process sensitive content.

## DoS Protection Profiles

DoS protection profiles provide detailed control for Denial of Service (DoS) protection policies. DoS policies allow you to control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. There are two DoS protection mechanisms that the Palo Alto Networks firewalls support.

- **Flood Protection**—Detects and prevents attacks where the network is flooded with packets resulting in too many half-open sessions and/or services being unable to respond to each request. In this case the source address of the attack is usually spoofed. See [DoS Protection Against Flooding of New Sessions](#).
- **Resource Protection**— Detects and prevent session exhaustion attacks. In this type of attack, a large number of hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources.

You can enable both types of protection mechanisms in a single DoS protection profile.

The DoS profile is used to specify the type of action to take and details on matching criteria for the DoS policy. The DoS profile defines settings for SYN, UDP, and ICMP floods, can enable resource protect and defines the maximum number of concurrent connections. After you configure the DoS protection profile, you then attach it to a DoS policy.

When configuring DoS protection, it is important to analyze your environment in order to set the correct thresholds and due to some of the complexities of defining DoS protection policies, this guide will not go into detailed examples. For more information, refer to the [Threat Prevention Tech Note](#).

## Zone Protection Profiles

Zone protection profiles provide additional protection between specific network zones in order to protect the zones against attack. The profile must be applied to the entire zone, so it is important to carefully test the profiles in order to prevent issues that may arise with the normal traffic traversing the zones. When defining packets per second (pps) thresholds limits for zone protection profiles, the threshold is based on the packets per second that do not match a previously established session. For more information, refer to the [Threat Prevention Tech Note](#).

## Security Profile Group

A security profile group is a set of security profiles that can be treated as a unit and then easily added to security policies. Profiles that are often assigned together can be added to profile groups to simplify the creation of security policies. You can also setup a default security profile group—new security policies will use the settings defined in the default profile group to check and control traffic that matches the security policy. Name a security profile group *default* to allow the profiles in that group to be added to new security policies by default. This allows you to consistently include your organization's preferred profile settings in new policies automatically, without having to manually add security profiles each time you create new rules.

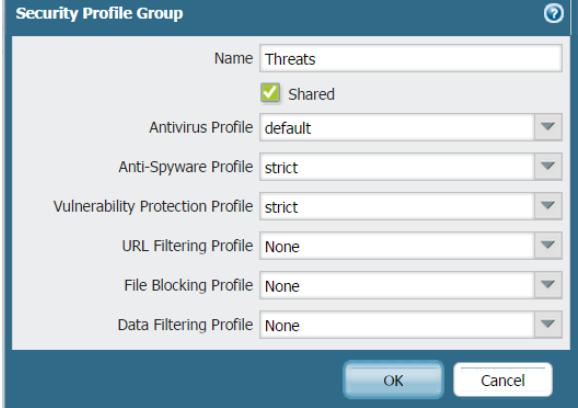
The following sections show how to create a security profile group and how to enable a profile group to be used by default in new security policies:

- ▲ [Create a Security Profile Group](#)
- ▲ [Set Up or Override a Default Security Profile Group](#)

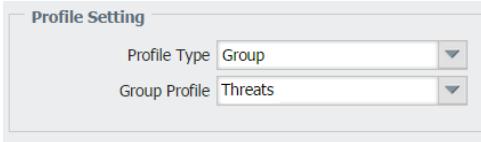
### Create a Security Profile Group

Use the following steps to create a security profile group and add it to a security policy.

#### Create a Security Profile Group

Step 1 Create a security profile group.	<ol style="list-style-type: none"><li>1. Select <b>Objects &gt; Security Profile Groups</b> and <b>Add</b> a new security profile group.</li><li>2. Give the profile group a descriptive <b>Name</b>, for example, Threats.</li><li>3. If the firewall is in Multiple Virtual System Mode, enable the profile to be <b>Shared</b> by all virtual systems.</li><li>4. Add existing profiles to the group.</li></ol>  <ol style="list-style-type: none"><li>5. Click <b>OK</b> to save the profile group.</li></ol>
---	---

### Create a Security Profile Group

<p><b>Step 2</b> Add a security profile group to a security policy.</p>	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; Security</b> and <b>Add</b> or modify a security policy rule.</li><li>2. Select the <b>Actions</b> tab.</li><li>3. In the Profile Setting section, select <b>Group</b> for the <b>Profile Type</b>.</li><li>4. In the <b>Group Profile</b> drop-down, select the group you created (for example, select the Threats group):</li></ol>  <ol style="list-style-type: none"><li>5. Click <b>OK</b> to save the policy and <b>Commit</b> your changes.</li></ol>
<p><b>Step 3</b> Save your changes.</p>	<p>Click <b>Commit</b>.</p>

### Set Up or Override a Default Security Profile Group

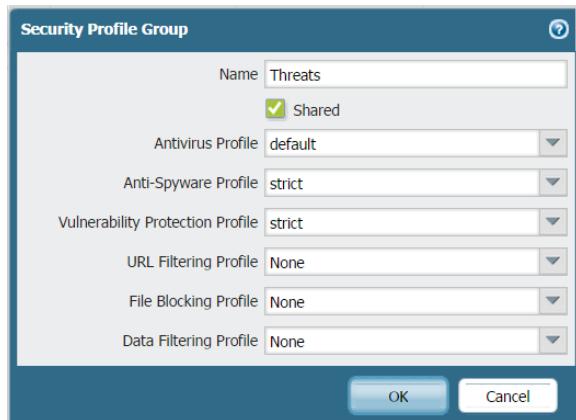
Use the following options to set up a default security profile group to be used in new security policies, or to override an existing default group. When an administrator creates a new security policy, the default profile group will be automatically selected as the policy's profile settings, and traffic matching the policy will be checked according to the settings defined in the profile group (the administrator can choose to manually select different profile settings if desired). Use the following options to set up a default security profile group or to override your default settings.



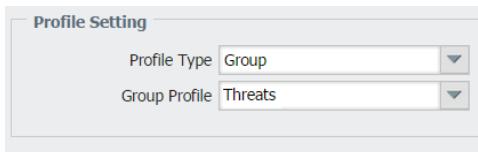
If no default security profile exists, the profile settings for a new security policy are set to **None** by default.

### Set Up or Override a Default Security Profile Group

- Create a security profile group.
1. Select **Objects > Security Profile Groups** and Add a new security profile group.
  2. Give the profile group a descriptive **Name**, for example, Threats.
  3. If the firewall is in Multiple Virtual System Mode, enable the profile to be **Shared** by all virtual systems.
  4. Add existing profiles to the group. For details on creating profiles, see [Security Profiles](#).



5. Click **OK** to save the profile group.
6. **Add the security profile group to a security policy.**
7. **Add or modify a security policy rule and select the Actions tab.**
8. **Select Group for the Profile Type.**
9. In the **Group Profile** drop-down, select the group you created (for example, select the Threats group):

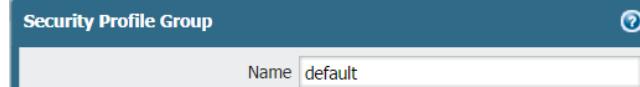


10. Click **OK** to save the policy and **Commit** your changes.

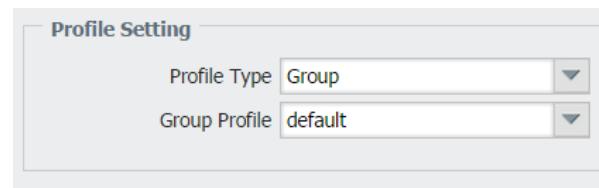
**Set Up or Override a Default Security Profile Group**

- Set up a default security profile group.

1. Select **Objects > Security Profile Groups** and add a new security profile group or modify an existing security profile group.
2. Name the security profile group *default*:



3. Click **OK** and **Commit**.
4. Confirm that the *default* security profile group is included in new security policies by default:
  - a. Select **Policies > Security** and **Add** a new security policy.
  - b. Select the **Actions** tab and view the **Profile Setting** fields:



By default, the new security policy correctly shows the **Profile Type** set to Group and the *default* **Group Profile** is selected.

- Override a default security profile group.

If you have an existing default security profile group, and you do not want that set of profiles to be attached to a new security policy, you can continue to modify the Profile Setting fields according to your preference. Begin by selecting a different Profile Type for your policy (**Policies > Security > Security Policy Rule > Actions**).

## Enumeration of Rules Within a Rulebase

Each rule within a rulebase is automatically numbered and the ordering adjusts as rules are moved or reordered. When filtering rules to find rules that match the specified filter(s), each rule is listed with its number in the context of the complete set of rules in the rulebase and its place in the evaluation order.

On Panorama, pre-rules, post-rules, and default rules are independently numbered. When Panorama pushes rules to a firewall, the rule numbering reflects the hierarchy and evaluation order of shared rules, device-group pre-rules, firewall rules, device-group post-rules, and default rules. The **Preview Rules** option in Panorama displays an ordered list view of the total number of rules on a firewall.

### View the Ordered List of Rules Within a Rulebase

- View the numbered list of rules on the firewall.

Select **Policies** and any rulebase under it. For example, **Policies > QoS**. The left-most column in the table displays the rule number.

	Name	Tags	Type	Zone	Address	User
1	foobar security policy	none	universal	any	any	paloaltonet...
2	Watch PM-Firewall ...	Jamie	universal	trust	any	any
3	DMZ rule	schlumberger	universal	DMZ	any	any
4	pre-rule1	Jamie	universal	DMZ	any	any
5	Block exe from shop...	none	universal	any	any	any
6	block User	\$My tag	universal	any	Loopback: My MacBook ...	jamie_fitz user

- View the numbered list of rules on Panorama.

Select **Policies** and any rulebase under it. For example, **Policies > Security> Pre-rules**.

	Name	Location	Tags	Type	Zone	Address
1	test	Shared	none	universal	any	any
2	corp_AUP	PA-200_TechPub...	none	universal	any	any
3	corporate_deny	PA-200_TechPub...	none	universal	any	Corp
4	bogus rule	PA-200_TechPub...	none	universal	any	any
5	Pass_everything	PA-200_TechPub...	none	universal	!3-trust	any
6	block file transfers	PA-200_TechPub...	none	universal	any	any
7	BLOCK_SKYPE	PA-200_TechPub...	none	universal	!3-trust	any
8	Allow Skype probe	PA-200_TechPub...	none	universal	!3-trust	any
9	access with public IP	PA-200_TechPub...	none	universal	!3-untrust	any
10	unknown apps	PA-200_TechPub...	none	universal	any	any

### View the Ordered List of Rules Within a Rulebase (Continued)

- After you push the rules from Panorama, view the complete list of rules with numbers on the firewall.

From the web interface of the firewall, select **Policies** and pick any rulebase under it. For example, select **Policies > Security** and view the complete set of numbered rules that the firewall will evaluate.

	Name	Tags	Type	Zone	Address	Source	
						User	Source
1	foobar security policy	none	universal	any	any	paloaltonet...	
2	Watch PM-Firewall ...	Jamie	universal	px trust	any	any	
3	DMZ rule	schlumberger	universal	px DMZ	any	any	
4	pre-rule1	Jamie	universal	px DMZ	any	any	
5	Block exe from shop...	none	universal	any	any	any	
6	block User	\$My tag	universal	any	Loopback My MacBook ... My MacBook ... My MacBook ... My MacBook ... My iPhone new test more...	jamie_fitz user zone	
7	Watch SSL	Core-infrastru...	universal	any	any	any	
8	Watch DNS	Core-infrastru...	universal	any	any	any	
9	Watch iCloud	Core-infrastru...	universal	any	any	any	
10	Watch itunes	Cloud Music Bandwidth-ho...	universal	any	any	any	
11	Watch Spotify	Music Bandwidth-ho...	universal	any	any	any	
12	Watch Gmail	time-waster	universal	any	any	any	
13	Watch Sports	time-waster	universal	any	any	any	
14	Watch Jabber	productivity time-waster	universal	any	any	any	
15	Watch Corp Mail	productivity	universal	any	any	any	
16	Allow All	productivity a b	universal	any	any	any	
17	syslog-test	none	universal	any	any	any	
18	post1	none	universal	any	any	any	
19	shared-post-rule1	none	universal	any	any	any	
20	intrazone-default	none	intrazone	any	any	any	
21	interzone-default	none	interzone	any	any	any	

# Move or Clone a Policy Rule or Object to a Different Virtual System

On a firewall that has more than one virtual system (vsys), you can move or clone policy rules and objects to a different vsys or to the Shared location. Moving and cloning save you the effort of deleting, recreating, or renaming rules and objects. If the policy rule or object that you will move or clone from a vsys has references to objects in that vsys, move or clone the referenced objects also. If the references are to shared objects, you do not have to include those when moving or cloning. You can perform a [Use Global Find](#) to check for references.

## Move or Clone a Policy Rule or Object to a Virtual System

**Step 1** Select the policy type (for example, **Policy > Security**) or object type (for example, **Objects > Addresses**).

**Step 2** Select the **Virtual System** and select one or more policy rules or objects.

**Step 3** Perform one of the following steps:

- Select **Move > Move to other vsys** (for policy rules).
- Click **Move** (for objects).
- Click **Clone** (for policy rules or objects).

**Step 4** In the **Destination** drop-down, select the new virtual system or **Shared**. The default is the **Virtual System** selected in [Step 2](#).

**Step 5** (Policy rules only) Select the **Rule order**:

- **Move top** (default)—The rule will come before all other rules.
- **Move bottom**—The rule will come after all other rules.
- **Before rule**—In the adjacent drop-down, select the rule that comes after the Selected Rules.
- **After rule**—In the adjacent drop-down, select the rule that comes before the Selected Rules.

**Step 6** The **Error out on first detected error in validation** check box is selected by default. The firewall stops performing the checks for the move or clone action when it finds the first error, and displays just this error. For example, if an error occurs when the **Destination** vsys doesn't have an object that the policy rule you are moving references, the firewall will display the error and stop any further validation. When you move or clone multiple items at once, selecting this check box will allow you to find one error at a time and troubleshoot it. If you clear the check box, the firewall collects and displays a list of errors. If there are any errors in validation, the object is not moved or cloned until you fix all the errors.

**Step 7** Click **OK** to start the error validation. If the firewall displays errors, fix them and retry the move or clone operation. If the firewall doesn't find errors, the object is moved or cloned successfully. After the operation finishes, click **Commit**.

## Use Tags to Group and Visually Distinguish Objects

You can tag objects to group related items and add color to the tag in order to visually distinguish tagged objects. Tags can be added to the following objects: address objects, address groups, zones, service groups, and policy rules.

The firewall and Panorama support both static tags and dynamic tags, dynamic tags are registered from a variety of sources and are not displayed with the static tags, because dynamic tags are not part of the device configuration. See [Register IP Addresses and Tags Dynamically](#) for information on registering tags dynamically. The tags discussed in this section are statically added and are part of the device configuration.

One or more tags can be applied to objects and to policy rules; a maximum of 64 tags can be applied to an object. Panorama supports a maximum of 10,000 tags that can be apportioned across Panorama (shared and device groups) and the managed devices (including devices with multiple virtual systems).

To use tags effectively, see the following topics:

- ▲ [Create and Apply Tags](#)
- ▲ [Modify Tags](#)
- ▲ [Use the Tag Browser](#)

## Create and Apply Tags

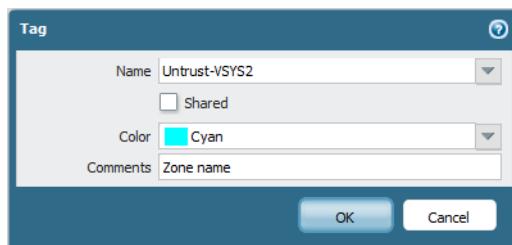
### Create and Apply tags

#### Step 1 Create tags.



To tag a zone, you must create a tag with the same name as the zone. When the zone is attached in policy rules, the tag color automatically displays as the background color against the zone name.

1. Select **Objects > Tags**.
2. On Panorama or a multiple virtual system firewall, select the **Device Group** or the **Virtual System** to which this object must belong.
3. Click **Add** and enter a **Name** to identify the tag. The maximum length is 127 characters.
4. (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.
5. (Optional) Assign one of the 16 predefined colors to the tag. By default, no color is selected.



6. Click **OK** and **Commit** to save the changes.

#### Step 2 Apply tags to policy.

1. Select **Policies** and any rulebase under it.
2. Click **Add** to create a policy rule and use the tagged objects you created in Step 1.
3. Verify that the tags are in use.

Source		Destination			
Zone	User	Zone	Address	Application	Service
Trust-VSYS2	known-user	Untrust-VSYS2	FTP	ftp	application

#### Step 3 Apply tags to an address object, address group, service, or service group.

1. Create the object.  
For example to create a service group, select **Objects > Service Groups > Add**.
2. Select the tag(s) from the **Tag** drop-down or enter a phrase to create a new tag.  
To edit a tag or add color to the tag, see [Modify Tags](#).

## Modify Tags

### Modify Tags

- Select **Objects > Tags** to perform any of the following operations with tags:
  - Click the link in the **Name** column to edit the properties of a tag.
  - Select a tag in the table, and click **Delete** to remove the tag from the firewall.
  - Click **Clone** to create a duplicate tag with the same properties. A numerical suffix is added to the tag name.  
For example, FTP-1.

For details on creating tags, see [Create and Apply Tags](#). For information on working with tags, see [Use the Tag Browser](#).

## Use the Tag Browser

The tag browser provides a way to view all the [tags](#) used within a rulebase. In rulebases with a large number of rules, the tag browser simplifies the display by presenting the tags, the color code, and the rule numbers in which the tags are used.

It also allows you to group rules using the first tag applied to the rule. As a best practice, use the first tag to identify the primary purpose for a rule. For example, the first tag can identify a rule by a high-level function such as best practice, or Internet access or IT sanctioned applications or high-risk applications. In the tag browser, when you **Filter by first tag in rule**, you can easily identify gaps in coverage and move rules or add new rules within the rulebase. All the changes are saved to the candidate configuration until you commit the changes on the firewall and make them a part of the running configuration.

For devices that are managed by Panorama, the tags applied to pre-rules and post-rules that have been pushed from Panorama, display in a green background and are demarcated with green lines so that you can identify these tags from the local tags on the device.

Source							
Name	Tags	Type	Zone	Address	User	HIP Priority	
6 object_resolution_te...	none	universal	any	any	any	any	
7 Allow-Jamie-PA-200...	Mgmt-access	universal	any untrust	any	any	any	
8 Allow Jamie PA-200 ...	Mgmt-access	universal	any untrust	any	any	any	
9 deny non-eng-pm pla...	Josh	universal	any untrust	any	any	any	
10 ALLOW PM	none	universal	any	any	paloaltonetw...	any	
11 Allow all	Alarm-tag	universal	any	any	any	any	
12 allow planner access	Exceptions	universal	any untrust	any	paloaltonetw...	any	
13 IT Sanctioned SaaS ...	Best Practice	universal	trust	any	any	any	
14 IT DNS Services	Best Practice	universal	trust	any	any	any	
15 IT Deployed Apps	Best Practice	universal	trust	any	any	any	
16 General Business Apps	Best Practice	universal	trust	any	any	any	
17 General Web Infrastr...	Best Practice	universal	trust	any	any	any	

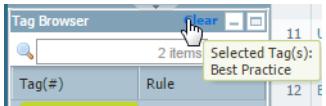
## Use the Tag Browser

- Explore the tag browser.

- Access the **Tag Browser** on the left pane of the **Policies >** tab. The tag browser displays the tags that have been used in the rules for the selected rulebase, for example **Policies > Security**.
- Tag (#)**—Displays the label and the rule number or range of numbers in which the tag is used contiguously. Hover over the label to see the location where the rule was defined, it can be inherited from a shared location, a device group, or a virtual system.
- Rule**—Lists the rule number or range of numbers associated with the tags.
- Sort the tags.
  - Filter by first tag in rule**—Sorts rules using the first tag applied to each rule in the rulebase. This view is particularly useful if you want to narrow the list and view related rules that might be spread around the rulebase. For example if the first tag in each rule denotes its function—best practices, administration, web-access, data center access, proxy—you can narrow the result and scan the rules based on function.
  - Rule Order**—Sorts the tags in the order of appearance within the selected rulebase. When displayed in order of appearance, tags used in contiguous rules are grouped. The rule number with which the tag is associated is displayed along with the tag name.
  - Alphabetical**—Sorts the tags in alphabetical order within the selected rulebase. The display lists the tag name and color (if a color is assigned) and the number of times it is used within the rulebase.
- The label **None** represents rules without any tags; it does not display rule numbers for untagged rules. When you select **None**, the right pane is filtered to display rules that have no tags assigned to them.
- Clear**—Clears the filter on the currently selected tags in the search bar.
- Search bar**—To search for a tag, enter the term and click the green arrow icon to apply the filter. It also displays the total number of tags in the rulebase and the number of selected tags.
- Expand or collapse the tag browser.



### Use the Tag Browser (Continued)

<ul style="list-style-type: none"> <li>Tag a rule.</li> </ul>	<ol style="list-style-type: none"> <li>Select a rule on the right pane.</li> <li>Do one of the following:           <ul style="list-style-type: none"> <li>Select a tag in the tag browser and select <b>Apply the Tag to the Selection(s)</b> from the drop-down.</li> <li>Drag and drop tag(s) from the tag browser on to the Tags column of the rule. When you drop a tag, a confirmation dialog displays.</li> </ul> </li> <li><b>Commit</b> the changes.</li> </ol>
<ul style="list-style-type: none"> <li>View rules that match the selected tags.</li> </ul> <p>You can filter rules based on tags with an AND or an OR operator.</p>	<ul style="list-style-type: none"> <li>OR filter: To view rules that have specific tags, select one or more tags in the tag browser; the right pane only displays the rules that include any of the currently selected tags.</li> <li>AND filter: To view rules that have all the selected tags, hover over the number associated with the tag in the <b>Rule</b> column of the tag browser and select <b>Filter</b>. Repeat to add more tags.</li> </ul>  <p>Click the apply filter icon in the search bar on the right pane. The results are displayed using an AND operator.</p>
<ul style="list-style-type: none"> <li>View the currently selected tags.</li> </ul>	<p>To view the currently selected tags, hover over the <b>Clear</b> label in the tag browser.</p> 
<ul style="list-style-type: none"> <li>Untag a rule.</li> </ul>	<p>Hover over the rule number associated with a tag in the <b>Rule</b> column of the tag browser and select <b>Untag Rule(s)</b>. Confirm that you want to remove the selected tag from the rule. <b>Commit</b> the changes.</p>
<ul style="list-style-type: none"> <li>Reorder rules using tags.</li> </ul>	<p>Select one or more tags and hover over the rule number in the Rule column of the tag browser and select <b>Move Rule(s)</b>.</p> <p>Select a tag from the drop-down in the move rule window and select whether you want to <b>Move Before</b> or <b>Move After</b> the tag selected in the drop-down. <b>Commit</b> the changes.</p>

**Use the Tag Browser (Continued)**

<ul style="list-style-type: none"><li>• Add a new rule that applies the selected tags.</li></ul>	Select one or more tags and hover over the rule number in the <b>Rule</b> column of the tag browser, and select <b>Add New Rule</b> . Define the rule and <b>Commit</b> the changes. The numerical order of the new rule varies by whether you selected a rule on the right pane. If you did not select a rule on the right pane, the new rule will be added after the rule to which the selected tag(s) belongs. Otherwise, the new rule is added after the selected rule.
<ul style="list-style-type: none"><li>• Search for a tag.</li></ul>	In the tag browser, enter the first few letters of the tag name you want to search for and click the Apply Filter icon. The tags that match your input will display.

## Use a Dynamic Block List in Policy

The firewall or Panorama typically enforce policy for a source or destination IP address that is defined as a static object on the firewall. If you need agility in enforcing policy for a list of source/destination IP addresses that emerge ad hoc, you can use dynamic block lists.

A dynamic block list is a text file that contains a list of IP addresses, IP ranges, or IP subnets, and is hosted on a web server. The dynamic block list can be used to deny or allow access to the IP addresses (IPv4 and IPv6) included in the list. For example, you can use it as a whitelist for allowing a set of IP addresses or as a blacklist to disallow access to the specified IP addresses. At a configured interval, the firewall dynamically imports the list and enforces policy for the IP addresses included in the list. When you modify the list, the firewall retrieves the updates; a configuration change or commit is not required on the firewall. If the web server is unreachable, the firewall or Panorama will use the last successfully retrieved list for enforcing policy until the connection is restored with the web server that hosts the list.

- ▲ [View the IP Address Limit For Your Firewall Model](#)
- ▲ [Formatting Guidelines for Dynamic Block Lists](#)
- ▲ [Enforce Policy with a Dynamic Block List](#)
- ▲ [View the List of IP addresses in the Dynamic Block List](#)
- ▲ [Retrieve a Dynamic Block List from Web Server](#)

### View the IP Address Limit For Your Firewall Model

Irrespective of the firewall model, each firewall supports a maximum of 10 Dynamic Block Lists.

To find the maximum number of addresses, address groups, and IP addresses per group, for your model of the firewall, use the following CLI command:

```
show system state | match cfg.general.max-address
```

For example:

```
admin@PA-7050> show system state | match cfg.general.max-address
cfg.general.max-address: 80000
cfg.general.max-address-group: 8000
cfg.general.max-address-per-group: 500
```



Each list can contain the maximum number of addresses supported by your firewall model minus 300. Up to 300 IP addresses are reserved for internal use on the firewall and are deducted from the available limit. Therefore, in the example above, the firewall can have a maximum of 79,700 IP addresses.

## Formatting Guidelines for Dynamic Block Lists

The dynamic block list can include individual IP addresses, subnet addresses (address/mask), or range of IP addresses. In addition, the block list can include comments and special characters such as \*, :, ;, #, or /. The syntax for each line in the list is [ IP address, IP/Mask, or IP start range-IP end range ] [ space ] [ comment ].

Because the firewall ignores incorrectly formatted lines, use these guidelines when defining the list:

- Enter each IP address/range/subnet in a new line; URLs are not supported in this list.
- If you add comments, the comment must be on the same line as the IP address/range/subnet. The space at the end of the IP address is the delimiter that separates a comment from the IP address.

An example:

```
192.168.20.10/32
2001:db8:123:1::1 #test IPv6 address
192.168.20.0/24 ; test internal subnet
2001:db8:123:1::/64 test internal IPv6 range
192.168.20.40-192.168.20.50
```



For an IP address that is blocked, you can display a notification page only if the protocol is HTTP.

## Enforce Policy with a Dynamic Block List

### Enforce Policy with a Dynamic Block List

<p><b>Step 1</b> Create the dynamic block list and host it on a web server, so that the firewall can retrieve the list for policy evaluation.</p>	<p>1. Create a text file and enter the IP addresses for which you want to enforce policy. For syntax, see <a href="#">Formatting Guidelines for Dynamic Block Lists</a>.</p>
<p><b>Step 2</b> Create a dynamic block list object on the firewall.</p>	<p>1. Select <b>Objects &gt; Dynamic Block Lists</b>. 2. Click <b>Add</b> and enter a descriptive <b>Name</b> for the list. 3. (Optional) Select <b>Shared</b>, to share the list with all virtual systems on a device that is enabled for multiple virtual systems. By default, the object is created on the virtual system that is currently selected in the <b>Virtual Systems</b> drop-down. 4. Enter the <b>Source URL</b> (hostname or IP address and the path) for the list you just created on the web server. For example, <a href="https://1.2.3.4/DBL_2014">https://1.2.3.4/DBL_2014</a> 5. Click <b>Test Source URL</b> to verify that the firewall or Panorama can connect to the web server. 6. (Optional) Specify the <b>Repeat</b> frequency at which the firewall or Panorama must retrieve the list. By default the list is retrieved ever hour. 7. Click <b>OK</b> to save the changes.</p>

### Enforce Policy with a Dynamic Block List

<p><b>Step 3</b> Use the dynamic block list as a source or destination address object in policy.</p> <p> Create separate dynamic block lists if you want to specify allow and deny actions for specific IP addresses.</p> <p>The list can be referenced in any policy type. In this example, we attach it as a destination object in security policy.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b>.</li> <li>2. Click <b>Add</b> and give the rule a descriptive name in the <b>General</b> tab.</li> <li>3. In the <b>Source</b> tab, select the <b>Source Zone</b>.</li> <li>4. In the <b>Destination</b> tab, select the <b>Destination Zone</b> and select the dynamic block list as the Destination Address.</li> <li>5. In the <b>Service/ URL Category</b> tab, make sure the <b>Service</b> is set to <b>application-default</b>.</li> <li>6. In the <b>Actions</b> tab, set the <b>Action Setting</b> to Allow or Deny.</li> <li>7. Leave all the other options at the default values.</li> <li>8. Click <b>OK</b> to save the changes.</li> <li>9. <b>Commit</b> the changes.</li> </ol>
<p><b>Step 4</b> Test that the policy action is enforced.</p>	<ol style="list-style-type: none"> <li>1. Access a IP address that is included in the dynamic block list and verify that action you defined is enforced.</li> <li>2. Select <b>Monitor &gt; Logs &gt; Traffic</b> and see the log entry for the session.</li> <li>3. To verify the policy rule that matches a flow, use the following CLI command:</li> </ol> <pre>test security-policy-match source &lt;IP_address&gt; destination &lt;IP_address&gt; destination port &lt;port_number&gt; protocol &lt;protocol_number&gt;</pre>

### View the List of IP addresses in the Dynamic Block List

#### View the IP Addresses Included in the Dynamic Block List

To view the list of IP addresses that the firewall has retrieved from the web server enter the following CLI command:

**request system external-list show name <name>**

For example, for a list named case DBL\_2014, the output is:

vsys1/DBL\_2014:

```
Next update at: Wed Aug 27 16:00:00 2014
IPs:
1.1.1.1
1.2.2.2/20 #test China
192.168.255.0; test internal
192.168.254.0/24 test internal range
```

## Retrieve a Dynamic Block List from Web Server

The firewall or Panorama can be configured to retrieve the list from the web server on an hourly, daily, weekly, or monthly basis. If you have added or deleted IP addresses on the list and need to trigger an immediate refresh, you must use the Command Line Interface.

### Retrieve a Dynamic Block List

1. Enter the command: `request system external-list refresh name <name>`

For example, `request system external-list refresh name DBL_2014`

2. Get the job ID for the refresh job using the CLI command: `show jobs all`

Look for the last EBL Refresh job in the list.

3. View the details for the job ID. Use the command `show jobs id <number>`

A message indicating the success or failure displays. For example:

```
admin@PA-200> show jobs id 55
Enqueued          ID      Type    Status Result Completed
-----
2014/08/26 15:34:14      55    EBLRefresh     FIN      OK 15:34:40
Warnings:
Details:
```

## Register IP Addresses and Tags Dynamically

To mitigate the challenges of scale, lack of flexibility and performance, the architecture in networks today allows for clients, servers, and applications to be provisioned, changed, and deleted on demand. This agility poses a challenge for security administrators because they have limited visibility into the IP addresses of the dynamically provisioned clients and servers, and the plethora of applications that can be enabled on these virtual resources.

The firewall (hardware-based platforms and the VM-Series) supports the ability to register IP addresses and tags dynamically. The IP addresses and tags can be registered on the firewall directly or registered on the firewall through Panorama. This dynamic registration process can be enabled using any of the following options:

- **User-ID agent for Windows**—In an environment where you've deployed the User-ID agent, you can enable the User-ID agent to monitor up to 100 VMware ESXi and/or vCenter Servers. As you provision or modify virtual machines on these VMware servers, the agent can retrieve the IP address changes and share them with the firewall.
- **VM Information Sources**—Allows you to monitor VMware ESXi and vCenter Server, and the AWS-VPC to retrieve IP address changes when you provision or modify virtual machines on these sources. VM Information Sources polls for a predefined set of attributes and does not require external scripts to register the IP addresses through the XML API. See [Monitor Changes in the Virtual Environment](#).
- **VMware Service Manager** (only available for the integrated NSX solution)—The integrated NSX solution is designed for automated provisioning and distribution of Palo Alto Networks next-generation security services and the delivery of dynamic context-based security policies using Panorama. The NSX Manager updates Panorama with the latest information on the IP addresses and tags associated with the virtual machines deployed in this integrated solution. For information on this solution, see [Set Up a VM-Series NSX Edition Firewall](#).
- **XML API**—The firewall and Panorama support an XML API that uses standard HTTP requests to send and receive data. You can use this API to register IP addresses and tags with the firewall or Panorama. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports REST-based services. Refer to the [PAN-OS XML API Usage Guide](#) for details.

For information on creating and using Dynamic Address Groups, see [Use Dynamic Address Groups in Policy](#).

For the CLI commands for registering tags dynamically, see [CLI Commands for Dynamic IP Addresses and Tags](#).

## Monitor Changes in the Virtual Environment

To secure applications and prevent threats in an environment where new users and servers are constantly emerging, your security policy must be nimble. To be nimble, the firewall must be able to learn about new or modified IP addresses and consistently apply policy without requiring configuration changes on the firewall.

This capability is provided by the coordination between the **VM Information Sources** and **Dynamic Address Groups** features on the firewall. The firewall and Panorama provide an automated way to gather information on the virtual machine (or guest) inventory on each monitored source and create policy objects that stay in sync with the dynamic changes on the network.

- ▲ [Enable VM Monitoring to Track Changes on the Virtual Network](#)
- ▲ [Attributes Monitored in the AWS and VMware Environments](#)
- ▲ [Use Dynamic Address Groups in Policy](#)

## Enable VM Monitoring to Track Changes on the Virtual Network

VM information sources provides an automated way to gather information on the Virtual Machine (VM) inventory on each monitored source (host); the firewall can monitor the VMware ESXi and vCenter Server, and the AWS-VPC. As virtual machines (guests) are deployed or moved, the firewall collects a predefined set of attributes (or metadata elements) as tags; these tags can then be used to define Dynamic Address Groups (see [Use Dynamic Address Groups in Policy](#)) and matched against in policy.

Up to 10 VM information sources can be configured on the firewall or pushed using Panorama templates. By default, the traffic between the firewall and the monitored sources uses the management (MGT) port on the firewall.



**VM Information Sources** offers easy configuration and enables you to monitor a predefined set of 16 metadata elements or attributes. See [Attributes Monitored in the AWS and VMware Environments](#)for the list.

## Set up the VM Monitoring Agent

### Step 1 Enable the VM Monitoring Agent.



Up to 10 sources can be configured for each firewall, or for each virtual system on a multiple virtual systems capable firewall.

If your firewalls are configured in a high availability configuration:

- An active/passive setup, only the active firewall monitors the VM sources.
- An active/active setup, only the firewall with the priority value of primary monitors the VM sources.

1. Select **Device > VM Information Sources**.

2. Click **Add** and enter the following information:

- A **Name** to identify the VMware ESX(i) or vCenter Server that you want to monitor.
- Enter the **Host information for the server**—hostname or IP address and the **Port** on which it is listening.
- Select the **Type** to indicate whether the source is a **VMware ESX(i)** server or a **VMware vCenter** Server.
- Add the credentials (**Username** and **Password**) to authenticate to the server specified above.
- Use the credentials of an administrative user to enable access.
- (Optional) Modify the **Update interval** to a value between 5-600 seconds. By default, the firewall polls every 5 seconds. The API calls are queued and retrieved within every 60 seconds, so updates may take up to 60 seconds plus the configured polling interval.

VM Information Source Configuration	
Name	10.5.124.5
Host	10.5.124.5
Description	
Port	443
<input checked="" type="checkbox"/> Enabled	
Type	<input type="radio"/> VMware ESXi <input checked="" type="radio"/> VMware VCenter
Username	root
Password	*****
Confirm Password	*****
Update Interval (sec)	10
<input type="checkbox"/> Enable timeout when source is disconnected	
Timeout (hours)	2
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- (Optional) Enter the interval in hours when the connection to the monitored source is closed, if the host does not respond. (default: 2 hours, range 2-10 hours)  
To change the default value, select the check box to **Enable timeout when the source is disconnected** and specify the value. When the specified limit is reached or if the host cannot be accessed or does not respond, the firewall will close the connection to the source.
- Click **OK**, and **Commit** the changes.
- Verify that the connection **Status** displays as connected

**Set up the VM Monitoring Agent (Continued)**

**Step 2** Verify the connection status.

Verify that the connection **Status** displays as  connected.



If the connection status is pending or disconnected, verify that the source is operational and that the firewall is able to access the source. If you use a port other than the MGT port for communicating with the monitored source, you must change the service route (**Device > Setup > Services**, click the **Service Route Configuration** link and modify the **Source Interface** for the **VM Monitor** service).

## Attributes Monitored in the AWS and VMware Environments

Each VM on a monitored ESXi or vCenter server must have VMware Tools installed and running. VMware Tools provide the capability to glean the IP address(es) and other values assigned to each VM.

In order to collect the values assigned to the monitored VMs, the firewall monitors the following predefined set of attributes:

Attributes Monitored on a VMware Source	Attributes Monitored on the AWS-VPC
• UUID	• Architecture
• Name	• Guest OS
• Guest OS	• Image ID
• VM State — the power state can be poweredOff, poweredOn, standBy, and unknown.	• Instance ID
• Annotation	• Instance State
• Version	• Instance Type
• Network — Virtual Switch Name, Port Group Name, and VLAN ID	• Key Name
• Container Name —vCenter Name, Data Center Object Name, Resource Pool Name, Cluster Name, Host, Host IP address.	• Placement—Tenancy, Group Name, Availability Zone • Private DNS Name
	• Public DNS Name
	• Subnet ID
	• Tag (key, value) (up to 5 tags supported per instance)
	• VPC ID

## Use Dynamic Address Groups in Policy

Dynamic address groups are used in policy. They allow you to create policy that automatically adapts to changes—adds, moves, or deletions of servers. It also enables the flexibility to apply different rules to the same server based on *tags* that define its role on the network, the operating system, or the different kinds of traffic it processes.

A dynamic address group uses tags as a filtering criteria to determine its members. The filter uses logical *and* and *or* operators. All IP addresses or address groups that match the filtering criteria become members of the dynamic address group. Tags can be defined statically on the firewall and/or registered (dynamically) to the firewall. The difference between static and dynamic tags is that static tags are part of the configuration on the firewall, and dynamic tags are part of the runtime configuration. This implies that a commit is not required to update dynamic tags; the tags must however be used by Dynamic Address Groups that are referenced in policy, and the policy must be committed on the device.

To dynamically register tags, you can use the XML API or the VM Monitoring agent on the firewall or on the User-ID agent. Each tag is a metadata element or attribute-value pair that is registered on the firewall or Panorama. For example, IP1 {tag1, tag2,...,tag32}, where the IP address and the associated tags are maintained as a list; each registered IP address can have up to 32 tags such as the operating system, the datacenter or the virtual switch to which it belongs. Within 60 seconds of the API call, the firewall registers the IP address and associated tags, and automatically updates the membership information for the dynamic address group(s).

The maximum number of IP addresses that can be registered for each platform is different. Use the following table for specifics on your platform:

Platform	Maximum number of dynamically registered IP addresses
PA-7000 Series, PA-5060, VM-1000-HV	100,000
PA-5050	50,000
PA-5020	25,000
PA-4000 Series, PA-3000 Series	5,000
PA-2000 Series, PA-500, PA-200, VM-300, VM-200, VM-100	1,000

The following example shows how dynamic address groups can simplify network security enforcement. The example workflow shows how to:

- Enable the VM Monitoring agent on the firewall, to monitor the VMware ESX(i) host or vCenter Server and register VM IP addresses and the associated tags.
- Create dynamic address groups and define the tags to filter. In this example, two address groups are created. One that only filters for dynamic tags and another that filters for both static and dynamic tags to populate the members of the group.
- Validate that the members of the dynamic address group are populated on the firewall.
- Use dynamic address groups in policy. This example uses two different security policies:
  - A security policy for all Linux servers that are deployed as FTP servers; this rule matches on dynamically registered tags.

- A security policy for all Linux servers that are deployed as web servers; this rule matches on a dynamic address group that uses static and dynamic tags.
- Validate that the members of the dynamic address groups are updated as new FTP or web servers are deployed. This ensure that the security rules are enforced on these new virtual machines too.

### Use Dynamic Address Groups in Policy

**Step 1** Enable VM Source Monitoring.

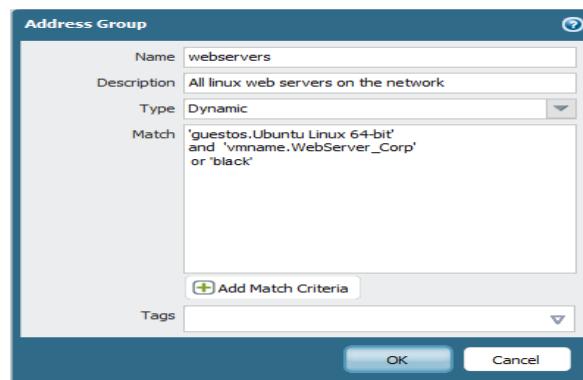
See [Enable VM Monitoring to Track Changes on the Virtual Network](#).

**Step 2** Create dynamic address groups on the firewall.



View the [tutorial](#) to see a big picture view of the feature.

1. Log in to the web interface of the firewall.
2. Select **Object > Address Groups**.
3. Click **Add** and enter a **Name** and a **Description** for the address group.
4. Select **Type** as **Dynamic**.
5. Define the match criteria. You can select dynamic and static tags as the match criteria to populate the members of the group. Click **Add Match Criteria**, and select the **And** or **Or** operator and select the attributes that you would like to filter for or match against. and then click **OK**.



6. Click **Commit**.

The match criteria for each dynamic address group in this example is as follows:

ftp\_server: matches on the guest operating system “Linux 64-bit” and annotated as “ftp” ('questos.Ubuntu Linux 64-bit' and 'annotation.ftp').

web-servers: matches on two criteria—the tag black or if the guest operating system is Linux 64-bit and the name of the server us Web\_server\_Corp. ('questos.Ubuntu Linux 64-bit' and 'vmname.WebServer\_Corp' or 'black')

Name	Location	Members Count	Addresses
ftp_servers		dynamic	more... ←
Web_servers		dynamic	more...

Click to see  
members/registered IP  
addresses

### Use Dynamic Address Groups in Policy (Continued)

**Step 3** Use dynamic address groups in policy.



View the [tutorial](#).

1. Select **Policies > Security**.
2. Click **Add** and enter a **Name** and a **Description** for the policy.
3. Add the **Source Zone** to specify the zone from which the traffic originates.
4. Add the **Destination Zone** at which the traffic is terminating.
5. For the **Destination Address**, select the Dynamic address group you created in **Step 2** above.
6. Specify the action—**Allow** or **Deny**—for the traffic, and optionally attach the default security profiles to the rule.
7. Repeats Steps 1 through 6 above to create another policy rule.
8. Click **Commit**.

This example shows how to create two policies: one for all access to FTP servers and the other for access to web servers.

Name	Tags	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action	Profile	Options
1. Access to web servers		any	any	any	any	pq untrust	Web_servers	any	application-d...	Allow	Profile A	Profile B
2. Access to FTP servers		any	any	any	any	pq untrust	ftp_servers	any	ftp	Allow	Profile C	Profile D

**Step 4** Validate that the members of the dynamic address group are populated on the firewall.

1. Select **Policies > Security**, and select the rule.
2. Select the drop-down arrow next to the address group link, and select **Inspect**. You can also verify that the match criteria is accurate.

3. Click the **more** link and verify that the list of registered IP addresses is displayed.

Address Groups - ftp_servers	
Address	Type
10.5.124.45	registered-ip
15.0.0.45	registered-ip
fe80::250:56ff:feb5:beaa	registered-ip
fe80::250:56ff:feb5:cee9	registered-ip

Policy will be enforced for all IP addresses that belong to this address group, and are displayed here.

## CLI Commands for Dynamic IP Addresses and Tags

The Command Line Interface on the firewall and Panorama give you a detailed view into the different sources from which tags and IP addresses are dynamically registered. It also allows you to audit registered and unregistered tags. The following examples illustrate the capabilities in the CLI.

Example	CLI Command
View all registered IP addresses that match the tag, <code>state.poweredOn</code> or that are not tagged as <code>vSwitch0</code>	<pre>show log iptag tag_name equal state.poweredOn show log iptag tag_name not-equal switch.vSwitch0</pre>
View all dynamically registered IP addresses that were sourced by VM Information Source with name <code>vmware1</code> and tagged as <code>poweredOn</code>	<pre>show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all  registered IP                                     Tags ----- fe80::20c:29ff:fe69:2f76      "state.poweredOn" 10.1.22.100                      "state.poweredOn" 2001:1890:12f2:11:20c:29ff:fe69:2f76 "state.poweredOn" fe80::20c:29ff:fe69:2f80      "state.poweredOn" 192.168.1.102                      "state.poweredOn" 10.1.22.105                      "state.poweredOn" 2001:1890:12f2:11:2cf8:77a9:5435:c0d "state.poweredOn" fe80::2cf8:77a9:5435:c0d       "state.poweredOn"</pre>
Clear all IP addresses and tags learned from a specific VM Monitoring source without disconnecting the source.	<pre>debug vm-monitor clear source-name &lt;name&gt;</pre>
Display IP addresses registered from all sources.	<pre>show object registered-ip all</pre>
Display the count for IP addresses registered from all sources.	<pre>show object registered-ip all option count</pre>
Clear IP addresses registered from all sources	<pre>debug object registered-ip clear all</pre>
Add or delete tags for a given IP address that was registered using the XML API.	<pre>debug object test registered-ip [&lt;register/unregister&gt;] &lt;ip/netmask&gt; &lt;tag&gt;</pre>

Example	CLI Command
View all tags registered from a specific information source.	<pre>show vm-monitor source source-name vmware1 tag all vlanId.4095 vswitch.vSwitch1 host-ip.10.1.5.22 portgroup.TOBUSED hostname.panserver22 portgroup.VM Network 2 datacenter.ha-datacenter vlanId.0 state.poweredOn vswitch.vSwitch0 vmname.Ubuntu22-100 vmname.win2k8-22-105 resource-pool.Resources vswitch.vSwitch2 guestos.Ubuntu Linux 32-bit guestos.Microsoft Windows Server 2008 32-bit annotation. version.vmx-08 portgroup.VM Network vm-info-source.vmware1 uuid.564d362c-11cd-b27f-271f-c361604dfad7 uuid.564dd337-677a-eb8d-47db-293bd6692f76 Total: 22</pre>
View all tags registered from a specific data source, for example from the VM Monitoring Agent on the firewall, the XML API, Windows User-ID Agent or the CLI.	<ul style="list-style-type: none"> <li>To view tags registered from the CLI:  <code>show log iptag datasource_type equal unknown</code></li> <li>To view tags registered from the XML API:  <code>show log iptag datasource_type equal xml-api</code></li> <li>To view tags registered from VM Information sources:  <code>show log iptag datasource_type equal vm-monitor</code></li> <li>To view tags registered from the Windows User-ID agent:  <code>show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent</code></li> </ul>
View all tags that are registered for a specific IP address (across all sources).	<code>debug object registered-ip show tag-source ip ip_address tag all</code>

## Identify Users Connected through a Proxy Server

If you have a proxy server deployed between the users on your network and the firewall, in HTTP/HTTPS requests the firewall might see the proxy server IP address as the source IP address in the traffic that the proxy forwards rather than the IP address of the client that requested the content. In many cases, the proxy server adds an X-Forwarded-For (XFF) header to traffic packets that includes the actual IPv4 or IPv6 address of the client that requested the content or from whom the request originated. In such cases, you can configure the firewall to read the XFF header values and determine the IP addresses of the client who requested the content. The firewall matches the XFF IP addresses with usernames that your policy rules reference so that those rules can control access for the associated users and groups. The firewall also uses the XFF-derived usernames to populate the source user fields of logs so you can monitor user access to web services.

You can also configure the firewall to add XFF values to URL Filtering logs. In these logs, an XFF value can be the client IP address, client username (if available), the IP address of the last proxy server traversed in a proxy chain, or any string of up to 128 characters that the XFF header stores.

XFF user identification applies only to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header. If the header has an invalid IP address, the firewall uses that IP address as a username for group mapping references in policies. If the XFF header has multiple IP addresses, the firewall uses the first entry from the left.

- ▲ [Use XFF Values for Policies and Logging Source Users](#)
- ▲ [Add XFF Values to URL Filtering Logs](#)

### Use XFF Values for Policies and Logging Source Users

You can configure the firewall to use XFF values in user-based policies and in the source user fields of logs. To use XFF values in policies, you must also [Map IP Addresses to Users](#), [Map Users to Groups](#) (if you have group-based policies), and [configure policies](#) based on users or groups.



Logging XFF values doesn't populate the source IP address values of logs. When you view the logs, the source field displays the IP address of the proxy server if one is deployed between the user clients and the firewall. However, you can configure the firewall to [Add XFF Values to URL Filtering Logs](#) so that you can see user IP addresses in those logs.

To ensure that attackers can't read and exploit the XFF values in web request packets that exit the firewall to retrieve content from an external server, you can also configure the firewall to strip the XFF values from outgoing packets.

These options are not mutually exclusive: if you configure both, the firewall zeroes out XFF values only after using them in policies and logs.

#### Use XFF Values for Policies and Logging Source Users

<b>Step 1</b>	Enable the firewall to use XFF values in policies and in the source user fields of logs.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Content-ID</b> and edit the X-Forwarded-For Headers settings.</li><li>2. Select the <b>Use X-Forwarded-For Header in User-ID</b> check box.</li></ol>
<b>Step 2</b>	Remove XFF values from outgoing web requests.	<ol style="list-style-type: none"><li>1. Select the <b>Strip X-Forwarded-For Header</b> check box.</li><li>2. Click <b>OK</b> and <b>Commit</b>.</li></ol>

### Use XFF Values for Policies and Logging Source Users (Continued)

<b>Step 3</b> Verify the firewall is populating the source user fields of logs.	<ol style="list-style-type: none"> <li>Select a log type that has a source user field (for example, <b>Monitor &gt; Logs &gt; Traffic</b>).</li> <li>Verify that the Source User column displays the usernames of users who access the web.</li> </ol>
---	--

## Add XFF Values to URL Filtering Logs

You can configure the firewall to add the XFF values from web requests to URL Filtering logs. The XFF values that the logs display can be client IP addresses, usernames if available, or any values of up to 128 characters that the XFF fields store.



This method of logging XFF values doesn't add usernames to the source user fields in URL Filtering logs. To populate the source user fields, see [Use XFF Values for Policies and Logging Source Users](#).

### Add XFF Values to URL Filtering Logs

<b>Step 1</b> Configure a URL Filtering profile.	<ol style="list-style-type: none"> <li>Select <b>Objects &gt; Security Profiles &gt; URL Filtering</b>.</li> <li>Select an existing profile or <b>Add</b> a new profile and enter a descriptive <b>Name</b>.   You can't enable XFF logging in the default URL Filtering profile.           </li> <li>In the <b>Categories</b> tab, <a href="#">Define how to control access to web content</a>.</li> <li>Select the <b>Settings</b> tab and select the <b>X-Forwarded-For</b> check box.</li> <li>Click <b>OK</b> to save the profile.</li> </ol>
<b>Step 2</b> Attach the URL Filtering profile to a policy rule.	<ol style="list-style-type: none"> <li>Select <b>Policies &gt; Security</b> and click the rule.</li> <li>Select the <b>Actions</b> tab, set the <b>Profile Type</b> to <b>Profiles</b>, and select the <b>URL Filtering</b> profile you just created.</li> <li>Click <b>OK</b> and <b>Commit</b>.</li> </ol>
<b>Step 3</b> Verify the firewall is logging XFF values.	<ol style="list-style-type: none"> <li>Select <b>Monitor &gt; Logs &gt; URL Filtering</b>.</li> <li>Display the XFF values in one of the following ways:           <ul style="list-style-type: none"> <li>To display the XFF value for a single log—Click the  icon for the log to displays its details. The HTTP Headers section displays the X-Forwarded-For value.</li> <li>To display the XFF values for all logs—Open the drop-down in any column header, select <b>Columns</b>, and select the <b>X-Forwarded-For</b> check box. The page then displays an X-Forwarded-For column.</li> </ul> </li> </ol>

## Policy-Based Forwarding

Normally, the firewall uses the destination IP address in a packet to determine the outgoing interface. The firewall uses the routing table associated with the virtual router to which the interface is connected to perform the route lookup. Policy-Based Forwarding (PBF) allows you to override the routing table, and specify the outgoing or *egress* interface based on specific parameters such as source or destination IP address, or type of traffic.

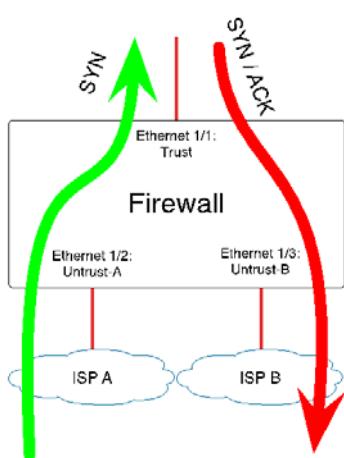
- ▲ PBF
- ▲ Create a Policy-Based Forwarding Rule
- ▲ Use Case: PBF for Outbound Access with Dual ISPs

## PBF

PBF rules allow traffic to take an alternative path from the next hop specified in the route table, and are typically used to specify an egress interface for security or performance reasons. Let's say your company has two links between the corporate office and the branch office: a cheaper Internet link and a more expensive leased line. The leased line is a high-bandwidth, low-latency link. For enhanced security, you can use PBF to send applications that aren't encrypted traffic, such as FTP traffic, over the private leased line and all other traffic over the Internet link. Or, for performance, you can choose to route business-critical applications over the leased line while sending all other traffic, such as web browsing, over the cheaper link.

## Egress Path and Symmetric Return

Using PBF, you can direct traffic to a specific interface on the firewall, drop the traffic, or direct traffic to another virtual system (on systems enabled for multiple virtual systems).



In networks with asymmetric routes, such as in a dual ISP environment, connectivity issues occur when traffic arrives at one interface on the firewall and leaves from another interface. If the route is asymmetrical, where the forward (SYN packet) and return (SYN/ACK) paths are different, the firewall is unable to track the state of the entire session and this causes a connection failure. To ensure that the traffic uses a symmetrical path, which means that the traffic arrives at and leaves from the same interface on which the session was created, you can enable the *Symmetric Return* option.

With symmetric return, the virtual router overrides a routing lookup for return traffic and instead directs the flow back to the MAC address from which it received the SYN packet (or first packet). However, if the destination IP address is on the same subnet as the ingress/egress interface's IP address, a route lookup is performed and symmetric return is not enforced. This behavior prevents traffic from being blackholed.



To determine the next hop for symmetric returns, the firewall uses an Address Resolution Protocol (ARP) table. The maximum number of entries that this ARP table supports is limited by the firewall model and the value is not user configurable. To determine the limit for your model, use the CLI command: `show pbf return-mac all`.

## Path Monitoring

Path monitoring allows you to verify connectivity to an IP address so that the firewall can direct traffic through an alternate route, when needed. The firewall uses ICMP pings as *heartbeats* to verify that the specified IP address is reachable.

A monitoring profile allows you to specify the threshold number of heartbeats to determine whether the IP address is reachable. When the monitored IP address is unreachable, you can either disable the PBF rule or specify a *fail-over* or *wait-recover* action. Disabling the PBF rule allows the virtual router to take over the routing

decisions. When the fail-over or wait-recover action is taken, the monitoring profile continues to monitor whether the target IP address is reachable, and when it comes back up, the firewall reverts back to using the original route.

The following table lists the difference in behavior for a path monitoring failure on a new session versus an established session.

Behavior of a session on a monitoring failure	If the rule stays enabled when the monitored IP address is unreachable	If rule is disabled when the monitored IP address is unreachable
For an established session	<input type="checkbox"/> Disable this rule if nexthop/monitor ip is unreachable	<input checked="" type="checkbox"/> Disable this rule if nexthop/monitor ip is unreachable
	<b>wait-recover</b> —Continue to use egress interface specified in the PBF rule  <b>fail-over</b> —Use path determined by routing table (no PBF)	<b>wait-recover</b> —Continue to use egress interface specified in the PBF rule  <b>fail-over</b> —Use path determined by routing table (no PBF)
For a new session	<b>wait-recover</b> —Use path determined by routing table (no PBF)	<b>wait-recover</b> —Check the remaining PBF rules. If no match, use the routing table
	<b>fail-over</b> —Use path determined by routing table (no PBF)	<b>fail-over</b> —Check the remaining PBF rules. If no match, use the routing table

## Service Versus Applications in PBF

PBF rules are applied either on the first packet (SYN) or the first response to the first packet (SYN/ACK). This means that a PBF rule may be applied before the firewall has enough information to determine the application. Therefore, application-specific rules are not recommended for use with PBF. Whenever possible, use a service object, which is the Layer 4 port (TCP or UDP) used by the protocol or application.

However, if you specify an application in a PBF rule, the firewall performs *App-ID caching*. When an application passes through the firewall for the first time, the firewall does not have enough information to identify the application and therefore cannot enforce the PBF rule. As more packets arrive, the firewall determines the application and creates an entry in the App-ID cache and retains this App-ID for the session. When a new session is created with the same destination IP address, destination port, and protocol ID, the firewall could identify the application as the same from the initial session (based on the App-ID cache) and apply the PBF rule. Therefore, a session that is not an exact match and is not the same application, can be forwarded based on the PBF rule.

Further, applications have dependencies and the identity of the application can change as the firewall receives more packets. Because PBF makes a routing decision at the start of a session, the firewall cannot enforce a change in application identity. YouTube, for example, starts as web-browsing but changes to Flash, RTSP, or YouTube based on the different links and videos included on the page. However with PBF, because the firewall identifies the application as web-browsing at the start of the session, the change in application is not recognized thereafter.



You cannot use custom-applications, application-filters or application groups in PBF rules.

## Create a Policy-Based Forwarding Rule

Use a **PBF** rule to direct traffic to a specific egress interface on the firewall, and override the default path for the traffic.

### Create a PBF Rule

#### Step 1 Create a PBF rule.

When creating a PBF rule you must specify a name for the rule, a source zone or interface, and an egress interface. All other components are either optional or have a default value provided.



You can specify the source and destination addresses using an IP address, an address object, or a FQDN. For the next hop, however, you must specify an IP address.

1. Select **Policies > Policy Based Forwarding** and click **Add**.

2. Give the rule a descriptive name in the **General** tab.

3. In the **Source** tab, select the following:

- a. Select the **Type—Zone or Interface**—to which the forwarding policy will be applied, and the relevant zone or interface. If you have an asymmetric routing environment and want to enforce symmetric return, you must select a source interface.



PBF is only supported on Layer 3 interfaces; loopback interfaces do not support PBF.

- b. (Optional) Specify the **Source Address** to which PBF will apply. For example, a specific IP address or subnet IP address from which you want to forward traffic to the interface or zone specified in this rule.



Use the **Negate** option to exclude a one or more source IP addresses from the PBF rule. For example, if your PBF rule directs all traffic from the specified zone to the Internet, **Negate** allows you to exclude internal IP addresses from the PBF rule.

The evaluation order is top down. A packet is matched against the first rule that meets the defined criteria; after a match is triggered the subsequent rules are not evaluated.

- c. (Optional) Add and select the **Source User** or groups of users to whom the policy applies.

4. In the **Destination/Application/Service** tab, select the following:

- a. **Destination Address.** By default the rule applies to **Any IP address**. Use the **Negate** option to exclude one or more destination IP addresses from the PBF rule.

- b. Select the Application(s) or Service(s) that you want to control using PBF.



Application-specific rules are not recommended for use with PBF. Whenever possible, use a service object, which is the Layer 4 port (TCP or UDP) used by the protocol or application. For more details, see [Service Versus Applications in PBF](#).

## Create a PBF Rule

### Step 2 Define the forwarding rules.



If you are [configuring PBF in a multi-VSYS environment](#), you must create separate PBF rules for each virtual system (and create the appropriate Security policy rules to enable the traffic).

### 5. In the **Forwarding** tab, select the following:

- Set the **Action**. The options are as follows:
  - **Forward**—Directs the packet to a specific **Egress Interface**. Enter the **Next Hop** IP address for the packet (you cannot use an FQDN for the next hop).
  - **Forward To VSYS**—(On a device enabled for multiple virtual systems) Select the virtual system to which to forward the packet.
  - **Discard**—Drop the packet.
  - **No PBF**—Exclude the packets that match the criteria for source/destination/application/service defined in the rule. Matching packets use the route table instead of PBF; the firewall uses the route table to exclude the matched traffic from the redirected port.

To trigger the specified action at a daily, weekly or non-recurring frequency, create and attach a **Schedule**.

- (Optional) Enable Monitoring to verify connectivity to a target IP address or to the next hop IP address. Select **Monitor** and attach a monitoring **Profile** (default or custom) that specifies the action when the IP address is unreachable.
- (Optional, required for asymmetric routing environments) Select **Enforce Symmetric Return** and enter one or more IP addresses in the **Next Hop Address List** (you cannot use an FQDN as the next hop). You can add up to 8 next-hop addresses per rule; tunnel and PPoE interfaces are not available as a next-hop IP address

Enabling symmetric return ensures that return traffic (say, from the Trust zone on the LAN to the Internet) is forwarded out through the same interface through which traffic ingresses from the Internet.

### Step 3 Save the policies to the running configuration on the device.

Click **Commit**.

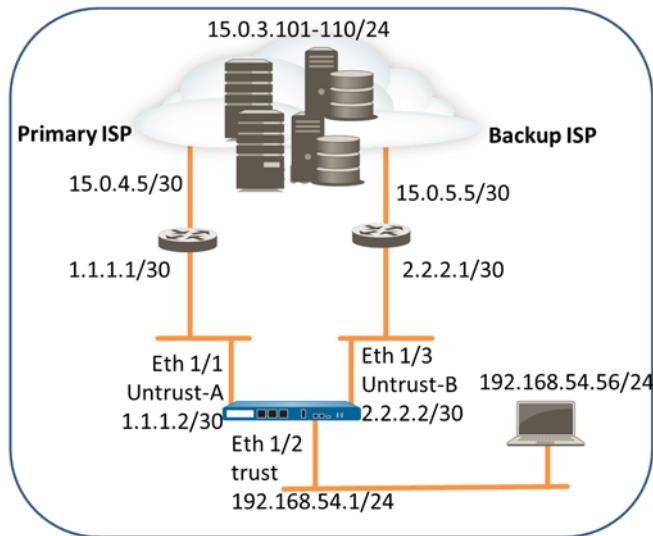
The PBF rule is in effect.

	Source		Destination				Forwarding			Monitoring				
	Name	Zone/Interface	Address	Address	Application	Service	Action	Egress I/F	Next Hop	Enforce Symmetric Return	Profile	Target	Disable If Unreachable	Schedule
1	HTTP to ISP-B		any		any		forward	ethernet1/4	10.3.4.54	false	default	none	false	none

## Use Case: PBF for Outbound Access with Dual ISPs

In this use case, the branch office has a dual ISP configuration and implements PBF for redundant Internet access. The backup ISP is the default route for traffic from the client to the web servers. In order to enable redundant Internet access without using an internetwork protocol such as BGP, we use PBF with destination interface-based source NAT and static routes, and configure the firewall as follows:

- Enable a PBF rule that routes traffic through the primary ISP, and attach a monitoring profile to the rule. The monitoring profile triggers the firewall to use the default route through the backup ISP when the primary ISP is unavailable.
- Define Source NAT rules for both the primary and backup ISP that instruct the firewall to use the source IP address associated with the egress interface for the corresponding ISP. This ensures that the outbound traffic has the correct source IP address.
- Add a static route to the backup ISP, so that when the primary ISP is unavailable, the default route comes into effect and the traffic is directed through the backup ISP.



### PBF for Outbound Access with Dual ISPs

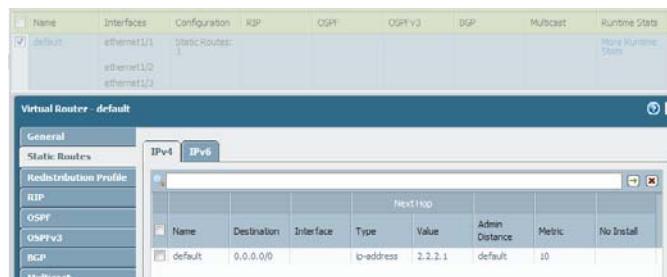
- Step 1** Configure the ingress and the egress interfaces on the firewall.

Egress interfaces can be in the same zone. In this example we assign the egress interfaces to different zones.

- Select **Network > Interfaces** and then select the interface you want to configure, for example, Ethernet1/1 and Ethernet1/3. The interface configuration on the firewall used in this example is as follows:
  - Ethernet 1/1 connected to the primary ISP:
    - Zone: ISP-East
    - IP Address:1.1.1.2/30
    - Virtual Router: Default
  - Ethernet 1/3 connected to the backup ISP:
    - Zone: ISP-West
    - IP Address:2.2.2.2/30
    - Virtual Router: Default
  - Ethernet 1/2 is the ingress interface, used by the network clients to connect to the Internet:
    - Zone: Trust
    - IP Address:192.168.54.1/24
    - Virtual Router: Default
- To save the interface configuration, click **OK**.

- Step 2** On the virtual router, add a static route to the backup ISP.

- Select **Network > Virtual Router** and then select the **default** link to open the Virtual Router dialog.
- Select the **Static Routes** tab and click **Add**. Enter a **Name** for the route and specify the **Destination** IP address for which you are defining the static route. In this example, we use 0.0.0.0/0 for all traffic.
- Select the **IP Address** radio button and set the **Next Hop** IP address (you cannot use an FQDN) for your router that connects to the backup Internet gateway. In this example, 2.2.2.1.
- Specify a cost metric for the route. In this example, we use 10.



5. Click **OK** twice to save the virtual router configuration.

### PBF for Outbound Access with Dual ISPs

**Step 3** Create a PBF rule that directs traffic to the interface that is connected to the primary ISP.

Make sure to exclude traffic destined to internal servers/IP addresses from PBF. Define a negate rule so that traffic destined to internal IP addresses is not routed through the egress interface defined in the PBF rule.

1. Select **Policies > Policy Based Forwarding** and click **Add**.
2. Give the rule a descriptive **Name** in the **General** tab.
3. In the **Source** tab, set the **Source Zone** to Trust.
4. In the **Destination/Application/Service** tab, set the following:
  - a. In the Destination Address section, **Add** the IP addresses or address range for servers on the internal network or create an address object for your internal servers. Select **Negate** to exclude the IP addresses or address object listed above from using this rule.
  - b. In the Service section, **Add** the **service-http** and **service-https** services to allow HTTP and HTTPS traffic to use the default ports. For all other traffic that is allowed by security policy, the default route will be used.



To forward all traffic using PBF, set the Service to **Any**.

5. In the **Forwarding** tab, specify the interface to which you want to forward traffic and enable path monitoring.
  - a. To forward traffic, set the **Action** to **Forward**, and select the **Egress Interface** and specify the **Next Hop**. In this example, the egress interface is **ethernet1/1**, and the next hop IP address is **1.1.1.1**.

### PBF for Outbound Access with Dual ISPs

- b. Enable **Monitor** and attach the default monitoring profile, to trigger a failover to the backup ISP. In this example, we do not specify a target IP address to monitor. The firewall will monitor the next hop IP address; if this IP address is unreachable the firewall will direct traffic to the default route specified on the virtual router.
- c. (Required if you have asymmetric routes). Select **Enforce Symmetric Return** to ensure that return traffic from the Trust zone to the Internet is forwarded out on the same interface through which traffic ingressed from the Internet. NAT ensures that the traffic from the Internet is returned to the correct interface/IP address on the firewall.
- d. Click **OK** to save the changes.

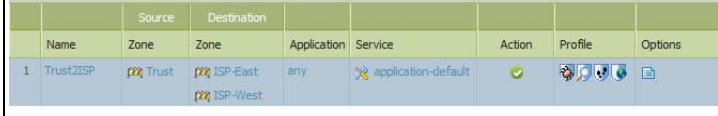
		Source	Destination			Forwarding		Monitoring		
	Name	Zone/Interface	Address	Service	Action	Egress I/F	Enforce Symmetric Return	Profile	Target	Disable If Unreachable
1	Use ISP-Primary	Trust	Internal servers	service-http service-https	forward	ethernet1/1	false	default	1.1.1.2	true

### PBF for Outbound Access with Dual ISPs

- Step 4** Create NAT rules based on the egress interface and ISP. These rules ensure that the correct source IP address is used for outbound connections.
1. Select **Policies > NAT** and click **Add**.
  2. In this example, the NAT rule we create for each ISP is as follows:
- NAT for Primary ISP**
- In the **Original Packet** tab,
- **Source Zone:** Trust
  - **Destination Zone:** ISP-West
- In the **Translated Packet** tab, under Source Address Translation
- **Translation Type:** Dynamic IP and Port
  - **Address Type:** Interface Address
  - **Interface:** ethernet1/1
  - **IP Address:** 1.1.1.2/30
- NAT for Backup ISP**
- In the **Original Packet** tab,
- **Source Zone:** Trust
  - **Destination Zone:** ISP-East
- In the **Translated Packet** tab, under Source Address Translation
- **Translation Type:** Dynamic IP and Port
  - **Address Type:** Interface Address
  - **Interface:** ethernet1/3
  - **IP Address:** 2.2.2.2/30

	Name	Original Packet					Translated Packet Source Translation
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	
1	NAT-Primary ISP	Trust	ISP-West	any	any	any	dynamic-ip-and-port ethernet1/1 1.1.1.2/30
2	NAT-Backup ISP	Trust	ISP-East	any	any	any	dynamic-ip-and-port ethernet1/3 2.2.2.2/30

### PBF for Outbound Access with Dual ISPs

<p><b>Step 5</b> Create security policy to allow outbound access to the Internet.</p>	<p>To safely enable applications, create a simple rule that allows access to the Internet and attach the security profiles available on the firewall.</p> <ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security</b> and click <b>Add</b>.</li> <li>2. Give the rule a descriptive <b>Name</b> in the <b>General</b> tab.</li> <li>3. In the <b>Source</b> tab, set the <b>Source Zone</b> to Trust.</li> <li>4. In the <b>Destination</b> tab, Set the <b>Destination Zone</b> to ISP-East and ISP-West.</li> <li>5. In the <b>Service/ URL Category</b> tab, leave the default <b>application-default</b>.</li> <li>6. In the <b>Actions</b> tab, complete these tasks:             <ol style="list-style-type: none"> <li>a. Set the <b>Action Setting</b> to <b>Allow</b>.</li> <li>b. Attach the default profiles for antivirus, anti-spyware, vulnerability protection and URL filtering, under <b>Profile Setting</b>.</li> </ol> </li> <li>7. Under <b>Options</b>, verify that logging is enabled at the end of a session. Only traffic that matches a security rule is logged.</li> </ol> 
<p><b>Step 6</b> Save the policies to the running configuration on the device.</p>	<p>Click <b>Commit</b>.</p>

**PBF for Outbound Access with Dual ISPs**

- Step 7** Verify that the PBF rule is active and that the primary ISP is used for Internet access.

- Launch a web browser and access a web server. On the firewall check the traffic log for web-browsing activity.

Traffic is sent through the interface attached to the primary ISP.

Traffic on port 80 is identified as web-browsing.

The security policy that allows the traffic.

	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Bytes
	11/05 08:24:04	end	Trust	ISP-West	192.168.54.56	204.79.197.200	80	web-browsing	allow	Trust2ISP	3.71

- From a client on the network, use the ping utility to verify connectivity to a web server on the Internet. and check the traffic log on the firewall.

```
C:\Users\pm-user1>ping 4.2.2.1
Pinging 4.2.2.1 with 32 bytes of data:
Reply from 4.2.2.1: bytes=32 time=34ms TTL=117
Reply from 4.2.2.1: bytes=32 time=13ms TTL=117
Reply from 4.2.2.1: bytes=32 time=25ms TTL=117
Reply from 4.2.2.1: bytes=32 time=3ms TTL=117
Ping statistics for 4.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 34ms, Average = 18ms
```

As defined by the PBF rule, only traffic on ports 80 or 443 use the Primary ISP; hence ping is sent through the interface attached to the backup ISP.

The security policy that allows the traffic.

	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	11/05 09:03:03	end	Trust	ISP-East	192.168.54.56	4.2.2.1	0	ping	allow	Trust2ISP

- To confirm that the PBF rule is active, use the CLI command **show pbf rule all**

```
admin@PA-NGFW> show pbf rule all
Rule      ID      Rule State Action   Egress IF/VSYS  NextHop
=====  ===  =====  =====  =====  =====  =====
Use ISP-Pr 1  Active  Forward  ethernet1/1  1.1.1.1
```

- Step 8** Verify that the failover to the backup ISP occurs and that the Source NAT is correctly applied.

- Unplug the connection to the primary ISP.

- Confirm that the PBF rule is inactive with the CLI command **show pbf rule all**

```
admin@PA-NGFW> show pbf rule all
Rule      ID      Rule State Action   Egress IF/VSYS  NextHop
=====  ===  =====  =====  =====  =====  =====
Use ISP-Pr 1  Disabled  Forward  ethernet1/1  1.1.1.1
```

- Access a web server, and check the traffic log to verify that traffic is being forwarded through the backup ISP.

Traffic is sent through the interface attached to the backup ISP.

The security policy that allows the traffic.

	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
	11/05 09:50:44	end	Trust	ISP-East	192.168.54.56	204.79.197.200	443	ssl	allow	Trust2ISP
	11/05 09:50:44	end	Trust	ISP-East	192.168.54.56	204.79.197.200	80	web-browsing	allow	Trust2ISP

### PBF for Outbound Access with Dual ISPs

4. View the session details to confirm that the NAT rule is working properly.

```
admin@PA-NGFW> show session all
-----
ID Application State Type Flag Src[Sport]/Zone/Proto
(translated IP[Port]) Vsys Dst[Dport]/Zone (translated
IP[Port])
87212 ssl ACTIVE FLOW NS 192.168.54.56[53236]/Trust/6
(2.2.2.2[12896]) vsys1 204.79.197.200[443]/ISP-East
(204.79.197.200[443])
```

5. Obtain the session identification number from the output and view the session details. Note that the PBF rule is not used and hence is not listed in the output.

```
admin@PA-NGFW> show session id 87212
Session 87212
c2s flow:
    source: 192.168.54.56 [Trust]
    dst: 204.79.197.200
    proto: 6
    sport: 53236 dport: 443
    state: ACTIVE type: FLOW
    src user: unknown
    dst user: unknown

s2c flow:
    source: 204.79.197.200 [ISP-East]
    dst: 2.2.2.2
    proto: 6
    sport: 443 dport: 12896
    state: ACTIVE type: FLOW
    src user: unknown
    dst user: unknown
start time : Wed Nov5 11:16:10 2014
    timeout : 1800 sec
    time to live : 1757 sec
    total byte count(c2s) : 1918
    total byte count(s2c) : 4333
    layer7 packet count(c2s) : 10
    layer7 packet count(s2c) : 7
    vsys : vsys1
    application : ssl
    rule : Trust2ISP
    session to be logged at end : True
    session in session ager : True
    session synced from HA peer : False
    address/port translation : source
nat-rule : NAT-Backup ISP(vsys1)
    layer7 processing : enabled
    URL filtering enabled : True
    URL category : search-engines
    session via syn-cookies : False
    session terminated on host : False
    session traverses tunnel : False
    captive portal session : False
    ingress interface : ethernet1/2
    egress interface : ethernet1/3
    session QoS rule : N/A (class 4)
```

## DoS Protection Against Flooding of New Sessions

The following topics describe how to configure DoS protection to better block IP addresses in order to handle high-volume attacks more efficiently.

- ▲ [DoS Protection Against Flooding of New Sessions](#)
- ▲ [Configure DoS Protection Against Flooding of New Sessions](#)
- ▲ [Use the CLI to End a Single Attacking Session](#)
- ▲ [Identify Sessions That Use an Excessive Percentage of the Packet Buffer](#)
- ▲ [Discard a Session Without a Commit](#)

## DoS Protection Against Flooding of New Sessions

DoS protection against flooding of new sessions is beneficial against high-volume single-session and multiple-session attacks. In a single-session attack, an attacker uses a single session to target a device behind the firewall. If a Security rule allows the traffic, the session is established and the attacker initiates an attack by sending packets at a very high rate with the same source IP address and port number, destination IP address and port number, and protocol, trying to overwhelm the target. In a multiple-session attack, an attacker uses multiple sessions (or connections per second [cps]) from a single host to launch a DoS attack.



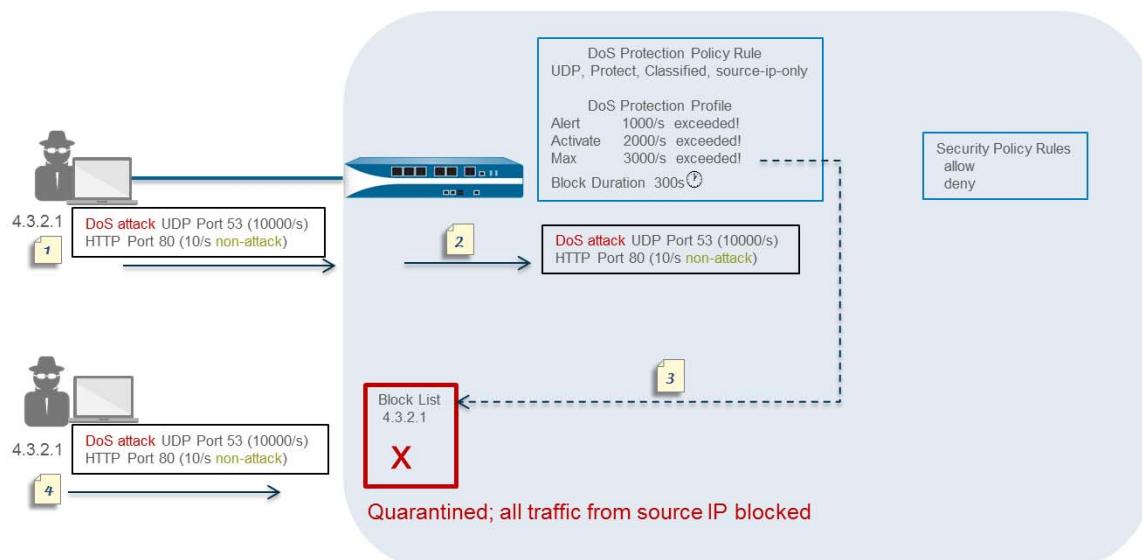
This feature defends only against DoS attacks of new sessions, that is, traffic that has not been offloaded to hardware. An offloaded attack is not protected by this feature. However, this topic describes how you can create a Security policy rule to reset the client; the attacker reinitiates the attack with numerous connections per second and is blocked by the defenses illustrated in this topic.

- ▲ [Multiple-Session DoS Attack](#)
- ▲ [Single-Session DoS Attack](#)

### Multiple-Session DoS Attack

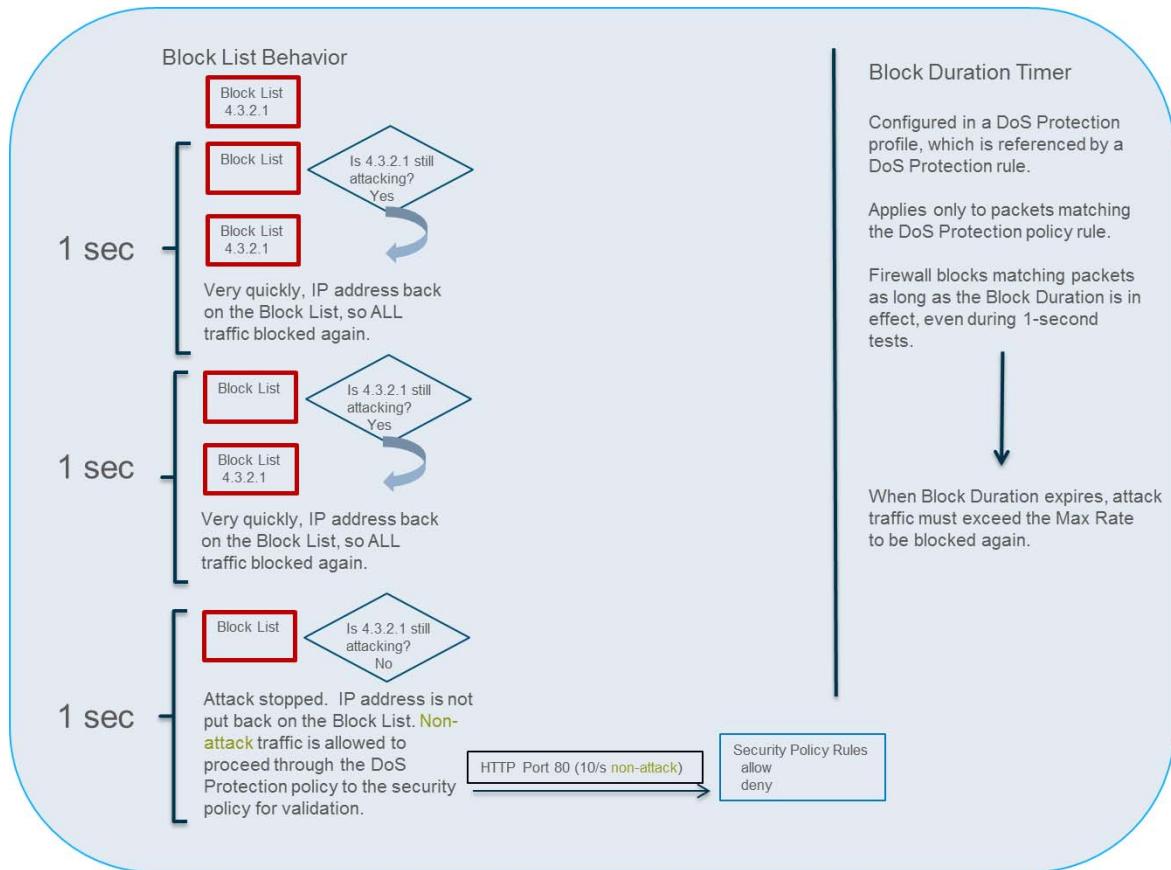
Configure DoS Protection Against Flooding of New Sessions by configuring a DoS Protection policy rule, which determines the criteria that, when matched by incoming packets, trigger the protect action. The DoS Protection profile counts each new connection toward the Alarm Rate, Activate Rate, and Max Rate thresholds. When the incoming new connections per second exceed the Max Rate allowed, the firewall takes the action specified in the DoS Protection policy rule.

The following figure and table describe how the Security policy rules, DoS Protection policy rules and profile work together in an example.



Sequence of Events as Firewall Quarantines an IP Address	
 1	In this example, an attacker launches a DoS attack at a rate of 10,000 new connections per second to UDP port 53. The attacker also sends 10 new connections per second to HTTP port 80.
 2	The new connections match criteria in the DoS Protection policy rule, such as a source zone or interface, source IP address, destination zone or interface, destination IP address, or a service, among other settings. In this example, the policy rule specifies UDP. The DoS rule also specifies the Protect action and Classified, two settings that dynamically put the DoS Protection Profile settings into effect. The DoS Protection Profile specifies that a Max Rate of 3000 packets per second is allowed. When incoming packets match the DoS rule, new connections per second are counted toward the Alert, Activate, and Max Rate thresholds.  You can also use a Security policy rule to block all traffic from the source IP address if you deem that address to be malicious all the time.
 3	The 10,000 new connections per second exceed the Max Rate threshold. When all of the following occur: <ul style="list-style-type: none"><li>• the threshold is exceeded,</li><li>• a Block Duration is specified, and</li><li>• Classified is set to includes source IP address,</li></ul> the firewall puts the offending source IP address on the block list.
 4	An IP address on the block list is in quarantine, meaning all traffic from that IP address is blocked. The firewall blocks the offending source IP address before additional attack packets reach the Security policy.

The following figure describes in more detail what happens after an IP address that matches the DoS Protection policy rule is put on the block list. It also describes the Block Duration timer.



Every one second, the firewall allows the IP address to come off the Block List so that the firewall can test the traffic patterns and determine if the attack is ongoing. The firewall takes the following action:

- During this one-second test period, the firewall allows packets that do not match the DoS Protection policy criteria (HTTP traffic in this example) through the DoS Protection policy rules to the Security policy for validation. Very few packets, if any, have time to get through because the first attack packet that the firewall receives after the IP address is let off the Block List will match the DoS Protection policy criteria, quickly causing the IP address to be placed back on the block list for another second. The firewall repeats this test each second until the attack stops.
- The firewall blocks all attack traffic from going past the DoS Protection policy rules until the Block Duration expires.

When the attack stops, the firewall does not put the IP address back on the block list. The firewall allows non-attack traffic to proceed through the DoS Protection policy rules to the Security policy rules for validation. You must configure a Security policy rule because without one, an implicit deny rule denies all traffic.

The block list is based on a source zone and source address combination. This behavior allows duplicate IP addresses to exist as long as they are in different zones belonging to separate virtual routers.

The Block Duration setting in a DoS Protection profile specifies how long the firewall blocks the [offending] packets that exactly match a DoS Protection policy rule. The attack traffic remains blocked until the Block Duration expires, after which the attack traffic must again exceed the Max Rate threshold to be blocked again.



If the attacker uses multiple sessions or bots that initiate multiple attack sessions, the sessions count toward the thresholds in the DoS Protection profile without a Security policy deny rule in place. Hence, a single-session attack requires a Security policy deny rule in order for each packet to count toward the thresholds; a multiple-session attack does not.

Therefore, the DoS protection against flooding of new sessions allows the firewall to efficiently defend against a source IP address while attack traffic is ongoing and to permit non-attack traffic to pass as soon as the attack stops. Putting the offending IP address on the block list allows the DoS protection functionality to take advantage of the block list, which is designed to quarantine all activity. Quarantining the IP address from all activity protects against a modern attacker who attempts a rotating application attack, in which the attacker simply changes applications to start a new attack or uses a combination of different attacks in a hybrid DoS attack.



Beginning with PAN-OS 7.0.2, it is a change in behavior that the firewall places the attacking source IP address on the block list. When the attack stops, non-attack traffic is allowed to proceed to the Security policy rules. The attack traffic that matched the DoS Protection profile and DoS Protection policy rules remains blocked until the Block Duration expires.

## Single-Session DoS Attack

A single-session DoS attack typically will not trigger Zone or DoS Protection profiles because they are attacks that are formed after the session is created. These attacks are allowed by the Security policy because a session is allowed to be created, and after the session is created, the attack drives up the packet volume and takes down the target device.

[Configure DoS Protection Against Flooding of New Sessions](#) to protect against flooding of new sessions (single-session and multiple-session flooding). In the event of a single-session attack that is underway, additionally [Use the CLI to End a Single Attacking Session](#).

## Configure DoS Protection Against Flooding of New Sessions

### Configure DoS Protection Against Flooding of New Sessions

**Step 1** (Required for single-session attack mitigation or attacks that have not triggered the DoS Protection policy threshold; optional for multiple-session attack mitigation)

Configure Security policy rules to deny traffic from the attacker's IP address and allow other traffic based on your network needs. You can specify any of the match criteria in a Security policy rule, such as source IP address.



This step is one of the steps typically performed to stop an existing attack. See [Use the CLI to End a Single Attacking Session](#).

- [Set Up Basic Security Policies](#)
- [Components of a Security Policy Rule](#)

**Configure DoS Protection Against Flooding of New Sessions (Continued)**

- |   |  |
|---|--|
| <p><b>Step 2</b> Configure a DoS Protection profile for flood protection.</p> <p> Because flood attacks can occur over multiple protocols, as a best practice, activate protection for all of the flood types in the DoS Protection profile.</p> | <ol style="list-style-type: none"><li>1. Select <b>Objects &gt; Security Profiles &gt; DoS Protection</b> and <b>Add</b> a profile <b>Name</b>.</li><li>2. Select <b>Classified</b> as the <b>Type</b>.</li><li>3. For <b>Flood Protection</b>, select the check boxes for all of the following types of flood protection:<ul style="list-style-type: none"><li>• <b>SYN Flood</b></li><li>• <b>UDP Flood</b></li><li>• <b>ICMP Flood</b></li><li>• <b>ICMPv6 Flood</b></li><li>• <b>Other IP Flood</b></li></ul></li><li>4. (Optional) On each of the flood tabs, change the following thresholds to suit your environment:<ul style="list-style-type: none"><li>• <b>Alarm Rate (packets/s)</b>—Specify the threshold rate (packets per second [pps]) above which a DoS alarm is generated. (Range is 0-2000000; default is 10000.)</li><li>• <b>Activate Rate (packets/s)</b>—Specify the threshold rate (pps) above which a DoS response is activated. The DoS response is configured in the <b>Action</b> field of the DoS policy where this profile is referenced. When the <b>Activate Rate</b> threshold is reached, <b>Random Early Drop</b> occurs. (Range is 0-2000000; default is 10000.)</li><li>• <b>Max Rate (packets/s)</b>—Specify the threshold rate of incoming packets per second that the firewall allows. When the threshold is exceeded, new packets that arrive are dropped and the <b>Action</b> specified in the DoS Policy rule is triggered. (Range is 2-2000000; default is 40000.)</li></ul><p> The default threshold values in this step are only starting points and might not be appropriate for your network. You must analyze the behavior of your network to properly set initial threshold values.</p></li><li>5. On each of the flood tabs, specify the <b>Block Duration</b> (in seconds), which is the length of time the firewall blocks packets that match the DoS Protection policy rule that references this profile. Specify a value greater than zero. (Range is 1-21600; default is 300.)<p> Set a low Block Duration value if you are concerned that packets you incorrectly identified as attack traffic will be blocked unnecessarily.</p><p>Set a high Block Duration value if you are more concerned about blocking volumetric attacks than you are about incorrectly blocking packets that are not part of an attack.</p></li><li>6. Click <b>OK</b>.</li></ol> |
|---|--|

**Configure DoS Protection Against Flooding of New Sessions (Continued)**

<p><b>Step 3</b> Configure a DoS Protection policy rule that specifies the criteria for matching the incoming traffic.</p>	<ol style="list-style-type: none"><li>1. Select <b>Policies &gt; DoS Protection</b> and <b>Add a Name</b> on the <b>General</b> tab. The name is case-sensitive and can be a maximum of 31 characters, including letters, numbers, spaces, hyphens, and underscores.</li><li>2. On the <b>Source</b> tab, choose the <b>Type</b> to be a <b>Zone</b> or <b>Interface</b>, and then <b>Add</b> the zone(s) or interface(s).</li><li>3. (Optional) For <b>Source Address</b>, select <b>Any</b> for any incoming IP address to match the rule or <b>Add</b> an address object such as a geographical region.</li><li>4. (Optional) For <b>Source User</b>, select <b>any</b> or specify a user.</li><li>5. (Optional) Select <b>Negate</b> to match any sources except those you specify.</li><li>6. (Optional) On the <b>Destination</b> tab, choose the <b>Type</b> to be a <b>Zone</b> or <b>Interface</b>, and then <b>Add</b> the destination zone(s) or interface(s). For example, enter the security zone you want to protect.</li><li>7. (Optional) For <b>Destination Address</b>, select <b>Any</b> or enter the IP address of the device you want to protect.</li><li>8. (Optional) On the <b>Option/Protection</b> tab, <b>Add a Service</b>. Select a service or click <b>Service</b> and enter a <b>Name</b>. Select <b>TCP</b> or <b>UDP</b>. Enter a <b>Destination Port</b>. Not specifying a particular service allows the rule to match a flood of any protocol type without regard to an application-specific port.</li><li>9. On the <b>Option/Protection</b> tab, for <b>Action</b>, select <b>Protect</b>.</li><li>10. Select the <b>Classified</b> check box.</li><li>11. For <b>Profile</b>, select the name of the <b>DoS Protection</b> profile you created in <a href="#">Step 2</a>.</li><li>12. For <b>Address</b>, select <b>source-ip-only</b> or <b>src-dest-ip-both</b>, which determines the type of IP address to which the rule applies. Choose the setting based on how you want the firewall to identify offending traffic.<ul style="list-style-type: none"><li>• Specify <b>source-ip-only</b> if you want the firewall to classify only on the source IP address. Because attackers often test the entire network for hosts to attack, <b>source-ip-only</b> is the typical setting for a wider examination.</li><li>• Specify <b>src-dest-ip-both</b> if you want to protect only against DoS attacks on the server that has a specific destination address and also ensure that every source IP address will not surpass a specific connections-per-second threshold to that server.</li></ul></li><li>13. Click <b>OK</b>.</li></ol>
<p><b>Step 4</b> Save the configuration.</p>	<p>Click <b>Commit</b>.</p>

## Use the CLI to End a Single Attacking Session

To mitigate a single-session DoS attack, you would still [Configure DoS Protection Against Flooding of New Sessions](#) in advance. At some point after you configure the feature, a session might be established before you realize a DoS attack (from the IP address of that session) is underway. When you see a single-session DoS attack, perform the following task to end the session, so that subsequent connection attempts from that IP address trigger the DoS protection against flooding of new sessions.

### Use the CLI to End a Single Attacking Session

- Step 1** Identify the source IP address that is causing the attack.

For example, use the firewall Packet Capture feature with a destination filter to collect a sample of the traffic going to the destination IP address. Alternatively, in PAN-OS 7.0 and later, you can use ACC to filter on destination address to view the activity to the target host being attacked.

- Step 2** Create a DoS Protection policy rule that will block the attacker's IP address after the attack thresholds are exceeded.

- Step 3** Create a Security policy rule to deny the source IP address and its attack traffic.

- Step 4** End any existing attacks from the attacking source IP address by executing the `clear session all filter source <ip-address>` operational command.

Alternatively, if you know the session ID, you can execute the `clear session id <value>` command to end that session only.



If you use the `clear session all filter source <ip-address>` command, all sessions matching the source IP address are discarded, which can include both good and bad sessions.

After you end the existing attack session, any subsequent attempts to form an attack session are blocked by the Security policy. The DoS Protection policy counts all connection attempts toward the thresholds. When the Max Rate threshold is exceeded, the source IP address is blocked for the Block Duration, as described in [Sequence of Events as Firewall Quarantines an IP Address](#).

## Identify Sessions That Use an Excessive Percentage of the Packet Buffer

When a firewall exhibits signs of resource depletion, it might be experiencing an attack that is sending an overwhelming number of packets. In such events, the firewall starts buffering inbound packets. With PAN-OS 7.0.6 and later PAN-OS 7.0 releases, you can quickly identify the sessions that are using an excessive percentage of the packet buffer and mitigate their impact by discarding them.

Perform the following task on any hardware-based firewall platform (not a VM-Series firewall) to identify, for each slot and dataplane, the packet buffer percentage used, the top five sessions using more than two percent of the packet buffer, and the source IP addresses associated with those sessions. Having that information allows you to take appropriate action.

### View Firewall Resource Usage, Top Sessions, and Session Details

**Step 1** View firewall resource usage, top sessions, and session details. Execute the following operational command in the CLI (sample output from the command follows):

```
admin@PA-7050> show running resource-monitor ingress-backlogs
-- SLOT:s1, DP:dp1 --
USAGE - ATOMIC: 92%  TOTAL: 93%
TOP SESSIONS:
SESS-ID      PCT      GRP-ID      COUNT
 6          92%        1          156
 7            7          1732
SESSION DETAILS
SESS-ID PROTO SZONE SRC           SPORT DST           DPORT IGR-IF     EGR-IF     APP
 6       6   trust 192.168.2.35  55653  10.1.8.89  80  ethernet1/21 ethernet1/22
undecided
```

The command displays a maximum of the top five sessions that each use 2% or more of the packet buffer.

The sample output above indicates that Session 6 is using 92% of the packet buffers with TCP packets (protocol 6) coming from source IP address 192.168.2.35.

- **GRP-ID**—indicates an internal stage of processing packets.
- **COUNT**—indicates how many packets are in that GRP-ID for that session.
- **SESS-ID**—indicates the global session ID that is used in all other `show session` commands. The global session ID is unique within the firewall.
- **APP**—indicates the App-ID extracted from the Session information, which can help you determine whether the traffic is legitimate. For example, if packets use a common TCP or UDP port but the CLI output indicates an APP of undecided, the packets are possibly attack traffic. The APP is undecided when Application IP Decoders cannot get enough information to determine the application. An APP of unknown indicates that Application IP Decoders cannot determine the application; a session of unknown APP that uses a high percentage of the packet buffer is also suspicious.

To restrict the display output:

On a PA-7000 Series platform, you can limit output to a slot, a dataplane, or both. For example:

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1 dp dp1
```

On a PA-5000 Series platform, you can limit output to a dataplane. For example:

```
admin@PA-5060> show running resource-monitor ingress-backlogs dp dp1
```

**View Firewall Resource Usage, Top Sessions, and Session Details (Continued)**

- Step 2** Use the command output to determine whether the source at the source IP address using a high percentage of the packet buffer is sending legitimate or attack traffic.

In the sample output above, a single-session attack is likely occurring. A single session (Session ID 6) is using 92% of the packet buffer for Slot 1, DP 1, and the application at that point is undecided.

- If you determine a single user is sending an attack and the traffic is in the slow path, you can [Use the CLI to End a Single Attacking Session](#). At a minimum, you can [Configure DoS Protection Against Flooding of New Sessions](#).
- If the traffic is offloaded to hardware (the traffic is in the fast path), clearing the session does not help because the software then has to handle the barrage of packets. You should [Discard a Session Without a Commit](#) instead.

To see whether a session is offloaded or not, use the `show session id <session-id>` operational command in the CLI as shown in the following example. The `layer7` processing value indicates `completed` for sessions offloaded or `enabled` for sessions not offloaded.

```
admin@PA-5060> show session id 68088184
Session      68088184

c2s flow:
    source:  1.1.42.15 [trust]
    dst:    1.2.27.99
    proto:   6
    sport:   55993      dport:    6881
    state:   ACTIVE      type:     FLOW
    src user: unknown
    dst user: unknown
    offload: Yes

s2c flow:
    source:  1.2.27.99 [untrust]
    dst:    1.1.42.15
    proto:   6
    sport:   6881      dport:    55993
    state:   ACTIVE      type:     FLOW
    src user: unknown
    dst user: unknown
    offload: Yes

DP                      : 2
index(local):           : 979320
start time              : Tue Oct 27 14:20:09 2015
timeout                 : 1200 sec
time to live             : 1167 sec
total byte count(c2s)   : 270
total byte count(s2c)   : 270
layer7 packet count(c2s): 3
layer7 packet count(s2c): 3
vsys                    : vsys1
application             : bittorrent
rule                   : rule1
session to be logged at end: True
session in session aqer: True
session updated by HA peer: False
layer7 processing        : completed
URL filtering enabled: False
session via syn-cookies: False
session terminated on host: False
session traverses tunnel: False
captive portal session: False
ingress interface       : ethernet1/21
egress interface        : ethernet1/22
session QoS rule        : N/A (class 4)
tracker stage l7proc    : ctd decoder bypass
end-reason              : unknown
```

## Discard a Session Without a Commit

With PAN-OS 7.0.6 and later PAN-OS 7.0 releases, you can perform this task to permanently discard a session, such as a session that is overloading the packet buffer. No commit is required; the session is discarded immediately after executing the command. The commands you use for this task apply to both offloaded and non-offloaded sessions.

---

### Discard a Session Without a Commit

---

- Step 1** In the CLI, execute the following operational command on any hardware platform:

```
admin@PA-7050> request session-discard [timeout <seconds>] [reason <reason-string>] id <session-id>
```

The default timeout is 3600 seconds.

---

- Step 2** Verify that sessions have been discarded:

```
admin@PA-7050> show session all filter state discard
```

---





# Virtual Systems

---

---

This topic describes virtual systems, their benefits, typical use cases, and how to configure them. It also provides links to other topics where virtual systems are documented as they function with other features.

- ▲ [Virtual Systems Overview](#)
- ▲ [Communication Between Virtual Systems](#)
- ▲ [Shared Gateway](#)
- ▲ [Configure Virtual Systems](#)
- ▲ [Configure Inter-Virtual System Communication within the Firewall](#)
- ▲ [Configure a Shared Gateway](#)
- ▲ [Service Routes for Virtual Systems](#)
- ▲ [Customize Service Routes for a Virtual System](#)
- ▲ [DNS Resolution—Three Use Cases](#)
- ▲ [Virtual System Functionality with Other Features](#)

# Virtual Systems Overview

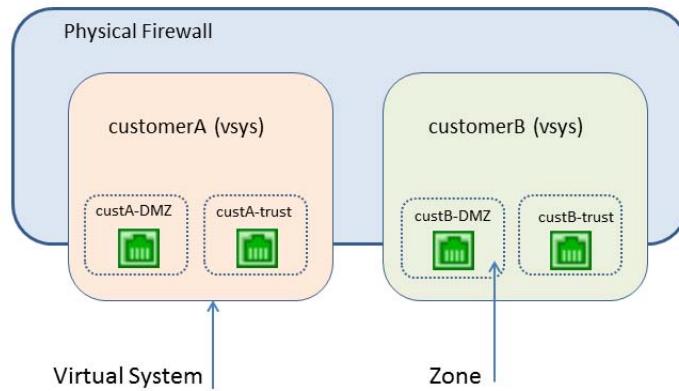
Virtual systems are separate, logical firewall instances within a single physical Palo Alto Networks firewall. Rather than using multiple firewalls, managed service providers and enterprises can use a single pair of firewalls (for high availability) and enable virtual systems on them. Each virtual system (vsys) is an independent, separately-managed firewall with its traffic kept separate from the traffic of other virtual systems.

This topic includes the following:

- ▲ [Virtual System Components and Segmentation](#)
- ▲ [Benefits of Virtual Systems](#)
- ▲ [Use Cases for Virtual Systems](#)
- ▲ [Platform Support and Licensing for Virtual Systems](#)
- ▲ [Administrative Roles for Virtual Systems](#)
- ▲ [Shared Objects for Virtual Systems](#)

## Virtual System Components and Segmentation

A virtual system is an object that creates an administrative boundary, as shown in the following figure.



A virtual system consists of a set of physical and logical interfaces and subinterfaces (including VLANs and virtual wires), virtual routers, and security zones. You choose the deployment mode(s) (any combination of virtual wire, Layer 2, or Layer 3) of each virtual system. By using virtual systems, you can segment any of the following:

- Administrative access
- The management of all policies (security, NAT, QoS, policy-based forwarding, decryption, application override, captive portal, and DoS protection)
- All objects (such as address objects, application groups and filters, dynamic block lists, security profiles, decryption profiles, custom objects, etc.)
- User-ID

- Certificate management
- Server profiles
- Logging, reporting, and visibility functions

Virtual systems affect the security functions of the firewall, but virtual systems alone do not affect networking functions such as static and dynamic routing. You can segment routing for each virtual system by creating one or more virtual routers for each virtual system, as in the following use cases:

- If you have virtual systems for departments of one organization, and the network traffic for all of the departments is within a common network, you can create a single virtual router for multiple virtual systems.
- If you want routing segmentation and each virtual system's traffic must be isolated from other virtual systems, you can create one or more virtual routers for each virtual system.

## Benefits of Virtual Systems

Virtual systems provide the same basic functions as a physical firewall, along with additional benefits:

- **Segmented administration**—Different organizations (or customers or business units) can control (and monitor) a separate firewall instance, so that they have control over their own traffic without interfering with the traffic or policies of another firewall instance on the same physical device.
- **Scalability**—After the physical firewall is configured, adding or removing customers or business units can be done efficiently. An ISP, managed security service provider, or enterprise can provide different security services to each customer.
- **Reduced capital and operational expenses**—Virtual systems eliminate the need to have multiple physical firewalls at one location because virtual systems co-exist on one firewall. By not having to purchase multiple firewalls, an organization can save on the hardware expense, electric bills, and rack space, and can reduce maintenance and management expenses.

## Use Cases for Virtual Systems

There are many ways to use virtual systems in a network. One common use case is for an ISP or a managed security service provider (MSSP) to deliver services to multiple customers with a single firewall. Customers can choose from a wide array of services that can be enabled or disabled easily. The firewall's role-based administration allows the ISP or MSSP to control each customer's access to functionality (such as logging and reporting) while hiding or offering read-only capabilities for other functions.

Another common use case is within a large enterprise that requires different firewall instances because of different technical or confidentiality requirements among multiple departments. Like the above case, different groups can have different levels of access while IT manages the firewall itself. Services can be tracked and/or billed back to departments to thereby make separate financial accountability possible within an organization.

## Platform Support and Licensing for Virtual Systems

Virtual systems are supported on the PA-2000, PA-3000, PA-4000, PA-5000, and PA-7000 Series firewalls. Each firewall series supports a base number of virtual systems; the number varies by platform. A Virtual Systems license is required in the following cases:

- To support multiple virtual systems on PA-2000 or PA-3000 Series firewalls.
- To create more than the base number of virtual systems supported on a platform.

For license information, see [Activate Licenses and Subscriptions](#). For the base and maximum number of virtual systems supported, see [Compare Firewalls](#) tool.

Multiple virtual systems are not supported on the PA-200, PA-500 or VM-Series firewalls.

## Administrative Roles for Virtual Systems

A **superuser** administrator can create virtual systems and add a **Device Administrator**, **vsysadmin**, or **vsysreader**. A **Device Administrator** can access all virtual systems, but cannot add administrators. The two types of virtual system administrative roles are:

- **vsysadmin**—Grants full access to a virtual system.
- **vsysreader**—Grants read-only access to a virtual system.

A virtual system administrator can view logs of only the virtual systems assigned to that administrator. Someone with **superuser** or **Device Admin** permission can view all of the logs or select a virtual system to view.

Persons with **vsysadmin** permission can commit configurations for only the virtual systems assigned to them.

## Shared Objects for Virtual Systems

If your administrator account extends to multiple virtual systems, you can choose to configure objects (such as an address object) and policies for a specific virtual system or as shared objects, which apply to all of the virtual systems on the firewall. If you try to create a shared object with the same name and type as an existing object in a virtual system, the virtual system object is used.

## Communication Between Virtual Systems

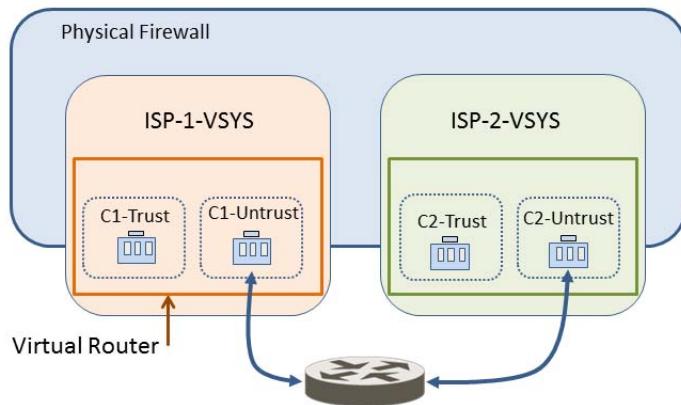
There are two typical scenarios where communication between virtual systems (inter-vsyst traffic) is desirable. In a multi-tenancy environment, communication between virtual systems can occur by having traffic leave the firewall, go through the Internet, and re-enter the firewall. In a single organization environment, communication between virtual systems can remain within the firewall. This section discusses both scenarios.

- ▲ [Inter-VSYS Traffic That Must Leave the Firewall](#)
- ▲ [Inter-VSYS Traffic That Remains Within the Firewall](#)
- ▲ [Inter-VSYS Communication Uses Two Sessions](#)

## Inter-VSYS Traffic That Must Leave the Firewall

An ISP that has multiple customers on a firewall (known as multi-tenancy) can use a virtual system for each customer, and thereby give each customer control over its virtual system configuration. The ISP grants **vsysadmin** permission to customers. Each customer's traffic and management are isolated from the others. Each virtual system must be configured with its own IP address and one or more virtual routers in order to manage traffic and its own connection to the Internet.

If the virtual systems need to communicate with each other, that traffic goes out the firewall to another Layer 3 routing device and back to the firewall, even though the virtual systems exist on the same physical firewall, as shown in the following figure.



## Inter-VSYS Traffic That Remains Within the Firewall

Unlike the preceding multi-tenancy scenario, virtual systems on a firewall can be under the control of a single organization. The organization wants to both isolate traffic between virtual systems and allow communications between virtual systems. This common use case arises when the organization wants to provide departmental separation and still have the departments be able to communicate with each other or connect to the same network(s). In this scenario, the inter-vsyst traffic remains within the firewall, as described in the following topics:

- ▲ [External Zone](#)
- ▲ [External Zones and Security Policies For Traffic Within a Firewall](#)

### External Zone

The communication desired in the use case above is achieved by configuring security policies that point to or from an *external* zone. An external zone is a security object that is associated with a specific virtual system that it can reach; the zone is external to the virtual system. A virtual system can have only one external zone, regardless of how many security zones the virtual system has within it. External zones are required to allow traffic between zones in different virtual systems, without the traffic leaving the firewall.

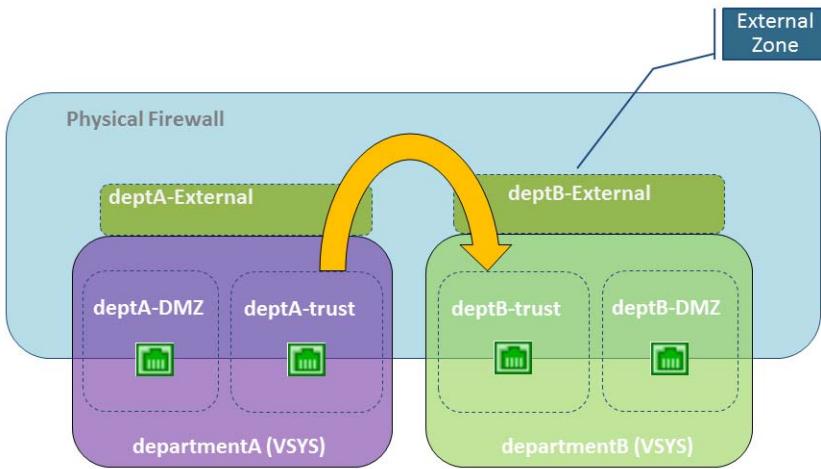
The virtual system administrator configures the security policies needed to allow traffic between two virtual systems. Unlike security zones, an external zone is not associated with an interface; it is associated with a virtual system. The security policy allows or denies traffic between the security (internal) zone and the external zone.

Because external zones do not have interfaces or IP addresses associated with them, some zone protection profiles are not supported on external zones.

Remember that each virtual system is a separate instance of a firewall, which means that each packet moving between virtual systems is inspected for security policy and App-ID evaluation.

### External Zones and Security Policies For Traffic Within a Firewall

In the following example, an enterprise has two separate administrative groups: the departmentA and departmentB virtual systems. The following figure shows the external zone associated with each virtual system, and traffic flowing from one trust zone, out an external zone, into an external zone of another virtual system, and into its trust zone.



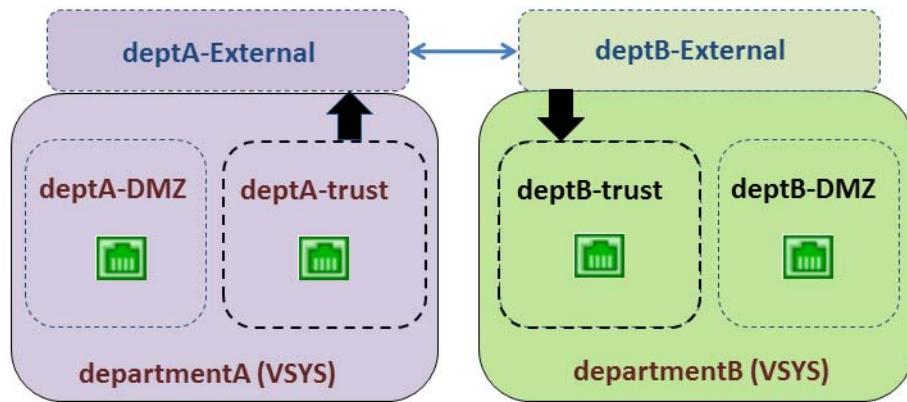
In order to create external zones, the device administrator must configure the virtual systems so that they are *visible* to each other. External zones do not have security policies between them because their virtual systems are visible to each other.

To communicate between virtual systems, the ingress and egress interfaces on the firewall are either assigned to a single virtual router or else they are connected using inter-virtual router static routes. The simpler of these two approaches is to assign all virtual systems that must communicate with each other to a single virtual router.

There might be a reason that the virtual systems need to have their own virtual router, for example, if the virtual systems use overlapping IP address ranges. Traffic can be routed between the virtual systems, but each virtual router must have static routes that point to the other virtual router(s) as the next hop.

Referring to the scenario in the figure above, we have an enterprise with two administrative groups: departmentA and departmentB. The departmentA group manages the local network and the DMZ resources. The departmentB group manages traffic in and out of the sales segment of the network. All traffic is on a local network, so a single virtual router is used. There are two external zones configured for communication between the two virtual systems. The departmentA virtual system has three zones used in security policies: deptA-DMZ, deptA-trust, and deptA-External. The departmentB virtual system also has three zones: deptB-DMZ, deptB-trust, and deptB-External. Both groups can control the traffic passing through their virtual systems.

In order to allow traffic from deptA-trust to deptB-trust, two security policies are required. In the following figure, the two vertical arrows indicate where the security policies (described below the figure) are controlling traffic.



- Security Policy 1: In the preceding figure, traffic is destined for the deptB-trust zone. Traffic leaves the deptA-trust zone and goes to the deptA-External zone. A security policy must allow traffic from the source zone (deptA-trust) to the destination zone (deptA-External). A virtual system allows any policy type to be used for this traffic, including NAT.

No policy is needed between external zones because traffic sent to an external zone appears in and has automatic access to the other external zones that are visible to the original external zone.

- Security Policy 2: In the preceding figure, the traffic from deptB-External is still destined to the deptB-trust zone, and a security policy must be configured to allow it. The policy must allow traffic from the source zone (deptB-External) to the destination zone (deptB-trust).

The departmentB virtual system could be configured to block traffic from the departmentA virtual system, and vice versa. Like traffic from any other zone, traffic from external zones must be explicitly allowed by policy to reach other zones in a virtual system.



In addition to external zones being required for inter-virtual system traffic that does not leave the firewall, external zones are also required if you configure a [Shared Gateway](#), in which case the traffic is intended to leave the firewall.

## Inter-VSYS Communication Uses Two Sessions

It is helpful to understand that communication between two virtual systems uses two sessions, unlike the one session used for a single virtual system. Let's compare the scenarios.

Scenario 1—Vsys1 has two zones: trust1 and untrust1. A host in the trust1 zone initiates traffic when it needs to communicate with a device in the untrust1 zone. The host sends traffic to the firewall, and the firewall creates a new session for source zone trust1 to destination zone untrust1. Only one session is needed for this traffic.

Scenario 2—A host from vsys1 needs to access a server on vsys2. A host in the trust1 zone initiates traffic to the firewall, and the firewall creates the first session: source zone trust1 to destination zone untrust1. Traffic is routed to vsys2, either internally or externally. Then the firewall creates a second session: source zone untrust2 to destination zone trust2. Two sessions are needed for this inter-vsys traffic.

## Shared Gateway

This topic includes the following information about shared gateways:

- ▲ [External Zones and Shared Gateway](#)
- ▲ [Networking Considerations for a Shared Gateway](#)

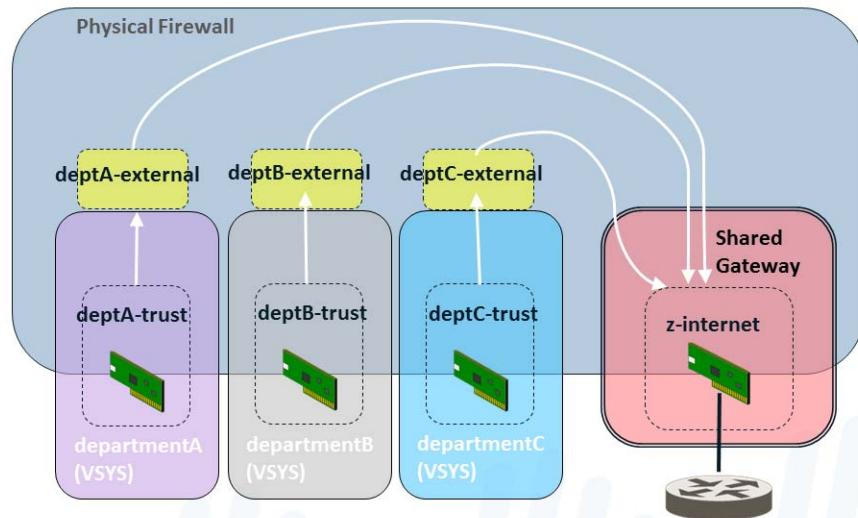
### External Zones and Shared Gateway

A shared gateway is an interface that multiple virtual systems share in order to communicate over the Internet. Each virtual system requires an [External Zone](#), which acts as an intermediary, for configuring security policies that allow or deny traffic from the virtual system's internal zone to the shared gateway.

The shared gateway uses a single virtual router to route traffic for all virtual systems. A shared gateway is used in cases when an interface does not need a full administrative boundary around it, or when multiple virtual systems must share a single Internet connection. This second case arises if an ISP provides an organization with only one IP address (interface), but multiple virtual systems need external communication.

Unlike the behavior between virtual systems, security policy and App-ID evaluations are not performed between a virtual system and a shared gateway. That is why using a shared gateway to access the Internet involves less overhead than creating another virtual system to do so.

In the following figure, three customers share a firewall, but there is only one interface accessible to the Internet. Creating another virtual system would add the overhead of App-ID and security policy evaluation for traffic being sent to the interface through the added virtual system. To avoid adding another virtual system, the solution is to configure a shared gateway, as shown in the following diagram.



The shared gateway has one globally-routable IP address used to communicate with the outside world. Interfaces in the virtual systems have IP addresses too, but they can be private, non-routable IP addresses.

You will recall that an administrator must specify whether a virtual system is visible to other virtual systems. Unlike a virtual system, a shared gateway is always visible to all of the virtual systems on the firewall.

A shared gateway ID number appears as **sg<ID>** on the web interface. It is recommended that you name your shared gateway with a name that includes its ID number.

When you add objects such as zones or interfaces to a shared gateway, the shared gateway appears as an available virtual system in the vsys drop-down menu.

A shared gateway is a limited version of a virtual system; it supports NAT and policy-based forwarding (PBF), but does not support security, DoS policies, QoS, decryption, application override, or captive portal policies.

## Networking Considerations for a Shared Gateway

Keep the following in mind while you are configuring a shared gateway.

- The virtual systems in a shared gateway scenario access the Internet through the shared gateway's physical interface, using a single IP address. If the IP addresses of the virtual systems are not globally routable, configure source NAT to translate those addresses to globally-routable IP addresses.
- A virtual router routes the traffic for all of the virtual systems through the shared gateway.
- The default route for the virtual systems should point to the shared gateway.
- Security policies must be configured for each virtual system to allow the traffic between the internal zone and external zone, which is visible to the shared gateway.
- A device administrator should control the virtual router, so that no member of a virtual system can affect the traffic of other virtual systems.
- Within a Palo Alto Networks firewall, a packet may hop from one virtual system to another virtual system or a shared gateway. A packet may not traverse more than two virtual systems or shared gateways. For example, a packet cannot go from one virtual system to a shared gateway to a second virtual system within the firewall.

To save configuration time and effort, consider the following advantages of a shared gateway:

- Rather than configure NAT for multiple virtual systems associated with a shared gateway, you can configure NAT for the shared gateway.
- Rather than configure policy-based routing (PBR) for multiple virtual systems associated with a shared gateway, you can configure PBR for the shared gateway.

## Service Routes for Virtual Systems

The firewall uses the MGT interface (by default) to access external services, such as DNS servers, software updates, and software licenses. An alternative to using the MGT interface is to configure a data port (a regular interface) to access these services. The path from the interface to the service on a server is known as a *service route*. Service routes can be configured for the firewall or for individual virtual systems. Each service allows redirection of management services to the respective virtual system owner through one of the interfaces associated with that virtual system.

The ability to configure service routes per virtual system provides the flexibility to customize service routes for numerous tenants or departments on a single firewall. The service packets exit the firewall on a port that is assigned to a specific virtual system, and the server sends its response to the configured source interface and source IP address. Any virtual system that does not have a service route configured for a particular service inherits the interface and IP address that are set globally for that service.

- ▲ [Use Cases for Service Routes for a Virtual System](#)
- ▲ [PA-7000 Series Firewall LPC Support for Per-Virtual System Paths to Logging Servers](#)
- ▲ [DNS Proxy Object](#)
- ▲ [DNS Server Profile](#)
- ▲ [Multi-Tenant DNS Deployments](#)

To configure service routes for a virtual system, see [Customize Service Routes for a Virtual System](#).

## Use Cases for Service Routes for a Virtual System

One use case for configuring service routes at the virtual system level is when a large customer (such as an ISP) needs to support multiple individual tenants on a single Palo Alto Networks firewall. The ISP has configured virtual systems on the firewall, and wants to have separate service routes for each virtual system, rather than services routes configured at the global level. Each tenant requires service route capabilities so that it can customize service route parameters for DNS, email, Kerberos, LDAP, NetFlow, RADIUS, SNMP trap, syslog, TACACS+, User-ID Agent, and VM Monitor.

Another use case is an IT organization that wants to provide full autonomy to groups that set servers for services. Each group can have a virtual system and define its own service routes.

If **Multi Virtual System Capability** is enabled, any virtual system that does not have specific service routes configured inherits the global service and service route settings for the device.

An organization can have multiple virtual systems, but use a global service route for a service rather than different service routes for each virtual system. For example, the firewall can use a shared email server to originate email alerts to its virtual systems.

A firewall with multiple virtual systems must have interfaces and subinterfaces with non-overlapping IP addresses.

A per-virtual system service route for SNMP traps or for Kerberos is for IPv4 only.

You can select a virtual router for a service route in a virtual system; you cannot select the egress interface. After you select the virtual router and the firewall sends the packet from the virtual router, the firewall selects the egress interface based on the destination IP address. Therefore:

- If a virtual system has multiple virtual routers, packets to all of the servers for a service must egress out of only one virtual router.
- A packet with an interface source address may egress a different interface, but the return traffic would be on the interface that has the source IP address, creating asymmetric traffic.

## PA-7000 Series Firewall LPC Support for Per-Virtual System Paths to Logging Servers

For Traffic, HIP Match, Threat, and Wildfire log types, the PA-7000 Series firewall does not use service routes for SNMP Trap, syslog and email services. Instead, the PA-7000 Series firewall Log Processing Card (LPC) supports virtual system-specific paths from LPC subinterfaces to an on-premise switch to the respective service on a server. For System and Config logs, the PA-7000 Series firewall uses global service routes, and not the LPC.

In other Palo Alto Networks platforms, the dataplane sends logging service route traffic to the management plane, which sends the traffic to logging servers. In the PA-7000 Series firewall, each LPC has only one interface, and data planes for multiple virtual systems send logging server traffic (types mentioned above) to the PA-7000 Series firewall LPC. The LPC is configured with multiple subinterfaces, over which the platform sends the logging service traffic out to a customer's switch, which can be connected to multiple logging servers.

Each LPC subinterface can be configured with a subinterface name and a dotted subinterface number. The subinterface is assigned to a virtual system, which is configured for logging services. The other service routes on a PA-7000 Series firewall function similarly to service routes on other Palo Alto Networks platforms.

To configure the LPC for per-virtual system logging services, see [Configure a PA-7000 Series Firewall for Logging Per Virtual System](#). For information about the LPC itself, see the [PA-7000 Series Hardware Reference Guide](#).

## DNS Proxy Object

Domain Name System (DNS) servers perform the service of resolving a domain name to an IP address, and vice versa. DNS proxy is a role in which the firewall is an intermediary between DNS clients and servers; it acts as a DNS server itself by resolving queries from its DNS proxy cache. If the domain name is not found in the DNS proxy cache, the firewall searches for a match to the domain name among the entries in the specific DNS proxy object (on the interface on which the DNS query arrived), and forwards the query to a DNS server based on the match results. If no match is found, the default DNS servers are used.

A DNS proxy object is where you configure the settings that determine how the firewall functions as a DNS proxy. You can assign a DNS proxy object to a single virtual system or it can be shared among all virtual systems.

- If the DNS proxy object is for a virtual system, you can specify a [DNS Server Profile](#), which specifies the primary and secondary DNS server addresses, along with other information. The DNS server profile simplifies configuration.
- If the DNS proxy object is shared, you must specify at least the primary address of a DNS server.



When configuring tenants with DNS services, each tenant should have its own DNS proxy defined, which keeps the tenant's DNS service separate from other tenants' services.

In the proxy object, you specify the interfaces for which the firewall is acting as DNS proxy. The DNS proxy for the interface does not use the service route; responses to the DNS requests are always sent to the interface assigned to the virtual router where the DNS request arrived.

You can supply the DNS proxy with static FQDN-to-address mappings. You can create DNS proxy rules that control to which DNS server the specified domain name queries are directed. A DNS proxy has other options; to configure a DNS proxy, see [Configure a DNS Proxy Object](#). A maximum of 256 DNS proxy objects can be configured on a firewall.

## DNS Server Profile

To simplify configuration for a virtual system, a DNS server profile allows you to specify the virtual system that is being configured, an inheritance source or the primary and secondary IP addresses for DNS servers, and a source interface and source address (service route) that will be used in packets sent to the DNS server. The source interface determines the virtual router, which has a route table. The destination IP address is looked up in the routing table of the virtual router where the source interface is assigned. It is possible that the result of the destination IP egress interface differs from the source interface. The packet would egress out of the destination IP egress interface determined by the route table lookup, but the source IP address would be the address configured. The source address is used as the destination address in the reply from the DNS server.

The virtual system report and virtual system server profile send their queries to the DNS server specified for the virtual system, if there is one. (The DNS server used is defined in **Device > Virtual Systems > General > DNS Proxy**.) If there is no DNS server specified for the virtual system, the DNS server specified for the device is queried.

A DNS server profile is for a virtual system only; it is not for a global **Shared** location. To configure a DNS server profile, see [Configure a DNS Server Profile](#).

For more information on DNS server profiles, see [DNS Resolution—Three Use Cases](#).

## Multi-Tenant DNS Deployments

There are three use cases for multi-tenant DNS deployments:

- **Global Management DNS Resolution**—The firewall needs DNS resolution for its own purposes, for example, when the request is coming from the management plane to resolve an FQDN in a security policy. The firewall uses the service route to get to a DNS server because there is no incoming virtual router. The DNS server is configured in **Device > Setup > Services > Global**, and **Servers** are configured by entering a primary and secondary DNS server.
- **Policy and Report FQDN Resolution for a Virtual System**—For DNS queries that need to be resolved from a security policy or a report, you can specify a set of DNS servers specific to the virtual system (tenant) or you can default to the global DNS servers. If your use case requires a different set of DNS servers per virtual system, the DNS server is configured in **Device > Virtual Systems > General > DNS Proxy**. The DNS proxy object is configured in **Network > DNS Proxy**. The resolution is specific to the virtual system to which the DNS proxy is assigned. If you don't have specific DNS servers applicable to this virtual system and want to use the global DNS setting, the global DNS servers take precedence.
- **Dataplane DNS Resolution for a Virtual System**—This method is also known as a Network Request for DNS Resolution. The tenant's virtual system can be configured so that specified domain names are resolved on the tenant's DNS server in its network. This method supports *split DNS*, meaning that the tenant can also use its own ISP DNS servers for the remaining DNS queries not resolved on its own server. DNS Proxy rules control the split DNS; the tenant's domain redirects DNS requests to its DNS servers, which are configured in a DNS server profile. The DNS server profile has primary and secondary DNS servers designated, and also DNS service routes for IPv4 and IPv6, which override the default DNS settings.

For more information on DNS deployments, see [DNS Resolution—Three Use Cases](#).

# Configure Virtual Systems

Creating a virtual system requires that you have the following:

- A **superuser** administrative role.
- An interface configured.
- A Virtual Systems license if you are configuring a PA-2000 or PA-3000 Series firewall, or if you are creating more than the base number of virtual systems supported on the platform. See [Platform Support and Licensing for Virtual Systems](#).

## Configure a Virtual System

<b>Step 1</b> Enable virtual systems.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Management</b> and edit the <b>General Settings</b>.</li><li>2. Select the <b>Multi Virtual System Capability</b> check box and click <b>OK</b>. This action triggers a commit if you approve it. Only after enabling virtual systems will the <b>Device</b> tab display the <b>Virtual Systems</b> and <b>Shared Gateways</b> options.</li></ol>
<b>Step 2</b> Create a virtual system.	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Virtual Systems</b>, click <b>Add</b> and enter a virtual system <b>ID</b>, which is appended to “vsys” (range is 1-255).  The default ID is 1, which makes the default virtual system <b>vsys1</b>. This default appears even on platforms that do not support multiple virtual systems.</li><li>2. Check the <b>Allow forwarding of decrypted content</b> check box if you want to allow the firewall to forward decrypted content to an outside service. For example, you must enable this option for the firewall to be able to send decrypted content to WildFire for analysis.</li><li>3. Enter a descriptive <b>Name</b> for the virtual system. A maximum of 31 alphanumeric, space, and underscore characters is allowed.</li></ol>

<b>Configure a Virtual System</b>	
<b>Step 3</b> Assign interfaces to the virtual system. The virtual routers, vwires, or VLANs can either be configured already or you can configure them later, at which point you specify the virtual system associated with each. The procedure to configure a virtual router, for example, is in Step 6 below.	<ol style="list-style-type: none"> <li>On the <b>General</b> tab, select a <b>DNS Proxy</b> object if you want to apply DNS proxy rules to the interface.</li> <li>In the <b>Interfaces</b> field, click <b>Add</b> to enter the interfaces or subinterfaces to assign to the virtual system. An interface can belong to only one virtual system.</li> <li>Do any of the following, based on the deployment type(s) you need in the virtual system: <ul style="list-style-type: none"> <li>In the <b>VLANs</b> field, click <b>Add</b> to enter the VLAN(s) to assign to the vsys.</li> <li>In the <b>Virtual Wires</b> field, click <b>Add</b> to enter the virtual wire(s) to assign to the vsys.</li> <li>In the <b>Virtual Routers</b> field, click <b>Add</b> to enter the virtual router(s) to assign to the vsys.</li> </ul> </li> <li>In the <b>Visible Virtual System</b> field, check all virtual systems that should be made visible to the virtual system being configured. This is required for virtual systems that need to communicate with each other. In a multi-tenancy scenario where strict administrative boundaries are required, no virtual systems would be checked.</li> <li>Click <b>OK</b>.</li> </ol>
<b>Step 4</b> (Optional) Limit the resource allocations for sessions, rules, and VPN tunnels allowed for the virtual system. The flexibility of being able to allocate limits per virtual system allows you to effectively control device resources.	<ol style="list-style-type: none"> <li>On the <b>Resource</b> tab, optionally set limits for a virtual system. There are no default values. <ul style="list-style-type: none"> <li><b>Sessions Limit</b>—Range is 1-262144.</li> <li><b>Security Rules</b>—Range is 0-2500.</li> <li><b>NAT Rules</b>—Range is 0-3000.</li> <li><b>Decryption Rules</b>—Range is 0-250.</li> <li><b>QoS Rules</b>—Range is 0-1000.</li> <li><b>Application Override Rules</b>—Range is 0-250.</li> <li><b>Policy Based Forwarding Rules</b>—Range is 0-500.</li> <li><b>Captive Portal Rules</b>—Range is 0-1000.</li> <li><b>DoS Protection Rules</b>—Range is 0-1000.</li> <li><b>Site to Site VPN Tunnels</b>—Range is 0-1024.</li> <li><b>Concurrent SSL VPN Tunnels</b>—Range is 0-1024.</li> </ul> </li> <li>Click <b>OK</b>.</li> </ol>
<b>Step 5</b> Save the configuration.	Click <b>Commit</b> and <b>OK</b> . The virtual system is now an object accessible from the <b>Objects</b> tab.

<b>Configure a Virtual System</b>	
<b>Step 6</b> Create at least one virtual router for the virtual system in order to make the virtual system capable of networking functions, such as static and dynamic routing.  Alternatively, your virtual system might use a VLAN or a virtual wire, depending on your deployment.	<ol style="list-style-type: none"> <li>Select <b>Network &gt; Virtual Routers</b> and <b>Add</b> a virtual router by <b>Name</b>.</li> <li>For <b>Interfaces</b>, click <b>Add</b> and from the drop-down, select the interfaces that belong to the virtual router.</li> <li>Click <b>OK</b>.</li> </ol>
<b>Step 7</b> Configure a security zone for each interface in the virtual system.	For at least one interface, create a Layer 3 security zone. See <a href="#">Configure Interfaces and Zones</a> .
<b>Step 8</b> Configure the security policies allowing or denying traffic to and from the zones in the virtual system.	See <a href="#">Set Up Basic Security Policies</a> .
<b>Step 9</b> Save the configuration.	<p>Click <b>Commit</b> and <b>OK</b>.</p>  After a virtual system is created, a device administrator can use the CLI to commit a configuration for only a specific virtual system: <pre>PA-5060&gt; commit partial vsys vsys&lt;id&gt;</pre>
<b>Step 10</b> (Optional) View the security policies configured for a virtual system.	Open an SSH session to use the CLI. To view the security policies for a virtual system, in operational mode, use the following commands: <pre>PA-5060&gt; set system setting target-vsys &lt;vsys-id&gt; PA-5060&gt; show running security-policy</pre>

# Configure Inter-Virtual System Communication within the Firewall

Perform this task if you have a use case, perhaps within a single enterprise, where you want the virtual systems to be able to communicate with each other within the firewall. Such a scenario is described in [Inter-VSYS Traffic That Remains Within the Firewall](#). This task presumes:

- You completed the task, [Configure Virtual Systems](#).
- When configuring the virtual systems, in the **Visible Virtual System** field, you checked the boxes of all virtual systems that must communicate with each other to be visible to each other.

## Configure Inter-Virtual System Communication within the Firewall

<b>Step 1</b> Configure an external zone for each virtual system.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Zones</b> and <b>Add</b> a new zone by <b>Name</b>.</li><li>2. For <b>Location</b>, select the virtual system for which you are creating an external zone.</li><li>3. For <b>Type</b>, select <b>External</b>.</li><li>4. For <b>Virtual Systems</b>, click <b>Add</b> and enter the virtual system that the external zone can reach.</li><li>5. <b>Zone Protection Profile</b>—Optionally select a zone protection profile (or configure one later) that provides flood, reconnaissance, or packet-based attack protection.</li><li>6. <b>Log Setting</b>—Optionally select a log forwarding profile for forwarding zone protection logs to an external system.</li><li>7. Optionally select the <b>Enable User Identification</b> check box to enable User-ID for the external zone.</li><li>8. Click <b>OK</b>.</li></ol>
<b>Step 2</b> Configure the security policies allowing or denying traffic from the internal zones to the external zone of the virtual system, and vice versa.	<ul style="list-style-type: none"><li>• See <a href="#">Set Up Basic Security Policies</a>.</li><li>• See <a href="#">Inter-VSYS Traffic That Remains Within the Firewall</a>.</li></ul>
<b>Step 3</b> Save the configuration.	Click <b>Commit</b> .

## Configure a Shared Gateway

Perform this task if you need multiple virtual systems to share an interface (a [Shared Gateway](#)) to the Internet. This task presumes:

- You configured an interface with a globally-routable IP address, which will be the shared gateway.
- You completed the prior task, [Configure Virtual Systems](#). For the interface, you chose the external-facing interface with the globally-routable IP address.
- When configuring the virtual systems, in the **Visible Virtual System** field, you checked the boxes of all virtual systems that must communicate to be visible to each other.

### Configure a Shared Gateway

Step 1 Configure a <a href="#">Shared Gateway</a> .	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Shared Gateway</b>, click <b>Add</b> and enter an <b>ID</b>.</li><li>2. Enter a helpful <b>Name</b>, preferably including the <b>ID</b> of the gateway.</li><li>3. In the <b>DNS Proxy</b> field, select a DNS proxy object if you want to apply DNS proxy rules to the interface.</li><li>4. <b>Add an Interface</b> that connects to the outside world.</li><li>5. Click <b>OK</b>.</li></ol>
Step 2 Configure the zone for the shared gateway.   When adding objects such as zones or interfaces to a shared gateway, the shared gateway itself will be listed as an available vsys in the <b>VSYS</b> drop-down menu.	<ol style="list-style-type: none"><li>1. Select <b>Network &gt; Zones</b> and <b>Add</b> a new zone by <b>Name</b>.</li><li>2. For <b>Location</b>, select the shared gateway for which you are creating a zone.</li><li>3. For <b>Type</b>, select <b>Layer3</b>.</li><li>4. <b>Zone Protection Profile</b>—Optionally select a zone protection profile (or configure one later) that provides flood, reconnaissance, or packet-based attack protection.</li><li>5. <b>Log Setting</b>—Optionally select a log forwarding profile for forwarding zone protection logs to an external system.</li><li>6. Optionally select the <b>Enable User Identification</b> check box to enable User-ID for the shared gateway.</li><li>7. Click <b>OK</b>.</li></ol>
Step 3 Save the configuration.	Click <b>Commit</b> .

# Customize Service Routes for a Virtual System

- ▲ [Customize Service Routes to Services for Virtual Systems](#)
- ▲ [Configure a PA-7000 Series Firewall for Logging Per Virtual System](#)
- ▲ [Configure a DNS Proxy Object](#)
- ▲ [Configure a DNS Server Profile](#)
- ▲ [Configure Administrative Access Per Virtual System or Device](#)

## Customize Service Routes to Services for Virtual Systems

- Prior to performing this task, in order to see the **Global** and **Virtual Systems** tabs, you must enable **Multi Virtual System Capability**.

If **Multi Virtual System Capability** is enabled, any virtual system that does not have specific service routes configured inherits the global service and service route settings for the device.



The firewall supports syslog forwarding on a virtual system basis. When multiple virtual systems on a firewall are connecting to a syslog server using SSL transport, the firewall can generate only one certificate for secure communication. The firewall does not support each virtual system having its own certificate.

In the following use case, you are configuring individual services routes for a firewall with multiple virtual systems.

<b>Customize Service Routes to Services Per Virtual System</b>	
<p><b>Step 1</b> Customize service routes for a virtual system.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Setup &gt; Services &gt; Virtual Systems</b>, and select the virtual system you want to configure.</li><li>2. Click the <b>Service Route Configuration</b> link.</li><li>3. Select one of the radio buttons:<ul style="list-style-type: none"><li>• <b>Inherit Global Service Route Configuration</b>—Causes the virtual system to inherit the global service route settings relevant to a virtual system. If you choose this option, skip down to step 7.</li><li>• <b>Customize</b>—Allows you to specify a source interface and source address for each service.</li></ul></li><li>4. If you chose <b>Customize</b>, select the <b>IPv4</b> or <b>IPv6</b> tab, depending on what type of addressing the server offering the service uses. You can specify both IPv4 and IPv6 addresses for a service. Click the check box(es) for the services for which you want to specify the same source information. (Only services that are relevant to a virtual system are available.) Click <b>Set Selected Service Routes</b>.<ul style="list-style-type: none"><li>• For <b>Source Interface</b>, select <b>Any</b>, <b>Inherit Global Setting</b>, or an interface from the drop-down to specify the source interface that will be used in packets sent to the external service(s). Hence, the server's response will be sent to that source interface. In our example deployment, you would set the source interface to be the subinterface of the tenant.</li><li>• <b>Source Address</b> will indicate <b>Inherited</b> if you selected <b>Inherit Global Setting</b> for the <b>Source Interface</b> or it will indicate the source address of the <b>Source Interface</b> you selected. If you selected <b>Any</b> for <b>Source Interface</b>, select an IP address from the drop-down, or enter an IP address (using the IPv4 or IPv6 format that matches the tab you chose) to specify the source address that will be used in packets sent to the external service.</li><li>• If you modify an address object and the IP family type (IPv4/IPv6) changes, a <b>Commit</b> is required to update the service route family to use.</li></ul></li><li>5. Click <b>OK</b>.</li><li>6. Repeat steps 4 and 5 to configure source addresses for other external services.</li><li>7. Click <b>OK</b>.</li></ol>
<p><b>Step 2</b> Save the configuration.</p>	<p>Click <b>Commit</b> and <b>OK</b>.</p> <p>If you are configuring per-virtual system service routes for logging services for a PA-7000 Series firewall, continue to the task <a href="#">Configure a PA-7000 Series Firewall for Logging Per Virtual System</a>.</p>

## Configure a PA-7000 Series Firewall for Logging Per Virtual System

- You must have enabled **Multi Virtual System Capability** (**Device > Setup > Management**) in order to access the LPC subinterface configuration.

Perform this task on your PA-7000 Series firewall to configure logging for different virtual systems. For more information, see [PA-7000 Series Firewall LPC Support for Per-Virtual System Paths to Logging Servers](#).

<b>Configure a PA-7000 Series Firewall Subinterface for Service Routes per Virtual System</b>	
<b>Step 1</b> Create a Log Card subinterface.	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces &gt; Ethernet</b> and select the interface that will be the Log Card interface.</li> <li>2. Enter the <b>Interface Name</b>.</li> <li>3. For <b>Interface Type</b>, select <b>Log Card</b> from the drop-down.</li> <li>4. Click <b>OK</b>.</li> </ol>
<b>Step 2</b> Add a subinterface for each tenant on the LPCs physical interface.	<ol style="list-style-type: none"> <li>1. Highlight the Ethernet interface that is a Log Card interface type and click <b>Add Subinterface</b>.</li> <li>2. For <b>Interface Name</b>, after the period, enter the subinterface assigned to the tenant's virtual system.</li> <li>3. For <b>Tag</b>, enter a VLAN tag value.   Make the tag the same as the subinterface number for ease of use, but it could be a different number.</li> <li>4. (Optional) Enter a <b>Comment</b>.</li> <li>5. On the <b>Config</b> tab, in the <b>Assign Interface to Virtual System</b> field, select the virtual system to which the LPC subinterface is assigned (from the drop-down). Alternatively, you can click <b>Virtual Systems</b> to add a new virtual system.</li> <li>6. Click <b>OK</b>.</li> </ol>
<b>Step 3</b> Enter the addresses assigned to the subinterface, and configure the default gateway.	<ol style="list-style-type: none"> <li>1. Select the <b>Log Card Forwarding</b> tab, and do one or both of the following: <ul style="list-style-type: none"> <li>• For the IPv4 section, enter the <b>IP Address</b> and <b>Netmask</b> assigned to the subinterface. Enter the <b>Default Gateway</b> (the next hop where packets will be sent that have no known next hop address in the Routing Information Base [RIB]).</li> <li>• For the IPv6 section, enter the <b>IPv6 Address</b> assigned to the subinterface. Enter the <b>IPv6 Default Gateway</b>.</li> </ul> </li> <li>2. Click <b>OK</b>.</li> </ol>
<b>Step 4</b> Save the configuration.	Click <b>OK</b> and <b>Commit</b> .
<b>Step 5</b> If you haven't already done so, configure the remaining service routes for the virtual system.	<a href="#">Customize Service Routes for a Virtual System</a> .

## Configure a DNS Proxy Object

If your firewall is to act as a DNS proxy for a virtual system, perform this task to configure a [DNS Proxy Object](#). The proxy object can either be shared among all virtual systems or applied to a specific virtual system.

<b>Configure a DNS Proxy Object</b>	
<b>Step 1</b> Configure the basic settings for a DNS Proxy object.	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; DNS Proxy</b> and <b>Add</b> a new object.</li> <li>2. Verify that <b>Enable</b> is selected.</li> <li>3. Enter a <b>Name</b> for the object.</li> <li>4. For <b>Location</b>, select the virtual system to which the object applies. If you select <b>Shared</b>, you must specify at least a <b>Primary</b> DNS server address., and optionally a <b>Secondary</b> address.</li> <li>5. If you selected a virtual system, for <b>Server Profile</b>, select a DNS Server profile or else click <b>DNS Server Profile</b> to configure a new profile. see <a href="#">Configure a DNS Server Profile</a>.</li> <li>6. For <b>Interface</b>, click <b>Add</b> and specify the interfaces to which the DNS Proxy object applies. <ul style="list-style-type: none"> <li>• If you use the DNS Proxy object for performing DNS lookups, an interface is required. The firewall will listen for DNS requests on this interface, and then proxy them.</li> <li>• If you use the DNS Proxy object for a service route, the interface is optional.</li> </ul> </li> </ol>
<b>Step 2</b> (Optional) Specify DNS Proxy rules.	<ol style="list-style-type: none"> <li>1. On the <b>DNS Proxy Rules</b> tab, click <b>Add</b> and enter a <b>Name</b> for the rule.</li> <li>2. <b>Turn on caching of domains resolved by this mapping</b> if you want the firewall to cache the resolved domains.</li> <li>3. For <b>Domain Name</b>, click <b>Add</b> and enter one or more domains, one entry per row. Each domain name can contain * as a wildcard. The number of tokens in a wildcard string must match the number of tokens in the requested domain. For example, *.engineering.local will not match 'engineering.local'. Both entries must be specified if you want both.</li> <li>4. In Step 4 above, for <b>Location</b>: <ul style="list-style-type: none"> <li>• If you chose a virtual system, select a <b>DNS Server profile</b> here.</li> <li>• If you chose <b>Shared</b>, enter a <b>Primary</b> address here.</li> </ul> </li> <li>5. Click <b>OK</b>.</li> </ol>
<b>Step 3</b> (Optional) Supply the DNS Proxy with static FQDN-to-address entries. Static DNS entries allow the firewall to resolve the FQDN to an IP address without going out to the DNS server.	<ol style="list-style-type: none"> <li>1. On the <b>Static Entries</b> tab, click <b>Add</b> and enter a <b>Name</b>.</li> <li>2. Enter the Fully Qualified Domain Name (<b>FQDN</b>).</li> <li>3. For <b>Address</b>, click <b>Add</b> and enter the IP address to which the FQDN should be mapped.</li> <li>4. Repeat steps 1-3 to provide additional static entries.</li> <li>5. Click <b>OK</b>.</li> </ol>

Configure a DNS Proxy Object (Continued)	
Step 4 (Optional) Enable caching and configure other advanced settings for the DNS Proxy.	<ol style="list-style-type: none"><li>On the <b>Advanced</b> tab, click <b>Cache</b> to enable the firewall to cache FQDN-to-address mappings that the firewall learns.<ul style="list-style-type: none"><li><b>Size</b>—Enter the maximum number of entries the firewall can cache (range is 1024-10240; default is 1024).</li><li><b>Timeout</b>—Enter the number of hours after which all cached entries are removed (range is 4-24; default is 4). DNS time-to-live values are used to remove cache entries when they have been stored for less than the configured timeout period. After a timeout, new DNS requests must be resolved and cached again.</li></ul></li><li>Select <b>TCP Queries</b> to enable DNS queries using TCP.<ul style="list-style-type: none"><li><b>Max Pending Requests</b>—Enter the maximum number of concurrent, pending TCP DNS requests that the firewall will support (range is 64-256; default is 64).</li></ul></li><li>For <b>UDP Queries Retries</b>, enter the following:<ul style="list-style-type: none"><li><b>Interval</b>—Enter the length of time (in seconds) after which another request is sent if no response has been received. (range is 1-30; default is 2).</li><li><b>Attempts</b>—Enter the maximum number of UDP query attempts (excluding the first attempt) after which the next DNS server is queried (range is 1-30; default is 5).</li></ul></li></ol>
Step 5 Save the configuration.	Click <b>OK</b> and <b>Commit</b> .

## Configure a DNS Server Profile

Perform this task to configure a [DNS Server Profile](#), which simplifies configuration of a virtual system. The **Primary DNS** or **Secondary DNS** address is used to create the DNS request that the virtual system sends to the DNS server.

<b>Configure a DNS Server Profile</b>	
<b>Step 1</b> Name the DNS server profile, select the virtual system to which it applies, and specify the primary and secondary DNS server addresses.	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Server Profiles &gt; DNS</b> and click <b>Add</b>.</li> <li>Enter a <b>Name</b> for the DNS server profile.</li> <li>For <b>Location</b>, select the virtual system to which the profile applies.</li> <li>For <b>Inheritance Source</b>, from the drop-down, select <b>None</b> if the DNS server addresses are not inherited. Otherwise, specify the DNS server from which the profile should inherit settings. If you choose a DNS server, click <b>Check inheritance source status</b> to see that information.</li> <li>Specify the IP address of the <b>Primary DNS</b> server, or leave as <b>inherited</b> if you chose an <b>Inheritance Source</b>.           <p> Keep in mind that if you specify an FQDN instead of an IP address, the DNS for that FQDN is resolved in <b>Device &gt; Virtual Systems &gt; DNS Proxy</b>.</p> </li> <li>Specify the IP address of the <b>Secondary DNS</b> server, or leave as <b>inherited</b> if you chose an <b>Inheritance Source</b>.</li> </ol>
<b>Step 2</b> Configure the service route that the firewall automatically uses, based on whether the target DNS Server has an IP address family type of IPv4 or IPv6.	<ol style="list-style-type: none"> <li>Click <b>Service Route IPv4</b> to enable the subsequent interface and IPv4 address to be used as the service route, if the target DNS address is an IPv4 address.</li> <li>Specify the <b>Source Interface</b> to select the DNS server's source IP address that the service route will use. The firewall determines which virtual router is assigned that interface, and then does a route lookup in the virtual router routing table to reach the destination network (based on the <b>Primary DNS</b> address).</li> <li>Specify the IPv4 <b>Source Address</b> from which packets going to the DNS server are sourced.</li> <li>Click <b>Service Route IPv6</b> to enable the subsequent interface and IPv6 address to be used as the service route, if the target DNS address is an IPv6 address.</li> <li>Specify the <b>Source Interface</b> to select the DNS server's source IP address that the service route will use. The firewall determines which virtual router is assigned that interface, and then does a route lookup in the virtual router routing table to reach the destination network (based on the <b>Primary DNS</b> address).</li> <li>Specify the IPv6 <b>Source Address</b> from which packets going to the DNS server are sourced.</li> <li>Click <b>OK</b>.</li> </ol>
<b>Step 3</b> Save the configuration.	Click <b>OK</b> and <b>Commit</b> .

## Configure Administrative Access Per Virtual System or Device

If you have a superuser administrative account, you now have the ability to create and configure more granular permissions for a vsysadmin or device admin role.

### Create an Admin Role Profile Per Virtual System or Device

- |        |  |  |
|--------|--|--|
| Step 1 | <p>Create an Admin Role Profile that grants or disables permission to an Administrator to configure or read-only various areas of the web interface.</p> | <ol style="list-style-type: none"><li>1. Select <b>Device &gt; Admin Roles</b> and <b>Add an Admin Role Profile</b>.</li><li>2. Enter a <b>Name</b> and optional <b>Description</b> of the profile.</li><li>3. For <b>Role</b>, specify which level of control the profile affects:<ul style="list-style-type: none"><li>• <b>Device</b>—The profile allows the management of the global settings and any virtual systems.</li><li>• <b>Virtual System</b>—The profile allows the management of only the virtual system(s) assigned to the administrator(s) who have this profile. (The administrator will be able to access <b>Device &gt; Setup &gt; Services &gt; Virtual Systems</b>, but not the <b>Global</b> tab.)</li></ul></li><li>4. On the <b>Web UI</b> tab for the Admin Role Profile, scroll down to <b>Device</b>, and leave the green check mark (Enable).<ul style="list-style-type: none"><li>• Under <b>Device</b>, enable <b>Setup</b>. Under <b>Setup</b>, enable the areas to which this profile will grant configuration permission to the administrator, as shown below. (The Read Only lock icon appears in the Enable/Disable rotation if Read Only is allowed for that setting)<ul style="list-style-type: none"><li>– <b>Management</b>—Allows an admin with this profile to configure settings on the <b>Management</b> tab.</li><li>– <b>Operations</b>—Allows an admin with this profile to configure settings on the <b>Operations</b> tab.</li><li>– <b>Services</b>—Allows an admin with this profile to configure settings on the <b>Services</b> tab. An admin must have <b>Services</b> enabled in order to access the <b>Device &gt; Setup Services &gt; Virtual Systems</b> tab. If the <b>Role</b> was specified as <b>Virtual System</b> in the prior step, <b>Services</b> is the only setting that can be enabled under <b>Device &gt; Setup</b>.</li><li>– <b>Content-ID</b>—Allows an admin with this profile to configure settings on the <b>Content-ID</b> tab.</li><li>– <b>WildFire</b>—Allows an admin with this profile to configure settings on the <b>WildFire</b> tab.</li><li>– <b>Session</b>—Allows an admin with this profile to configure settings on the <b>Session</b> tab.</li><li>– <b>HSM</b>—Allows an admin with this profile to configure settings on the <b>HSM</b> tab.</li></ul></li></ul></li><li>5. Click <b>OK</b>.</li><li>6. (Optional) Repeat the entire step to create another Admin Role profile with different permissions, as necessary.</li></ol> |
|--------|--|--|

**Create an Admin Role Profile Per Virtual System or Device (Continued)**

<p><b>Step 2</b> Apply the Admin role profile to an administrator.</p>	<ol style="list-style-type: none"><li>1. Select <b>Device &gt; Administrators</b>, click <b>Add</b> and enter the <b>Name</b> to add an Administrator.</li><li>2. (Optional) Select an <b>Authentication Profile</b>.</li><li>3. (Optional) Select <b>Use only client certificate authentication (Web)</b> to have bi-directional authentication; to get the server to authenticate the client.</li><li>4. Enter a <b>Password</b> and <b>Confirm Password</b>.</li><li>5. (Optional) Select <b>Use Public Key Authentication (SSH)</b> if you want to use a much stronger, key-based authentication method using an SSH public key rather than just a password.</li><li>6. For <b>Administrator Type</b>, select <b>Role Based</b>.</li><li>7. For <b>Profile</b>, select the profile that you just created.</li><li>8. (Optional) Select a <b>Password Profile</b>.</li><li>9. Click <b>OK</b>.</li></ol>
<p><b>Step 3</b> Save the configuration.</p>	<p>Click <b>Commit</b> and <b>OK</b>.</p>

## DNS Resolution—Three Use Cases

The firewall determines how to handle DNS requests based on where the request originated. This section illustrates three types of DNS resolution, which are listed in the following table. The binding location determines which DNS proxy object is used for the resolution. For illustration purposes, the use cases show how a service provider might configure DNS settings to provide DNS services for resolving DNS queries required on the firewall and for tenant (subscriber) virtual systems.

Resolution Type	Location: Shared	Location: Specific Vsyst
Firewall DNS resolution—performed by management plane	Binding: Global Illustrated in Use Case 1	N/A
Security profile, reporting, and server profile resolution—performed by management plane	Binding: Global Same behavior as Use Case 1	Binding: Specific vsys Illustrated in Use Case 2
DNS proxy resolution for DNS client hosts connected to interface on firewall, going through the firewall to a DNS Server—performed by dataplane		Binding: Interface Service Route: Interface and IP address on which the DNS Request was received. Illustrated in Use Case 3

- ▲ Use Case 1: Firewall Requires DNS Resolution for Management Purposes
- ▲ Use Case 2: ISP Tenant Uses DNS Proxy to Handle DNS Resolution for Security Policies, Reporting, and Services within its Virtual System
- ▲ Use Case 3: Firewall Acts as DNS Proxy Between Client and Server

### Use Case 1: Firewall Requires DNS Resolution for Management Purposes

In this use case, the firewall is the client requesting DNS resolutions of FQDNs for management events such as software update services, dynamic software updates, or WildFire. The shared, global DNS services perform the DNS resolution for the management plane functions.



### Configure DNS Services for the Firewall

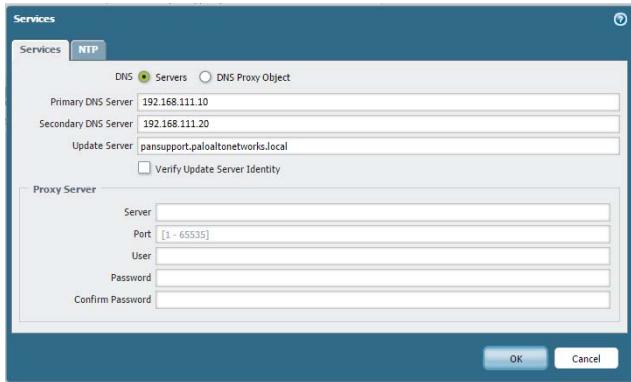
- Step 1** Configure the primary and secondary DNS servers you want the firewall to use for its management DNS resolutions.



You must manually configure at least one DNS server on the firewall or it will not be able to resolve hostnames; it will not use DNS server settings from another source, such as an ISP.

- 1.** Select **Device > Setup > Services > Global** and Edit. (For devices that do not support multiple virtual systems, there is no **Global** tab; simply edit the Services.)

- 2.** On the **Services** tab, for **DNS**, click **Servers** and enter the **Primary DNS Server** address and **Secondary DNS Server** address.

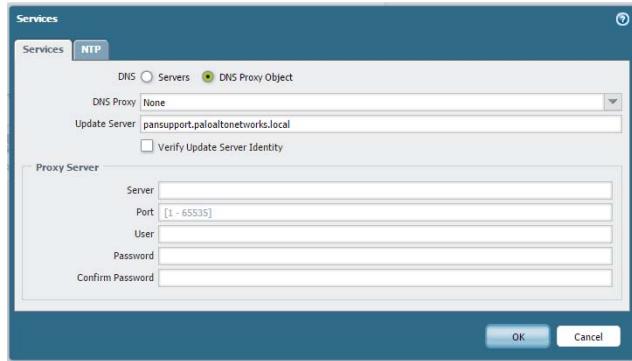


- 3.** Click **OK** and **Commit**.

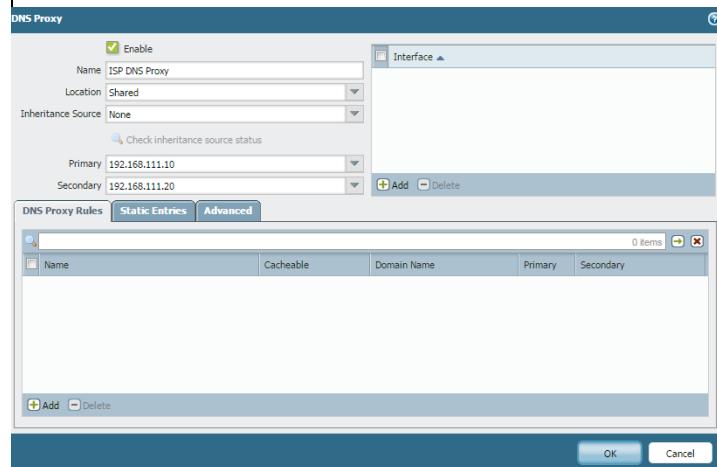
## Configure DNS Services for the Firewall (Continued)

**Step 2** Alternatively, you can configure a [DNS Proxy Object](#) if you want to configure advanced DNS functions such as split DNS, DNS proxy overrides, DNS proxy rules, static entries, or DNS inheritance.

- On the **Services** tab, for **DNS**, click **DNS Proxy Object**.



- From the **DNS Proxy** drop-down, select the DNS proxy that you want to use to configure global DNS services, or click **DNS Proxy** to configure a new DNS proxy object, as shown in the following screenshot and subsequent steps.



- To create a new proxy object, click **Enable** and enter a **Name** for the DNS proxy object.

- For **Location**, select **Shared** for global, device-wide DNS proxy services.

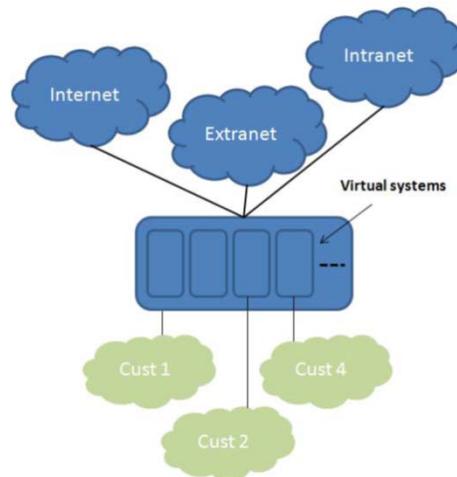


Shared DNS proxy objects do not use DNS server profiles because they do not require a specific service route belonging to a tenant virtual system.

- For **Primary**, enter the primary DNS server IP address. Optionally enter a **Secondary** DNS server IP address. In the ISP example in the screenshot above, the DNS proxy defines the primary and secondary DNS servers that are used to resolve the firewall management services.
- Click **OK** and **Commit**.

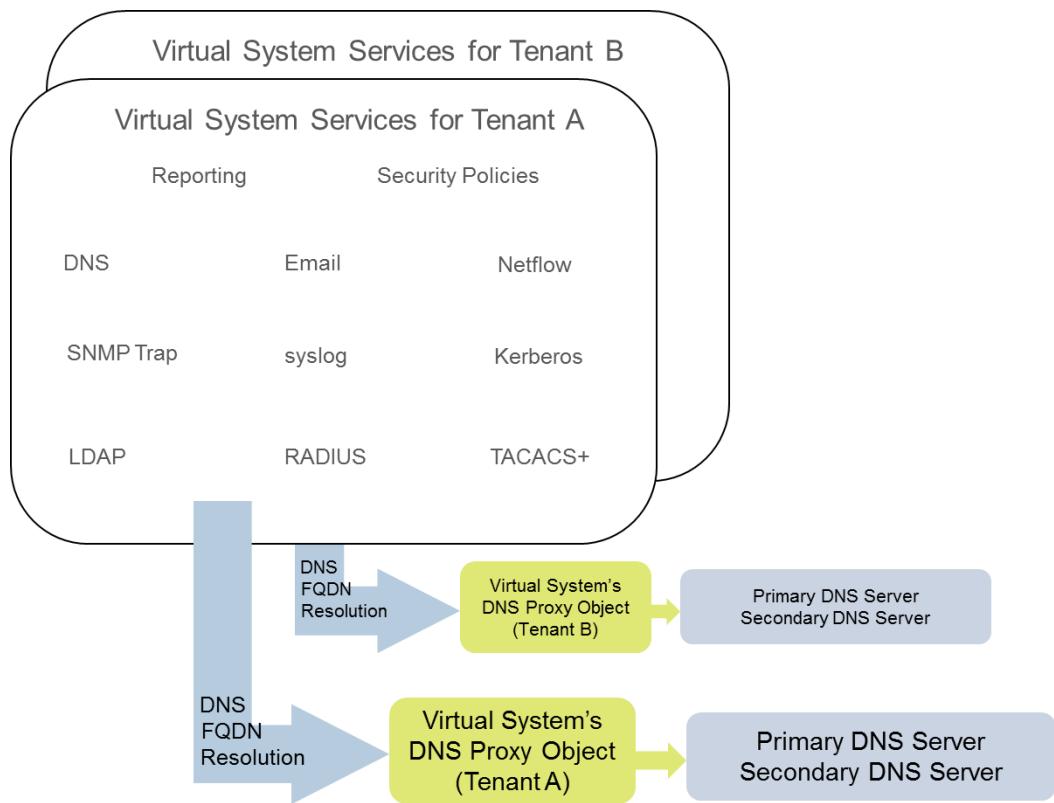
## Use Case 2: ISP Tenant Uses DNS Proxy to Handle DNS Resolution for Security Policies, Reporting, and Services within its Virtual System

In this use case, multiple tenants (ISP subscribers) are defined on the firewall and each tenant is allocated a separate virtual system (vsys) and virtual router in order to segment its services and administrative domains. The following figure illustrates several virtual systems within a firewall.



Each tenant has its own server profiles for its security policies, reporting, and management services (such as email, Kerberos, SNMP, syslog, and more) defined in its own networks.

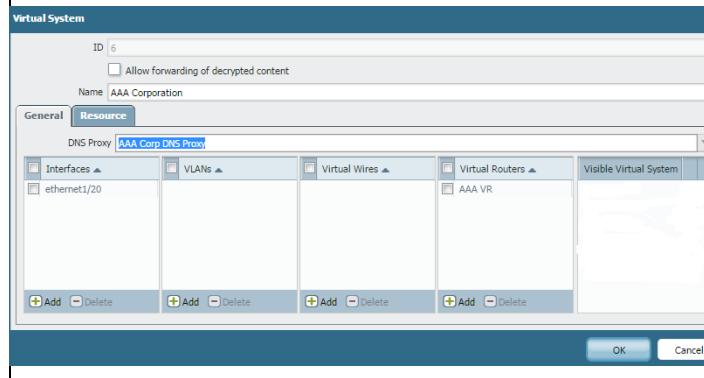
For the DNS resolutions initiated by these services, each virtual system is configured with its own DNS Proxy object to allow each tenant to customize how DNS resolution is handled within its virtual system. Any service with a **Location** will use the DNS Proxy object configured for the virtual system to determine the primary (or secondary) DNS server to resolve FQDNs, as illustrated in the following figure.



### Configure a DNS Proxy for a Virtual System

**Step 1** For each virtual system, specify the DNS Proxy to use.

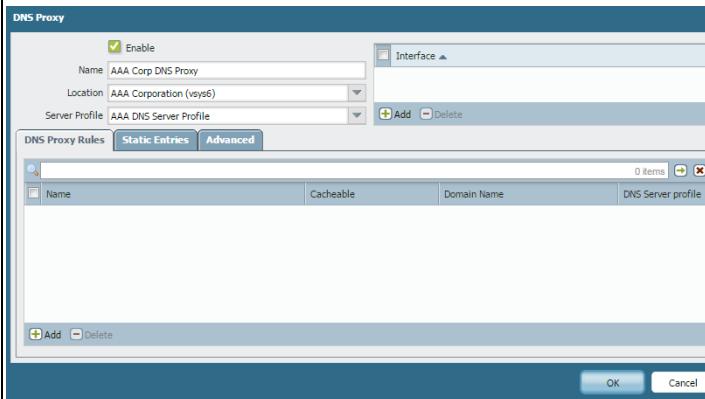
1. Select **Device > Virtual Systems** and click **Add**.
2. Enter the **ID** of the virtual system (range is 1-255), and an optional **Name**, in this example, Corp1 Corporation.
3. On the **General** tab, choose a **DNS Proxy** or create a new one. In this example, Corp1 DNS Proxy is selected as the proxy for Corp1 Corporation's virtual system.  
(If you need to create a new DNS Proxy, [Step 2](#) below shows how to create a DNS Proxy and a Server Profile.)
4. For **Interfaces**, click **Add**. In this example, Ethernet1/20 is dedicated to this tenant.
5. For **Virtual Routers**, click **Add**. A virtual router named Corp1 VR is assigned to the virtual system in order to separate routing functions.
6. Click **OK** to save the configuration.



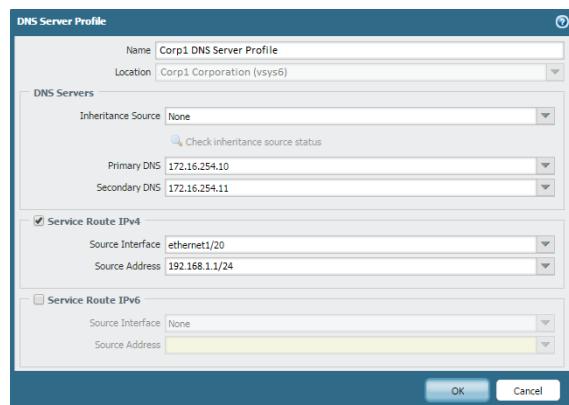
## Configure a DNS Proxy for a Virtual System

**Step 2** Configure a DNS Proxy and a server profile to support DNS resolution for a virtual system.

1. Select **Network > DNS Proxy** and click **Add**.
2. Click **Enable** and enter a **Name** for the DNS Proxy.
3. For **Location**, select the virtual system of the tenant, in this example, Corp1 Corporation (vsys6). (You could choose the **Shared** DNS Proxy resource instead.)



4. For **Server Profile**, choose or create a profile to customize DNS servers to use for DNS resolutions for this tenant's security policy, reporting, and server profile services. If the profile is not already configured, in the **Server Profile** field, click **DNS Server Profile** to [Configure a DNS Server Profile](#). In this example, the Corp1 DNS Server Profile was created.



The DNS server profile identifies the IP addresses of the primary and secondary DNS server to use for management DNS resolutions for this virtual system.

5. Also for this server profile, optionally configure a **Service Route IPv4** and/or a **Service Route IPv6** to instruct the firewall which **Source Interface** to use in its DNS requests. If that interface has more than one IP address, configure the **Source Address** also.
6. Click **OK** to save the DNS Server Profile.
7. Click **OK** and **Commit** to save the DNS Proxy.



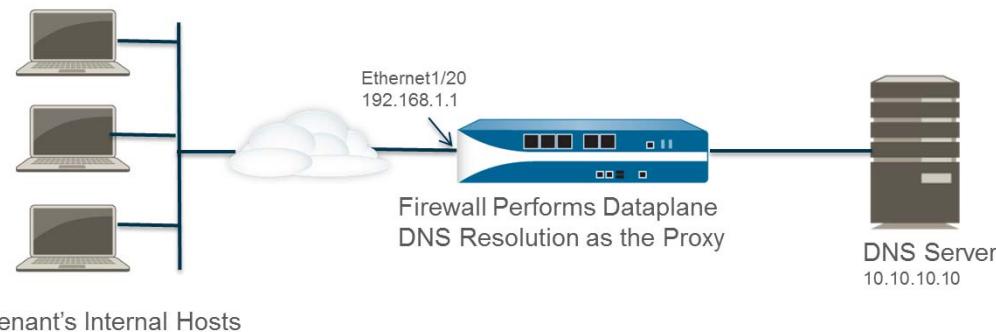
Optional advanced features such as split DNS can be configured using **DNS Proxy Rules**. A separate DNS server profile can be used to redirect DNS resolutions matching the **Domain Name** in a **DNS Proxy Rule** to another set of DNS servers, if required. Use Case 3 illustrates split DNS.

If you use two separate DNS server profiles in the same DNS Proxy object, one for the DNS Proxy and one for the DNS proxy rule, the following behaviors occur:

- If a service route is defined in the DNS server profile used by the DNS Proxy, it takes precedence and is used.
- If a service route is defined in the DNS server profile used in the DNS proxy rules, it is not used. If the service route differs from the one defined in the DNS server profile used by the DNS Proxy, the following warning message is displayed during the **Commit** process:  
Warning: The DNS service route defined in the DNS proxy object is different from the DNS proxy rule's service route. Using the DNS proxy object's service route.
- If no service route is defined in any DNS server profile, the global service route is used if needed.

## Use Case 3: Firewall Acts as DNS Proxy Between Client and Server

In this use case, the firewall is located between a DNS client and a DNS server. A DNS Proxy on the firewall is configured to act as the DNS server for the hosts that reside on the tenant's network connected to the firewall interface. In such a scenario, the firewall performs DNS resolution on its dataplane.



This scenario happens to use *split DNS*, a configuration where **DNS Proxy Rules** are configured to redirect DNS requests to a set of DNS servers based on a domain name match. If there is no match, the **Server Profile** determines the DNS servers to which the request is sent, hence the two, split DNS resolution methods.

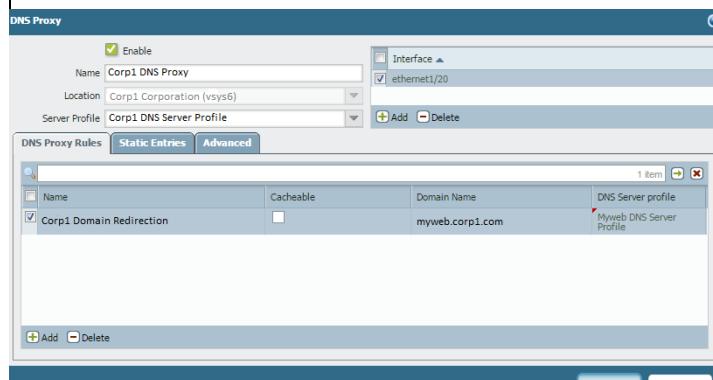


For dataplane DNS resolutions, the source IP address from the DNS proxy in PAN-OS to the outside DNS server would be the address of the proxy (the destination IP of the original request). Any service routes defined in the DNS Server Profile are not used. For example, if the request is from host 1.1.1.1 to the DNS proxy at 2.2.2.2, then the request to the DNS server (at 3.3.3.3) would use a source of 2.2.2.2 and a destination of 3.3.3.3.

### Configure a DNS Proxy and DNS Proxy Rules

**Step 1** Configure a DNS Proxy and DNS proxy rules.

1. Select **Network > DNS Proxy** and click **Add**.
2. Click **Enable** and enter a **Name** for the DNS Proxy.
3. For **Location**, select the virtual system of the tenant, in this example, Corp1 Corporation (vsys6).
4. For **Interface**, select the interface that will receive the DNS requests from the tenant's hosts, in this example, Ethernet1/20.
5. Choose or create a **Server Profile** to customize DNS servers to resolve DNS requests for this tenant. In this example, the Corp1 DNS Server Profile is selected.



6. On the **DNS Proxy Rules** tab, click **Add** and enter a **Name** for the rule.
7. Optionally select **Turn on caching of domains resolved by this mapping**.
8. Click **Add** and enter one or more **Domain Name(s)**, one entry per row.  
Each domain name can contain \* as a wild card. The number of characters in a wildcard string must equal the number of characters in the requested domain to match. For example, \*.engineering.local does not match 'engineering.local'. Both domain names must be specified in order for both to be matched.
9. For **DNS Server profile**, select a profile from the drop-down. The firewall compares the domain name in the DNS request to the domain name(s) defined in the **DNS Proxy Rules**. If there is a match, the **DNS Server profile** defined in the rule is used to determine the DNS server.  
In this example, if the domain in the request matches myweb.corp1.com, the DNS server defined in the myweb DNS Server Profile is used. If there is no match, the DNS server defined in the **Server Profile** (Corp1 DNS Server Profile) is used.
10. Click **OK** to save the rule.
11. Click **OK** to save the DNS Proxy.

## Virtual System Functionality with Other Features

Many of the firewall's features and functionality are capable of being configured, viewed, logged, or reported per virtual system. Therefore, virtual systems are mentioned in other relevant locations in the documentation and that information is not repeated here. Some of the specific chapters are the following:

- If you are configuring Active/Passive HA, the two firewalls must have the same virtual system capability (single or multiple virtual system capability). See [High Availability](#).
- To configure QoS for virtual systems, see [Configure QoS for a Virtual System](#).
- For information about configuring a firewall with virtual systems in a virtual wire deployment that uses subinterfaces (and VLAN tags), see the Virtual Wire Subinterfaces in [Interface Deployments](#).





# Certifications

---

---

The following topics describe how to configure the firewall to support the Common Criteria and the Federal Information Processing Standards 140-2 (FIPS 140-2), which are security certifications that ensure a standard set of security assurances and functionalities. These certifications are often required by civilian U.S. government agencies and government contractors.

- ▲ [Enable FIPS and Common Criteria Support](#)
- ▲ [CCEAL4 Security Functions](#)

# Enable FIPS and Common Criteria Support

Use the following procedure to enable CCEAL4 mode on a software version that supports Common Criteria and the Federal Information Processing Standards 140-2 (FIPS 140-2). When you enable CCEAL4 mode, all FIPS functionality is also included in this mode.

 When you enable CCEAL4 mode, the device will reset to the factory default settings; all configuration will be removed.

## Enable CCEAL4 Mode

**Step 1** Boot the device into maintenance mode as follows:

1. Establish a serial connection to the console port on the firewall.
2. Enter the following CLI command:  
`debug system maintenance-mode`
3. Press Enter to continue.



You can also reboot the firewall and enter `maint` at the maintenance mode prompt.

**Step 2** Select **Set CCEAL4 Mode** from the menu.



Official certification support is only provided with **CCEAL4** mode; not **FIPS** mode.

**Step 3** Select **Enable CCEAL4 Mode** from the menu.

**Step 4** When prompted, select **Reboot**.

After successfully switching to CCEAL4 mode, the following status displays: `cceal4 mode enabled successfully`. In addition, the following changes will take place:

- **CC** will display at all times in the status bar at the bottom of the web interface.
- The console port functions as a status output port only
- The default admin login credentials change to admin/paloalto.

## CCEAL4 Security Functions

When CCEAL4 mode is enabled, the following security functions are enforced:

- To log into the firewall, the browser must be TLS 1.0 (or later) compatible. On a WF-500 appliance, you manage the appliance using the CLI only and you must connect using an SSHv2 compatible client application.
- All passwords on the firewall must be at least six characters.
- You must enforce a **Failed Attempts** and **Lockout Time (min)** value that is greater than 0 in authentication settings. If an administrator reaches the **Failed Attempts** threshold, the administrator is locked out for the duration defined in the **Lockout Time (min)** field.
- You must enforce an **Idle Timeout** value greater than 0 in authentication settings. If a login session is idle for more than the specified value, the account is automatically logged out.
- The firewall automatically determines the appropriate level of self-testing and enforces the appropriate level of strength in encryption algorithms and cipher suites.
- Non-CC/FIPS approved algorithms are not decrypted and are thus ignored during decryption.
- When configuring an IPSec VPN, the administrator must select a cipher suite option presented to them during the IPSec setup.
- Self-generated and imported certificates must contain public keys that are either RSA 2048 bits (or more) or ECDSA 256 bits (or more) and you must use a digest of SHA256 or greater.
- The serial console port is only available as a status output port when CCEAL4 is enabled.
- Telnet, TFTP, and HTTP management connections are unavailable.
- High availability (HA) port encryption is required.

