



# **Palo Alto Networks Certified Network Security Engineer (PCNSE)**

## **Study Guide**

**2022**

Palo Alto Networks, Inc.  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2022 Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, PAN-OS, WildFire, RedLock, and Demisto are trademarks of Palo Alto Networks, Inc. All other trademarks are the property of their respective owners.

# Table of Contents

<b>Palo Alto Networks PCNSE Study Guide</b>	<b>14</b>
Overview	14
Exam Details	14
Audience	15
Qualifications	15
Skills Required	15
Recommended Training	15
About This Document	16
Disclaimer	16
Preliminary Score Report	16
<b>Domain 1 – Core Concepts</b>	<b>17</b>
1.1 Identify how Palo Alto Networks products work together to improve PAN-OS services	17
1.1.1 Security components	17
1.1.2 Firewall components	24
1.1.3 Panorama components	27
1.1.4 PAN-OS subscriptions and the features they enable	28
1.1.5 Plugin components	31
1.1.6 Heatmaps and Best Practice Assessment reports	31
1.1.7 References	37
1.1.8 Sample Questions	37
1.2 Determine and assess appropriate interface types for various environments	39
1.2.1 Layer 2 interfaces	40
1.2.2 Layer 3 interfaces	40
1.2.3 Virtual Wire interfaces	40
1.2.4 Tap interfaces	41
1.2.5 Subinterfaces	41
1.2.6 Tunnel interfaces	44
1.2.7 Aggregate interfaces	45

1.2.8 Loopback interfaces	45
1.2.9 Decrypt mirror interfaces	45
1.2.10 VLAN interface	46
1.2.11 References	46
1.2.12 Sample Questions	47
<b>1.3 Identify decryption deployment strategies</b>	<b>47</b>
1.3.1 Risks and implications of enabling decryption	47
1.3.2 Use cases	48
1.3.3 Decryption Types	50
1.3.4 Decryption Profiles and certificates	51
1.3.5 Create decryption policy in the firewall	53
1.3.6 Configure SSH proxy	55
1.3.7 References	56
1.3.8 Sample Questions	56
<b>1.4 Enforce User-ID</b>	<b>57</b>
1.4.1 Methods of building user-to-IP mappings	57
1.4.2 Determine if User-ID agent or agentless should be used	60
1.4.3 Compare and contrast User-ID agents	60
1.4.4 Methods of User-ID redistribution	60
1.4.5 Methods for group mapping	62
1.4.6 Server Profile and Authentication Profile	63
1.4.7 References	64
1.4.8 Sample Questions	65
<b>1.5 Determine when to use the Authentication policy and methods for doing so</b>	<b>66</b>
1.5.1 Purpose of, and use case for, the Authentication policy	66
1.5.2 Dependencies	69
1.5.3 Captive Portal versus GP Client	71
1.5.5 Sample Questions	73
<b>1.6 Differentiate between the fundamental functions that reside on the management plane and data plane</b>	<b>75</b>

1.6.1 References	77
1.6.2 Sample Questions	77
<b>Domain 2- Deploy and Configure Core Components</b>	<b>79</b>
2.1 Configure Management Profiles	79
2.1.1 Interface Management Profile	79
2.1.2 SSL/TLS profile	79
<b>2.1.3 References</b>	<b>80</b>
2.1.4 Sample Questions	80
2.2 Deploy and configure Security Profiles	81
2.2.1 Custom configuration of different Security Profiles and Security Profile Groups	81
2.2.2 Relationship between URL filtering and credential theft prevention	88
2.2.3 Use of username and domain name in HTTP header insertion	90
2.2.4 DNS Security	91
2.2.5 How to tune or add exceptions to a Security Profile	91
2.2.6 Compare and contrast threat prevention and advanced threat prevention	94
2.2.7 Compare and contrast URL Filtering and Advanced URL Filtering	95
2.2.8 References	96
2.2.9 Sample Questions	97
2.3 Configure zone protections, packet buffer protection, and DoS protection	99
2.3.1 References	102
2.3.2 Sample Questions	102
2.4 Define the initial design/deployment configuration of a Palo Alto Network firewall	103
2.4.1 Considerations for Advanced HA Deployments	103
2.4.2 Implement an HA Pair	103
2.4.3 Implement Zero Touch Provisioning	104
2.4.4 Configure Bootstrapping	104
2.4.5 References	106
2.4.6 Sample Questions	106
2.5 Configure authorization, authentication, and device access	107

2.5.1 Role-based access control for authorization	107
2.5.2 Different methods used to authenticate	108
2.5.3 The Authentication Sequence	112
2.5.4 The device access method	112
2.5.5 References	112
2.5.6 Sample Questions	113
2.6 Configure and manage certificates	113
2.6.1 Certificate Usage	113
2.6.2 Certificate Profiles	115
2.6.3 Certificate Chains	115
2.6.4 References	115
2.6.5 Sample Questions	116
2.7 Configure routing	118
2.7.1 Dynamic routing	118
2.7.2 Redistribution Profiles	123
2.7.3 Static routes	123
2.7.4 Route monitoring	124
2.7.5 Policy-based forwarding	124
2.7.6 Virtual routers versus logical routers	124
2.7.7 References	126
2.7.8 Sample Questions	126
2.8 Configure NAT	128
2.8.1 NAT policy rules	128
2.8.2 Security rules	128
2.8.3 Source NAT	128
2.8.4 No-NAT Policies	129
2.8.5 Use session browser to find NAT rule name	130
2.8.6 U-Turn NAT	132
2.8.7 Check HIT counts	134

2.8.7 Reference	138
2.8.8 Sample Questions	139
<b>2.9 Configure site-to-site tunnels</b>	<b>140</b>
2.9.1 IPsec components	140
2.9.2 Static peers and dynamic peers for IPsec	141
2.9.3 IPsec tunnel Monitor Profiles	142
2.9.4 IPsec tunnel testing	143
2.9.5 Generic Routing Encapsulation	144
2.9.6 One-to-one and one-to-many tunnels	145
2.9.7 Determine when to use proxy IDs	145
2.9.8 References	147
<b>2.10 Configure service routes</b>	<b>148</b>
2.10.1 Default service routes	148
2.10.2 Custom service routes	150
2.10.3 Destination service routes	150
2.10.4 Custom routes for different virtual systems versus destination routes	151
2.10.5 How to verify service routes	153
<b>2.10.6 References</b>	<b>153</b>
2.10.7 Sample Questions	153
<b>2.11 Configure application-based QoS</b>	<b>154</b>
2.11.1 Enablement requirements	154
2.11.2 QoS policy rule	154
2.11.3 Add Differentiated Services Code Point/ToS component	156
2.11.4 QoS profile	156
2.11.5 Determine how to control bandwidth use on a per-application basis	157
2.11.6 Use QoS to monitor bandwidth utilization	161
2.11.6 References	162
2.11.7 Sample Questions	163
<b>Domain 3- Deploy and Configure Features and Subscriptions</b>	<b>164</b>

3.1 Configure App-ID	164
3.1.1 Create Security rules with App-ID	164
3.1.2 Convert port and protocol rules to App-ID rules	167
3.1.3 Identify the impact of application override to overall firewall functionality	174
3.1.4 Create custom apps and threats	175
3.1.5 Review App-ID dependencies	175
3.1.6 References	176
3.1.7 Sample Questions	177
3.2 Configure GlobalProtect	179
3.2.1 GlobalProtect licensing	179
3.2.2 Configure the gateway and portal	179
3.2.3 GlobalProtect agent	181
3.2.4 Differentiate between logon methods	181
3.2.5 Configure clientless VPN	181
3.2.6 HIP	181
3.2.7 Configure multiple gateway agent profiles	182
3.2.8 Split tunneling	183
3.2.9 References	183
3.2.10 Sample Questions	184
3.3 Configure decryption	185
3.3.1 Inbound decryption	185
3.3.2 SSL Forward Proxy	186
3.3.3 SSL decryption exclusions	186
3.3.4 SSH Proxy	186
3.3.5 References	186
3.3.6 Sample Questions	187
3.4 Configure User-ID	187
3.4.1 User-ID agent and agentless	187
3.4.2 User-ID group mapping	187

3.4.3 Shared User-ID mapping across virtual systems	188
3.4.4 Data redistribution	188
3.4.5 User-ID methods	189
3.4.6 Benefits of using dynamic user groups in policy rules	190
3.4.7 Requirements to support DUGs	193
3.4.8 How GlobalProtect internal and external gateways can be used	196
<b>3.5 Configure Wildfire</b>	<b>196</b>
3.5.1 Configure a WildFire submission profile and add it to the Security rule	196
3.5.2 Configure a WildFire action profile and add it to the Security rule	198
3.5.3 Review the WildFire submissions and verdicts	201
3.5.4 Review WildFire signature actions	202
3.5.5 Supported file types and file sizes	202
3.5.6 Configure WildFire update schedule	206
3.5.7 Configure forwarding decrypted traffic to WildFire	207
3.5.8 Sample Questions	208
<b>Domain 4- Deploy and Configure Firewalls Using Panorama</b>	<b>211</b>
4.1 Configure templates and template stacks	211
4.1.1 Components configured in a template	211
4.1.2 How the order of templates in a stack affects the configuration push to a firewall	211
4.1.3 Overriding a template value in a stack	212
4.1.4 Configure variables in templates	212
4.1.5 Relationship between Panorama and devices for dynamic update versions, policy implementation, and HA peers	212
4.1.6 References	212
4.1.7 Sample Questions	213
4.2 Configure device groups	214
4.2.1 Device group hierarchies	214
4.2.2 Identify what device groups contain	215
4.2.3 Differentiate between different use cases for pre-rules, local rules, default rules, and post-rules	215

4.2.4 Identify the impact of configuring a primary device	216
4.2.5 Assign firewalls to device groups	218
4.3 Manage firewall configurations within Panorama	218
4.3.1 Licensing	218
4.3.2 Panorama commit recovery feature	219
4.3.3 Configuration settings for Panorama automatic commit recovery	219
4.3.4 Commit types and schedules	220
4.3.5 Configuration backups	221
4.3.6 Software and dynamic updates	221
4.3.7 Import firewall configurations into Panorama	224
4.3.8 Configure Log Collectors	225
4.3.9 Check firewall health and status from Panorama	225
4.3.10 Configure role-based access control on Panorama	226
4.3.11 References	226
4.3.12 Sample Questions	227
<b>Domain 5- Manage and Operate</b>	<b>229</b>
5.1 Manage and configure log forwarding	229
5.1.1 Identify log types and criticalities	229
5.1.2 Manage external services	232
5.1.3 Create and manage tags	236
5.1.4 Identify system and traffic issues using the web interface and CLI tools	237
5.1.5 Configure Log Forwarding Profile and device log settings	237
5.1.6 Log monitoring	240
5.1.7 Customize logging and reporting settings	240
5.1.8 References	245
5.1.9 Sample Questions	245
5.2 Plan and execute the process to update a Palo Alto Networks system	247
5.2.1 Update a single firewall	247
5.2.2 Update HA pairs	247

5.2.3 Perform Panorama push	248
5.2.4 Schedule and manage dynamic updates	248
5.2.5 References	248
5.2.6 Sample Questions	249
5.3 Manage HA functions	250
5.3.1 Link monitoring	250
5.3.2 Path monitoring	250
5.3.3 HA links	250
5.3.4 Failover	253
5.3.5 Active/active and active/passive	253
5.3.6 HA interfaces	255
5.3.7 Clustering	256
5.3.8 Election setting	259
5.3.9 References	259
5.3.10 Sample Question	261
<b>Domain 6- Troubleshooting</b>	<b>263</b>
6.1 Troubleshoot site-to-site tunnels	263
6.1.1 IPsec	263
6.1.2 GRE	263
6.1.3 One-to-one and one-to-many tunnels	264
6.1.4 Route-based versus policy-based remote hosts	264
6.1.5 Tunnel monitoring	265
6.1.6 References	265
6.2 Troubleshoot interfaces	267
6.2.1 Transceivers	268
6.2.2 Settings	268
6.2.3 Aggregate interfaces and Link Aggregation Control Protocol	271
6.2.4 Counter	271
6.2.5 Tagging	278

6.2.6 References	279
6.2.7 Sample Questions	280
6.3 Troubleshoot Decryption	280
6.3.1 Inbound decryption	283
6.3.2 SSL forward proxy	285
6.3.3 SSH proxy	285
6.3.4 Identify what cannot be decrypted and configure exclusions and bypasses	287
6.3.5 Certificates	287
6.3.6 Sample Questions	299
6.4 Troubleshoot routing	300
6.4.1 Dynamic routing	300
6.4.2 Redistribution profiles	300
6.4.3 Static routes	301
6.4.4 Route monitoring	301
6.4.5 PBF	302
6.4.6 Multicast routing	302
6.4.7 Service routes	304
6.5 Use logs, reports, and graphs to troubleshoot	305
6.5.1 Identify system and traffic issues using the web interface and CLI tools	305
6.5.2 Create and interpret reports	312
6.5.3 Create and interpret graphs	316
6.5.4 References	319
6.5.5 Sample Questions	321
6.6 Troubleshoot resource protections	322
6.6.1 Zone Protection profiles	322
6.6.2 DoS protections	322
<b>1. Session Table Full</b>	<b>323</b>
6.6.3 Packet buffer protections	325
6.6.5 Sample Questions	326

<b>6.7 Troubleshoot GlobalProtect</b>	<b>326</b>
6.7.1 Portal and Gateway	327
6.7.2 Access to resources	329
6.7.3 GlobalProtect client	331
<b>6.8 Troubleshoot Policies</b>	<b>333</b>
6.8.1 NAT policies	333
6.8.2 Security policies	335
6.8.3 Decryption policies	336
6.8.4 Authentication policies	338
<b>6.9 Troubleshoot HA functions</b>	<b>339</b>
6.9.1 Monitor	339
6.9.2 Failover triggers	341
<b>Appendix A: Sample Questions with Answers</b>	<b>343</b>
Domain 1	343
Domain 1.1.8	343
Domain 1.2.12	345
Domain 1.3.8	345
Domain 1.4.8	345
Domain 1.5.5	347
Domain 1.6.2	348
Domain 2	349
Domain 2.2.9	349
Domain 2.3.2	351
Domain 2.4.6	352
Domain 2.5.6	353
Domain 2.6.5	353
Domain 2.7.5	355
Domain 2.8.9	357
Domain 2.10.7	357

Domain 2.11.8	358
Domain 3	359
Domain 3.1.7	359
Domain 3.2.10	361
Domain 3.3.6	361
Domain 3.5.8	362
Domain 4	363
Domain 4.1.7	363
Domain 4.3.12	364
Domain 5	365
Domain 5.1.9	365
Domain 5.2.6	366
Domain 5.3.10	367
Domain 6	368
Domain 6.2.7	368
Domain 6.3.6	369
Domain 6.5.5	370
Domain 6.6.4	371
<b>Appendix B: Sample Test</b>	<b>372</b>
<b>Appendix C: Answers to the Sample Test</b>	<b>383</b>
<b>Appendix D: Glossary</b>	<b>393</b>

# Palo Alto Networks PCNSE Study Guide

Welcome to the *Palo Alto Networks PCNSE Study Guide*. The purpose of this guide is to help you prepare for your PCNSE exam and achieve your PCNSE credential. This study guide is a summary of the key topic areas that you are expected to know to be successful at the PCNSE exam. It is organized based on the exam blueprint and key exam objectives.

## Overview

The Palo Alto Networks Certified Network Security Engineer (PCNSE) is a formal, third-party proctored certification that indicates that those who have achieved it possess the in-depth knowledge to design, install, configure, maintain, and troubleshoot most implementations based on the Palo Alto Networks platform.

This exam will certify that the successful candidate has the knowledge and skills necessary to implement the Palo Alto Networks Next-Generation Firewall PAN-OS 10.1 platform in any environment.

More information is available from Palo Alto Networks at:

<https://www.paloaltonetworks.com/services/education>

## Exam Details

**Certification name:** Palo Alto Networks Certified Network Security Engineer

**Delivered through Pearson VUE:** [www.pearsonvue.com/paloaltonetworks](http://www.pearsonvue.com/paloaltonetworks)

**Exam series:** PCNSE

**Seat time:** 80 minutes

**Number of items:** 75

**Format:** Multiple Choice, Scenarios with Graphics, and Matching

**Languages:** English and Japanese

Palo Alto Networks Certified Network Security Engineer - PCNSE	
Domain	Weight (%)
Core Concepts	12
Deploy and Configure Core Components	20
Deploy and Configure Features and Subscriptions	17
Deploy and Configure Firewalls Using Panorama	17
Manage and Operate	16
Troubleshooting	18
Total	100

## Audience

The PCNSE exam should be taken by anyone who wants to demonstrate a deep understanding of Palo Alto Networks technologies, including customers who use Palo Alto Networks products, value-added resellers, pre-sales system engineers, system integrators, and support staff.

## Qualifications

Candidates should have 3 to 5 years' experience working in the networking or security industries and the equivalent of 6 to 12 months' experience deploying and configuring Palo Alto Networks Next-Generation Firewalls within the Palo Alto Networks product portfolio.

## Skills Required

- You can plan, deploy, configure, operate, and troubleshoot Palo Alto Networks product portfolio components.
- You have product expertise and understand the unique aspects of the Palo Alto Networks product portfolio and how to deploy one appropriately.
- You understand networking and security policies used by PAN-OS software.

## Recommended Training

Palo Alto Networks strongly recommends that you attend the following instructor-led training courses or equivalent virtual digital learning courses:

- Firewall Essentials: Configuration and Management (EDU-210) or digital learning
- Panorama: Managing Firewalls at Scale (EDU-220) or digital learning
- Optional training: Firewall: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214) or digital learning
  - Firewall: Troubleshooting (EDU-330)

After you have completed the courses, practice on the platform to master the basics. Use the following resources to prepare for the exam. All resources can be found here:

<https://www.paloaltonetworks.com/services/education/certification.html#pcnse>

- Cybersecurity Skills Practice Lab
- PCNSE Study Guide and Practice Exam
- Administrator's Guide: Specific configuration information and "best practice" settings
- Preparation videos and tutorials

## About This Document

Efforts have been made to introduce all relevant information that might be found in a PCNSE Certification Test. However, other related topics also may appear on any delivery of the exam. This document should not be considered a definitive test preparation guide, but an introduction to the knowledge required. Note that these guidelines may change at any time without notice. This document contains many references to outside information that should be considered essential to completing your understanding.

## Disclaimer

This study guide is intended to provide information about the objectives covered by this exam, related resources, and recommended courses. The material contained within this study guide is not intended to guarantee that a passing score will be achieved on the exam. Palo Alto Networks recommends that candidates thoroughly understand the objectives indicated in this guide and use the resources and courses recommended in this guide where needed to gain that understanding.

## Preliminary Score Report

The score report notifies candidates that, regardless of pass or fail results, an exam score may be revised any time after testing if there is evidence of misconduct, scoring inaccuracies, or aberrant response patterns.

# Domain 1 – Core Concepts

## 1.1 Identify how Palo Alto Networks products work together to improve PAN-OS services

### 1.1.1 Security components

#### *The Palo Alto Networks Cybersecurity Portfolio*

The Palo Alto Networks cybersecurity portfolio is organized into three offerings: Strata for enterprise security, Prisma for cloud security, and Cortex for security operations. The following sections describe how they work together to address some of the world's greatest security challenges.



#### *Strata: Enterprise Security*

Strata prevents attacks with the industry-leading network security suite that enables organizations to embrace network transformation while consistently securing users, applications, and data, no matter where they reside. The suite brings together the following:

#### *Machine Learning-Powered Next-Generation Firewalls*

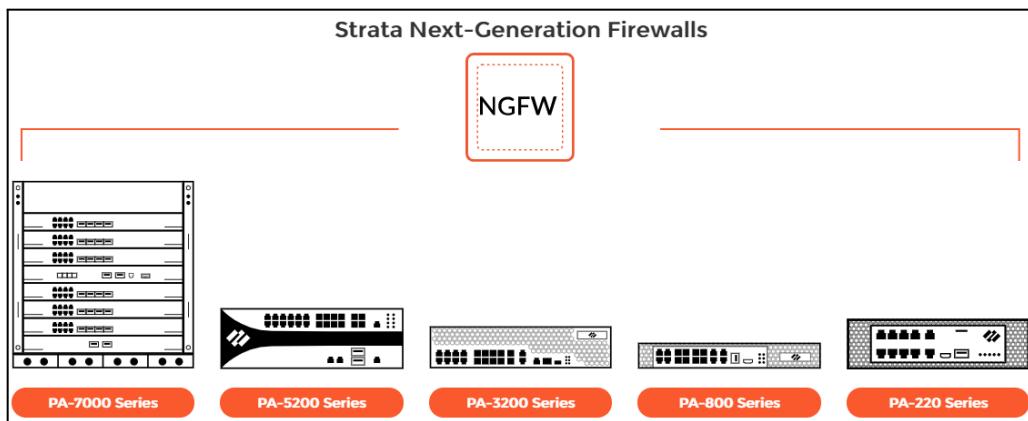
Palo Alto Networks machine learning (ML)-powered Next-Generation Firewalls (NGFWs) enable you to adopt best practices using application, user, and content-based policies to minimize opportunities for attack. They are available as physical appliances, virtualized appliances, and cloud-delivered services, all of which are managed with Panorama to ensure a consistent security stance.

The firewalls secure your business with a prevention-focused architecture and integrated innovations that are easy to deploy and use. Palo Alto Networks ML-powered NGFWs detect known and unknown threats, including those within encrypted traffic, using intelligence generated across many thousands of customer deployments. The firewalls reduce risks and prevent a broad range of attacks. For example, they enable users to access data and applications based on business requirements, and they stop credential theft and an attacker's ability to use stolen credentials.

With these ML-powered NGFWs, it is quick and easy to create and maintain Security rules that mirror business policies and adapt to your dynamic environment. Automation reduces manual effort and accelerates response times with automated, policy-based actions and workflows that can be integrated with your administrative tools, such as ticketing services via a RESTful API.

The family of NGFWs includes the following:

**PA-Series:** Physical appliances enable you to stay ahead of unknown threats, see everything (including internet of things [IoT]), and reduce errors with automatic policy recommendations. Form factors can provide consistent protection for your entire network perimeter, from your headquarters, data center, and office campus to your branch offices and mobile and remote workforce. The models available include the PA-220, PA-800, PA-3200, PA-5200, and PA-7000 Series.



**VM-Series:** The virtualized version of the ML-powered NGFW makes it easy to protect your private and public cloud deployments with segmentation and proactive threat prevention.



The VM-Series firewalls support the following virtualization environments:

- Amazon Web Services
- Cisco ACI
- Citrix NetScaler SDX
- Google CloudPlatform
- Kernel-Based Virtual Machine (KVM)
- Microsoft Azure and Microsoft Hyper-V
- OpenStack
- VMware ESXi, VMware NSX, and VMware vCloud Air

### ***Network Security Management: Panorama***

Panorama offers easy-to-implement and centralized management features to gain insight into network-wide traffic and threats and to administer your NGFWs everywhere. Panorama is available in both appliance and virtual forms. Panorama provides the following:

- **Policy management:** Create and edit Security rules in accordance with your organization's Security policy across your firewall deployment from one central location.
- **Centralized visibility:** Get deep visibility and comprehensive insights into network traffic and threats via the Application Command Center (ACC).

- **Network security insights:** Leverage the automated correlation engine to reduce data clutter, identify compromised hosts, and reveal malicious behavior.
- **Automated threat response:** Automate and customize security workflows using REST APIs to integrate with third-party systems and your existing operational tools.
- **Network security management:** Centrally manage devices and security configurations for all groups of firewalls.
- **Enterprise-level reporting and administration:** Simplify reporting with aggregated logs of managed NGFWs, User-ID redistribution to managed devices, and implementation of enterprise-level administration.



### *Prisma: Cloud Security*

Prisma Cloud delivers complete security across the development lifecycle on any cloud, enabling you to develop cloud-native applications with confidence. The Prisma suite includes Prisma Cloud, Prisma Access Secure Access Service Edge (SASE), Prisma SaaS, and the VM-Series ML-powered NGFWs.

#### *Prisma Cloud*

Prisma Cloud is a Cloud Security Posture Management and Cloud Workload Protection Platform that provides comprehensive visibility and threat detection across your organization's hybrid, multi-cloud infrastructure.

Prisma Cloud taps into the cloud providers' APIs for read-only access to your network traffic, user activity, and configuration of systems and services. It then correlates these disparate datasets to help cloud compliance and security analytics teams prioritize risks and quickly respond to issues. It also uses an agent-based approach to secure your host, container, and serverless computing environments against vulnerabilities, malware, and compliance violations.

The cloud-native security platform provides the following:

- **Comprehensive, cloud-native security:** Delivers complete visibility, automation, detection, and response across any compute, network, or cloud service for SecOps and DevOps teams. It enforces hundreds of out-of-the-box governance policies that help ensure compliance and enforce good behavior.
- **Full lifecycle protection:** Eliminates issues early and prevents alert fatigue by seamlessly integrating security early and throughout the application lifecycle, from IDE, SCM, CI/CD, and registries to runtime. It leverages continuous vulnerability management and automated risk prioritization across the entire cloud-native stack and lifecycle, and it easily investigates any incident.
- **Protection across any cloud:** Monitors, secures, and maintains compliance on multi- and hybrid-cloud environments with a single integrated platform. It leverages purpose-built solutions for public clouds, such as Amazon Web Services, Google CloudPlatform, and Microsoft Azure, and it secures your on-premises investments, such as OpenShift.

Prisma Cloud secures the following cloud-native infrastructures:

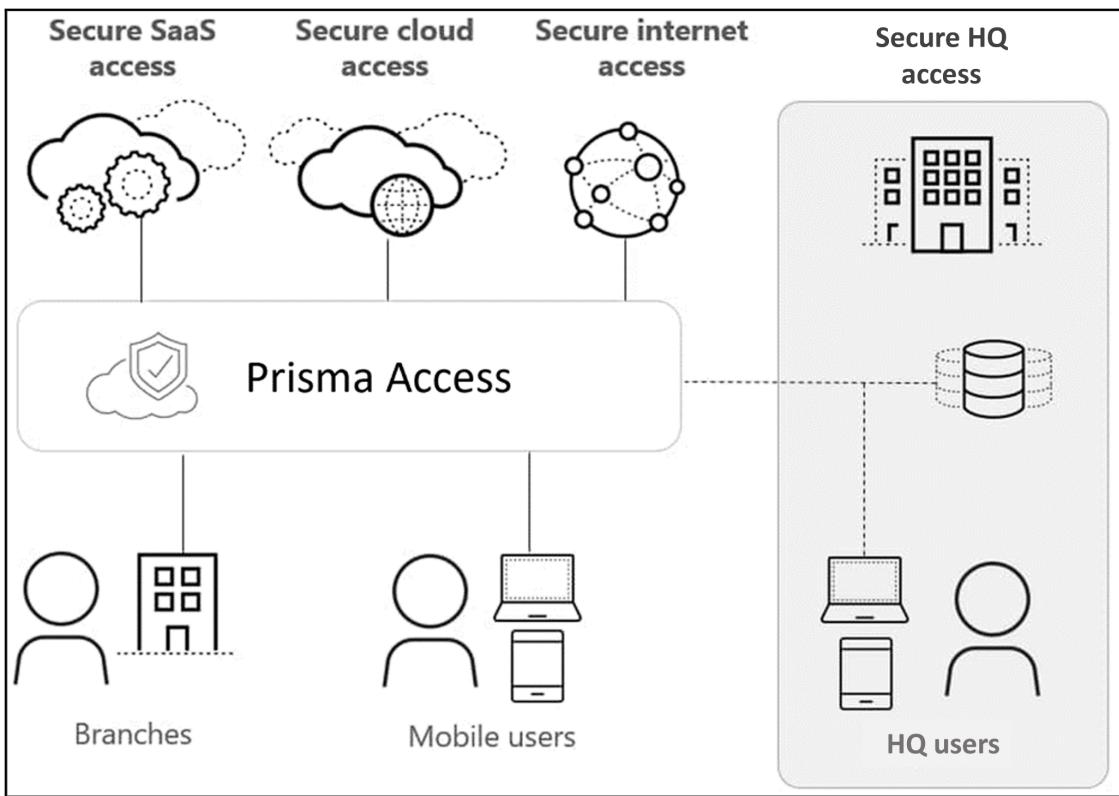
- Alibaba Cloud
- Amazon Web Services
- Docker EE
- Google CloudPlatform
- IBM Cloud
- Kubernetes
- Microsoft Azure
- Rancher
- Red Hat OpenShift
- VMware Tanzu

### ***Prisma Access (SASE)***

Global expansion, mobile workforces, and cloud computing are changing the ways that organizations implement and deploy applications. Prisma Access provides the protection you need, where you need it. Prisma Access delivers a SASE that provides globally distributed networking and security to all your users and applications.

SASE converges the capabilities of wide area networks (WANs) with network security to support the needs of the digital enterprise. These disparate networks and security services include software-defined wide area networks (SD-WANs), secure web gateways, cloud access security brokers (CASBs), software-defined perimeters, Domain Name System (DNS) protection, and firewall as a service.

Your users connect to Prisma Access to safely access the internet and cloud and data center applications, regardless of their location.



### ***Prisma SaaS***

Prisma SaaS (formerly known as Aperture) is a multimode CASB service that allows you to govern sanctioned software as a service (SaaS) application use across all users in your organization — and prevent risk from breaches and noncompliance. The service enables you to discover and classify data stored across supported SaaS applications, protect sensitive data from accidental exposure, identify and protect against known and unknown malware, and perform user activity monitoring to identify potential misuse or data exfiltration. It delivers complete visibility and granular enforcement across all user, folder, and file activity within sanctioned SaaS applications.

### ***VM-Series NGFWs***

VM-Series is the virtualized form factor of the Palo Alto Networks ML-powered NGFW. To meet the growing need for inline security across diverse cloud and virtualization use cases, you can deploy the VM-Series firewall on a wide range of private and public cloud computing environments. See the description in the [“Strata: Enterprise Security”](#) section.

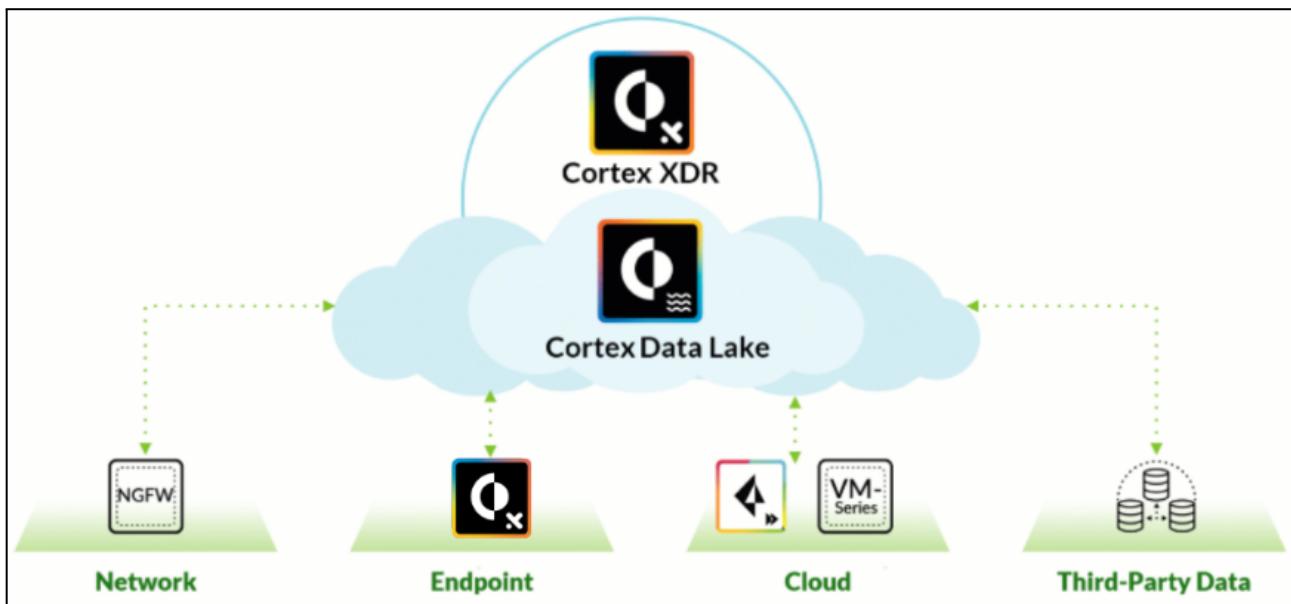


### ***Cortex: Security Operations***

Cortex is the industry's most comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities. The Cortex product suite includes Cortex XDR, Cortex XSOAR, Cortex Data Lake, and AutoFocus.

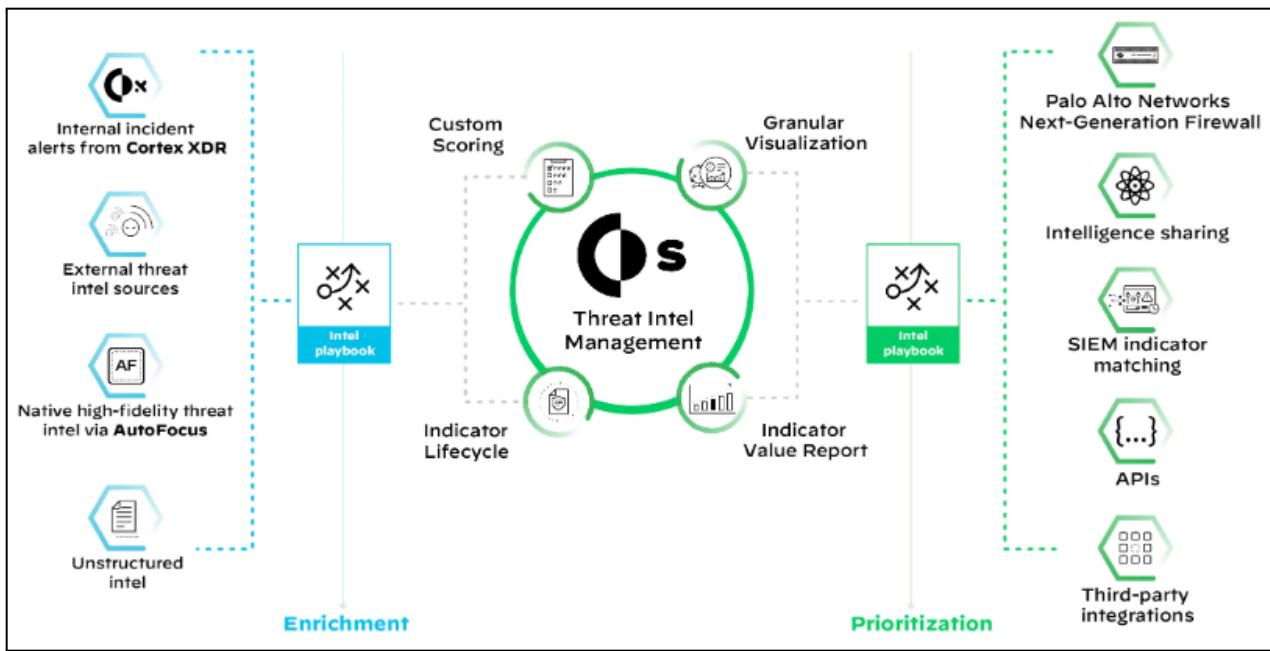
## Cortex XDR

Cortex XDR is the industry's first extended detection and response platform that runs on integrated endpoint, network, and cloud data to reduce noise and focus on real threats. It provides complete visibility over network traffic, user behavior, and endpoint activity. It simplifies your threat investigations by correlating logs from your sensors to reveal threats and their timelines, which enables you to easily identify the root cause of every alert. It also allows you to perform immediate response actions. Finally, to stop future attacks, you can proactively define indicators of compromise and behavioral indicators of compromise to detect and respond to malicious activity. The following diagram depicts the Cortex XDR architecture.



## Cortex XSOAR

Cortex XSOAR is the industry's first extended Security Orchestration, Automation, and Response (SOAR) platform with native threat intelligence management. The SOAR technology can automate up to 95 percent of all response actions that require human review, thus allowing overloaded security teams to focus on more crucial tasks. Cortex XSOAR integrates with a wide variety of products to provide enhanced automation and response across processes using multiple products. The following illustration depicts the Cortex XSOAR architecture, with its engine in the center, information sources on the left, and potential consumers on the right.

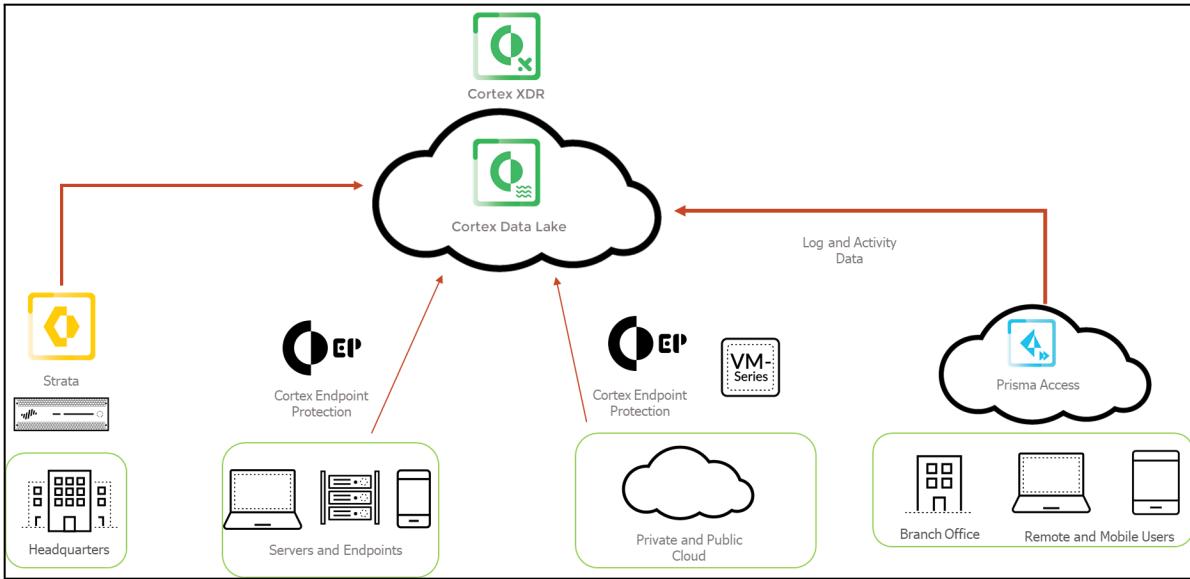


### Cortex Data Lake

Cortex Data Lake enables you to easily collect large volumes of log data so that innovative applications can gain insight from your environment. You can simplify your log infrastructure, automate log management, and use your data to prevent attacks more effectively. Cortex Data Lake can do the following:

- Radically simplify your security operations by collecting, integrating, and normalizing your enterprise's security data
- Effortlessly run advanced artificial intelligence and ML with cloud-scale data and compute
- Constantly learn from new data sources to evolve your defenses

The following illustration depicts Cortex Data Lake as the central destination for information consolidation from many Palo Alto Networks products.



The following products use Cortex Data Lake:

- Palo Alto Networks NGFWs and Prisma Access
- NGFWs and Panorama for network security management with the ability to connect to the cloud service
- NGFWs and Panorama running PAN-OS 8.0.5+
- Panorama with the cloud services plugin installed
- Old versions of Palo Alto Networks Traps for endpoint protection and response
- Traps running version 5.0+ with the Traps management service
- Cortex endpoint protection
- Cortex XDR
- Cortex XDR application (Cortex endpoint protection agent included)

### 1.1.2 Firewall components

#### Security Zones

Palo Alto Networks firewalls are zone-based. Zones designate a network segment where all nodes share similar network security requirements (i.e., users, data centers, demilitarized zone (DMZ) servers, and remote users). The firewall security model is based on evaluating traffic as it passes from one zone to another. These zones act as a logical way to group physical and virtual interfaces. Zones are required to control and log the traffic that traverses the interfaces. All defined interfaces should be assigned a zone that marks all traffic coming to or from the interface. Zones are defined for specific interface types (i.e., Tap, virtual wire, Layer 2, or Layer 3) and can be assigned to multiple interfaces of the same type only. An interface can be assigned only to a single zone.

All sessions on the firewall are defined by source and destination zones. Rules can use these defined zones to allow or deny traffic, apply Quality of Service (QoS) policies, or perform network address translation (NAT). All traffic can flow freely within a zone and is referred to as *intrazone* traffic. Traffic between zones (called

*interzone* traffic) is denied by default. Security policy rules are required to modify these default behaviors. Traffic can flow between zones only if a defined Security policy rule matches and allows the traffic. For *interzone* traffic, Security policy rules must reference a source zone and destination zone (not interfaces) to allow or deny traffic.

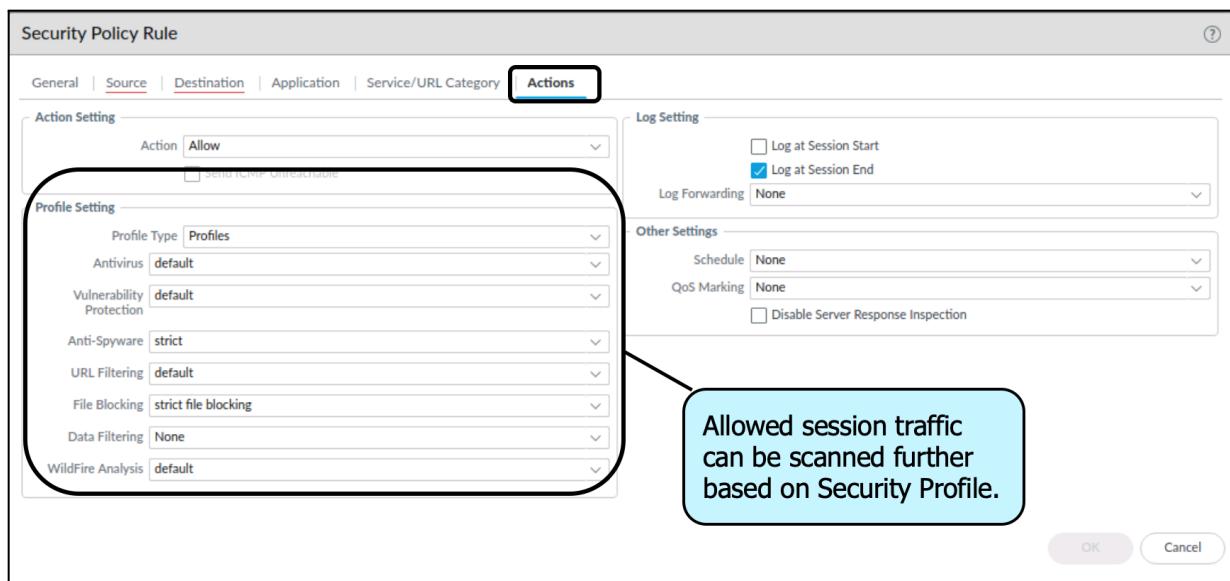
Security policies are used to create a positive (allow list) and negative (block list) enforcement model for traffic flowing through the firewall. These rules are set from the top down, and the first rule with the appropriate matching conditions will allow or deny matching traffic. If logging is enabled on the matching rule, and the traffic crosses a zone, the action for that session is logged. These logs are extremely useful for adjusting the positive/negative enforcement model. The log information can be used to characterize traffic, thus providing specific use information and allowing precise policy creation and control. Log entries can be forwarded to external locations, including email and web servers, syslog servers, Panorama, and Cortex Data Lake. Palo Alto Networks firewall logs, the ACC, App Scope, and other reporting tools all work to precisely describe traffic and use patterns.

### **Security Policy**

The Security policy consists of Security rules that serve as the basis of the firewall's ability to enable or block sessions. You can use multiple match conditions to create these rules. Traffic-matching criteria can include security zones, source and destination IP addresses, and source and destination devices, as well as information about the application (App-ID), source user (User-ID), service (port), HIP match, and URL. App-ID ensures positive application identification, regardless of their attempts to hide. Allowed session traffic also can be scanned based on Security Profiles (Content-ID) to identify unwanted traffic content. These profiles use signatures to identify known threats. Unknown threats are identified by WildFire, which creates signatures to turn them into known threats.

Here are examples of the steps to create a Security policy rule and choose profile settings:

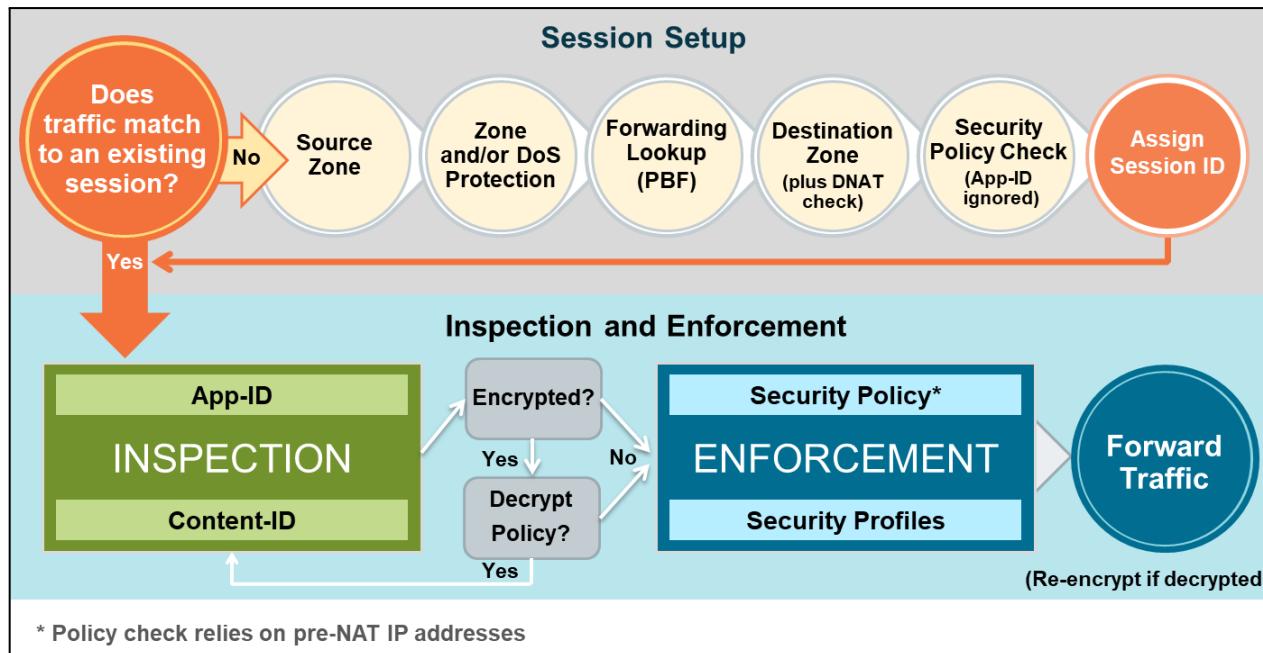
The screenshot shows the 'Security Policy Rule' dialog box with the 'General' tab selected. The 'Name' field is set to 'Security Policy Rule'. The 'Rule Type' dropdown is set to 'universal (default)'. The 'Description' and 'Tags' fields are empty. The 'Group Rules By Tag' dropdown is set to 'None'. The 'Audit Comment' field is empty. At the bottom, there is an 'Audit Comment Archive' link and 'OK' and 'Cancel' buttons.



### Traffic Processing Sequence

The following image can help you visualize Palo Alto Networks firewall processes. Understanding this traffic flow can help you better create an initial configuration and adjust the rules after installation. Note that the following image is a simplified version of the complete flow, as shown in <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>.

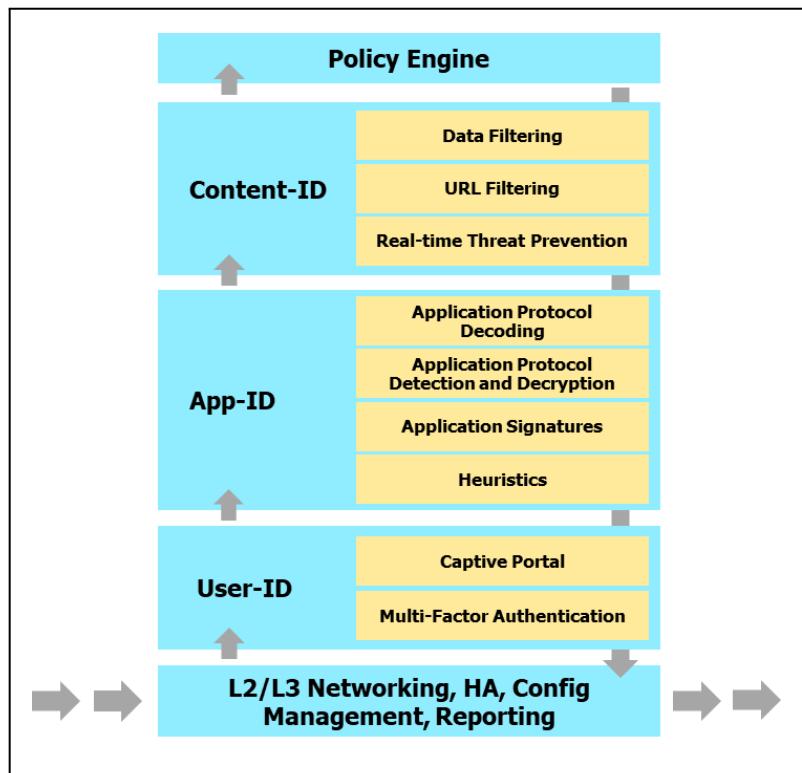
Advanced analysis and discussion of the firewall flow logic is included in the *Firewall: Troubleshooting* (EDU-330) course.



The Palo Alto Networks firewall was designed to use an efficient system known as *next-generation processing*. Next-generation processing enables packet evaluation, application identification, policy decisions, and content scanning in a single, efficient processing pass.

Palo Alto Networks firewalls contain the following next-generation features:

- **App-ID:** Scans traffic to identify the application involved, regardless of the protocol or port number used
- **Content-ID:** Scans traffic for security threats (e.g., data leak prevention and URL filtering, viruses, spyware, unwanted file transfers, specific data patterns, vulnerability attacks, and appropriate browsing access)
- **User-ID:** Matches a user to an IP address (or multiple IP addresses), allowing your Security policy to be based on who is behind the traffic, not the device



### 1.1.3 Panorama components

#### *Panorama Overview*

Without Panorama, Palo Alto Networks firewalls have no direct knowledge of each other and must be managed as independent entities. Panorama offers several important integration functions that provide enterprise management for multiple firewalls.

The Panorama management server provides centralized monitoring and management of multiple Palo Alto Networks NGFWs and of WildFire appliances and appliance clusters. It provides a single location for you to oversee all applications, users, and content traversing your network, and then it uses this knowledge to create application enablement policies that protect and control the network. Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

The PCNSE certification requires candidates to have knowledge of Panorama firewall management functions. The following sections review these management concepts, but they do not cover all Panorama features.

Panorama uses *device groups* and *templates* to group firewalls into logical sets that require similar configuration. You use device groups and templates to centrally manage all configuration elements, policies, and objects on the managed firewalls. Panorama also enables you to centrally manage licenses, software (e.g., PAN-OS software, secure sockets layer- virtual private network (SSL-VPN) client software, and GlobalProtect agent/app software), and content updates (e.g., application and threat, WildFire, and antivirus updates).

Panorama's management web interface looks like the firewall's management web interface.

Firewall menus from the management web interface:



Panorama menus from the management web interface:



You can use the Network and **Device** tabs under Templates in Panorama to deploy a common base configuration to multiple firewalls with similar settings. To do this, you use a template or a template stack (a combination of templates). When you manage firewall configurations with Panorama, you use a combination of device groups (to manage shared policies and objects) and templates (to manage shared device and network settings).

#### 1.1.4 PAN-OS subscriptions and the features they enable

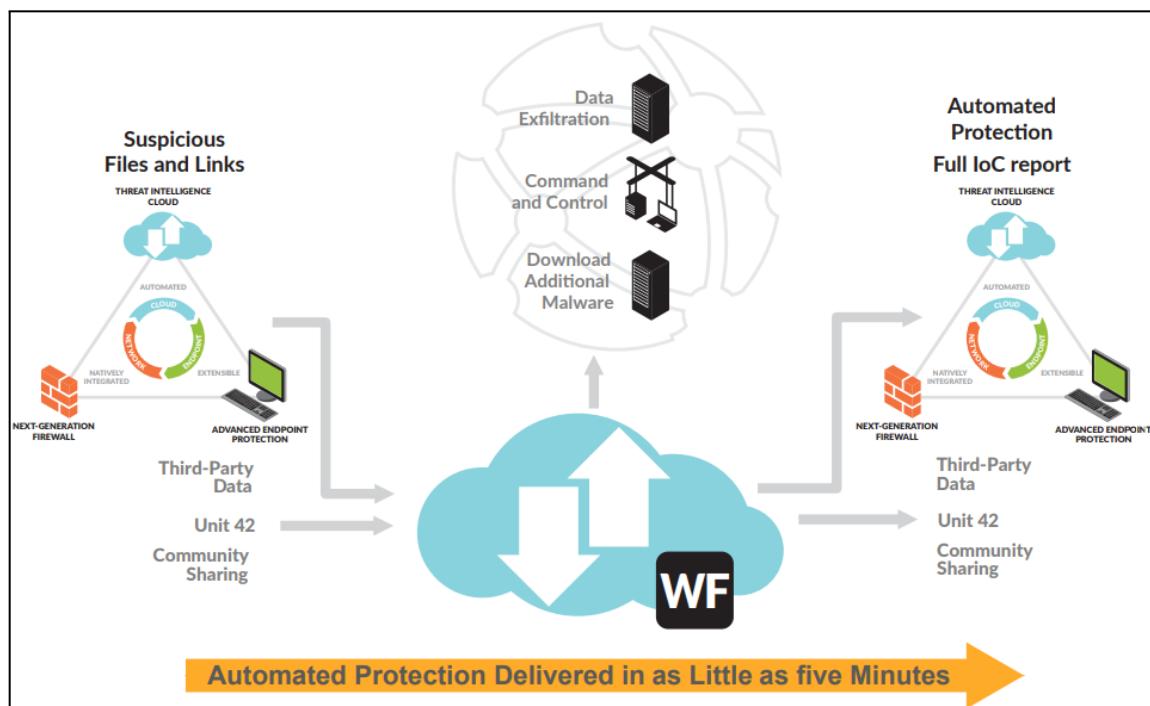
##### **Security Subscriptions**

Palo Alto Networks ML-powered NGFWs have a comprehensive range of security subscriptions natively integrated to provide comprehensive security that is automated and driven by ML. The subscriptions offered include the following:

- **Threat Prevention:** Go beyond typical intrusion prevention systems (IPSs) to inspect all traffic for threats — regardless of port, protocol, or encryption — and automatically block known vulnerabilities, malware, exploits, spyware, and command and control (C2). Customers can import, sanitize, manage, and completely automate workflows to rapidly apply IPS signatures in popular formats such as SNORT and Suricata, thus adding to our existing leading threat coverage.
- **URL Filtering:** Protect your organization against web-based threats such as phishing, malware, and C2. Inline ML instantly identifies and prevents new and unknown malicious websites before they can be accessed by users. Web Security rules are an extension of your NGFW policy, thus reducing complexity by giving you a single policy set to manage.

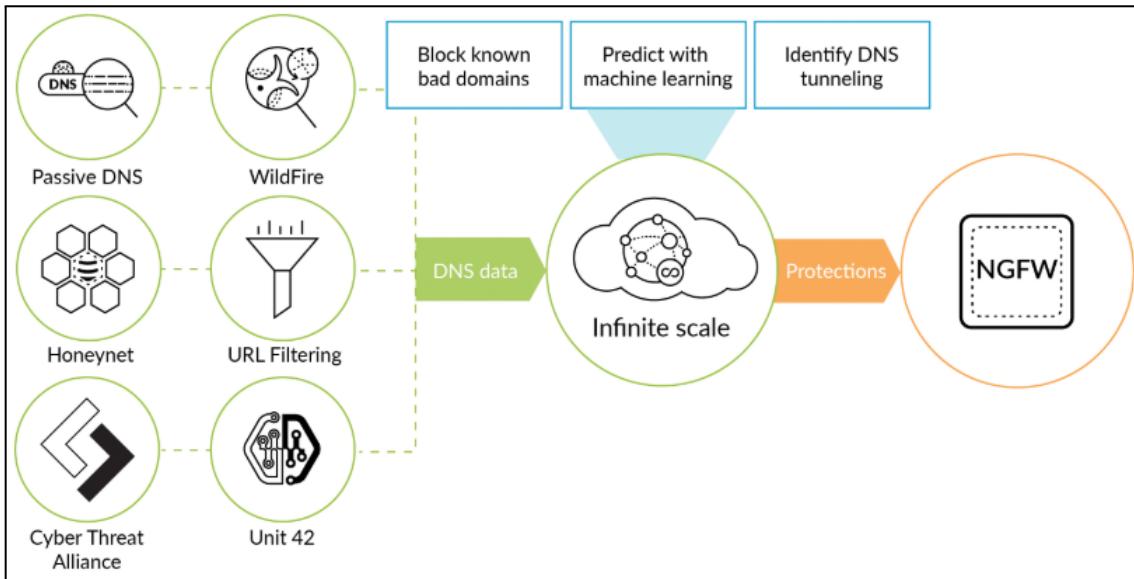
URL Filtering provides the following benefits:

- Reduces infection risk from dangerous websites and protects users and data from malware and credential-phishing pages
- Protects across the attack lifecycle through integration with WildFire and the cybersecurity portfolio
- Retains protections synchronized with the latest threat intelligence through Palo Alto Networks cloud-based URL categorization for phishing, malware, and undesired content
- Provides full visibility and threat inspection into normally opaque web traffic through granular control over SSL decryption
- WildFire:** Leverages cloud-based malware detection and multiple analysis techniques to identify and protect against unknown file-based threats while resisting attacker evasion techniques. The WildFire real-time signature streaming capability ensures that your organization is protected against previously unknown threats seconds after they are discovered. WildFire is the first to deploy inline ML modules on the NGFW to identify and prevent new and unknown file-based threats, thus protecting users before a threat can even enter your network. Basically, WildFire turns every Palo Alto Networks platform deployment into a distributed sensor and enforcement point to stop zero-day malware and exploits before they can spread and become successful. Within the WildFire environment, threats are detonated, intelligence is extracted, and preventions are automatically orchestrated across the Palo Alto Networks next-generation security product portfolio within 300 seconds of discovery anywhere in the world. The service employs a unique, multi-technique approach that combines dynamic and static analysis, innovative ML techniques, and a groundbreaking bare-metal analysis environment to detect unknown threats and prevent even the most evasive ones. The following illustration depicts WildFire, its information sources, and the services that it supports.



- DNS Security:** Applies predictive analytics, ML, and automation to block attacks that use DNS. Tight integration with the NGFW gives you automated protections and eliminates the need for independent tools. Now you can rapidly predict and prevent malicious domains, neutralize threats hidden in DNS

tunneling, and apply automation to quickly find and contain infected devices. The following illustration depicts DNS Security sources, intermediate processing of source data, and ultimate delivery to a firewall.



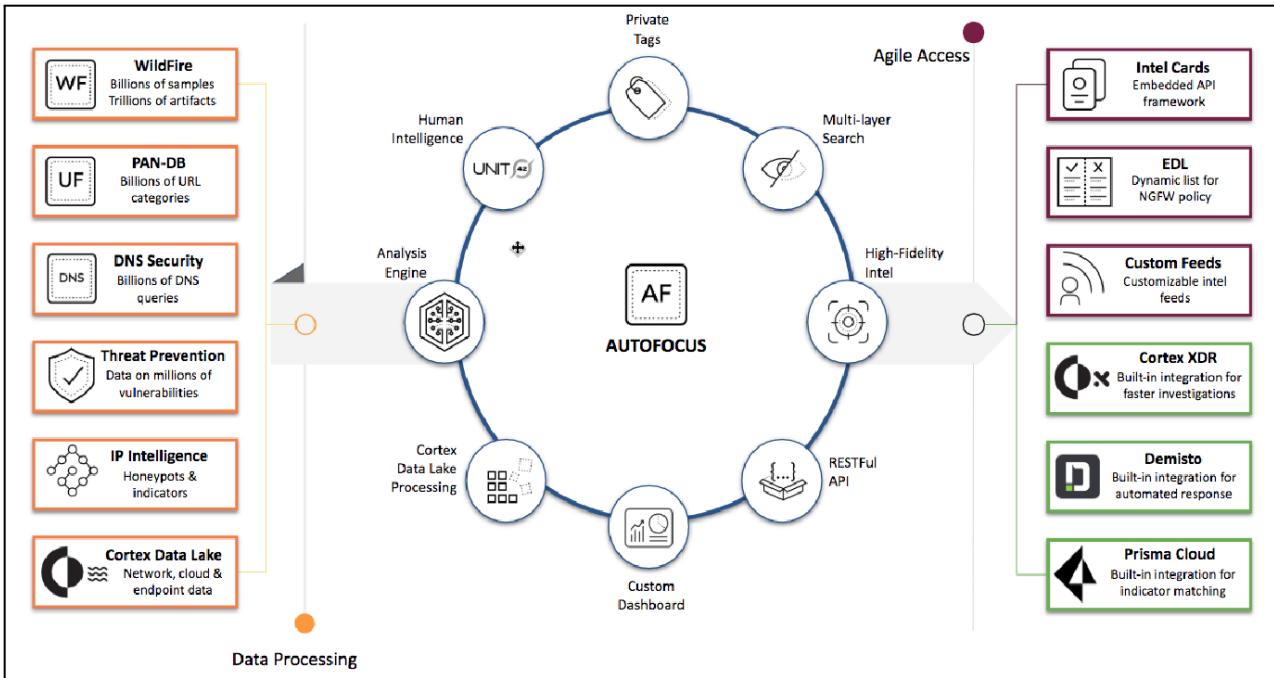
- **SD-WAN:** Connects branch offices without compromising on security. Leverage the SD-WAN subscription on your Palo Alto Networks NGFW and simply enable SD-WAN and security on a single, intuitive interface.

### *AutoFocus*

AutoFocus provides a single source for threat intelligence with unrivaled context to power up investigation, prevention, and response. AutoFocus gives you unique visibility into attacks crowdsourced from the industry's largest footprint of network, endpoint, and cloud intelligence sources. AutoFocus also:

- Enriches every threat with the deepest context from Unit 42 threat researchers
- Gives analysts a major time advantage by embedding intelligence in a custom threat feed and agile APIs

The following image shows AutoFocus as central point for many information sources, both within Palo Alto Networks and externally.



### 1.1.5 Plugin components

The VM-Series plugin is for VM-Series firewalls. It is pre-installed.

Panorama plugins are for both hardware-based firewalls and VM-Series firewalls. Panorama plugins are not built-in. You must install the plugin. The Google cloud platform (GCP) plugin on Panorama is for GCP deployments.

### 1.1.6 Heatmaps and Best Practice Assessment reports

#### *Comparing the Heatmap and BPA Reports*

The Palo Alto Networks Customer Success team is focused on ensuring that customers use their products as effectively as possible. The free Best Practice Assessment (BPA) tool for Palo Alto Networks firewalls and Panorama evaluates a device's configuration by measuring the adoption rate of a firewall's capabilities and validating whether the policies adhere to best practices. The BPA tool provides recommendations and instructions about how to remediate failed best practice checks. The goal for running the BPA tool is to reduce your attack surface. The BPA tool should be run on a scheduled basis (for example, quarterly) to ensure continuous improvement.

The two components of the BPA tool are the Security Policy Adoption Heatmap and the BPA assessment. The Heatmap analyzes a Palo Alto Networks deployment, measuring the adoption rate of features and capabilities across a targeted network infrastructure. The Heatmap can filter the information by device groups, serial numbers, zones, areas of architecture, and other categories. The results chart the progress of security improvement toward a Zero Trust network.

The BPA assessment compares a firewall or Panorama configuration against best practices and provides recommendations to strengthen your security posture by fully adopting Palo Alto Networks prevention capabilities. More than 200 security checks are performed on the firewall or Panorama configuration. A

pass/fail score is provided for each check. If a check returns a failing score, the tool provides a justification for the failing score and recommendations about how to resolve the issue.

Both components require the Tech Support File from either Panorama or a firewall to be uploaded to the Palo Alto Networks Customer Support Portal. After importing the Tech Support File, you should complete architecture mapping, which maps your existing zone names to predefined architecture classifications. Examples of architecture classifications are Enterprise – Perimeter – Internet, Internal – Core – Users, and Mobility – Remote Users/VPN.

### ***Heatmap Component***

The Heatmap measures the adoption rate of Palo Alto Networks features. The results display the adoption rate based on source zone to destination zone. Column filters are available to allow you to examine specific device groups, source zones, and destination zones.

The Heatmap measures the adoption rate of the following Palo Alto Networks firewall features:

- WildFire
- Threat Prevention (IPS)
- Anti-Spyware
- DNS Sinkhole
- Antivirus
- Vulnerability Protection
- URL Filtering
- File Blocking
- Data Filtering
- User-ID
- App-ID
- Service/Port
- Logging

## Example Heatmap Report

Security Policy Capability Adoption Heatmaps																
Documentation / Help <a href="#">?</a>												Column Filters				
Source Zone	Destination Zone				WildFire		Threat Prevention (IPS)			URL-Filtering						
		Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
Lokalnettet_L3_VPN	untrust_vr1	27	26	1	100.0	100.0	92.3	100.0	100.0	100.0	100.0	0.0	92.6	96.3	92.3	100.0
Lokalnettet_L3	untrust_vr1	18	16	2	100.0	100.0	56.3	93.8	100.0	93.8	100.0	0.0	38.9	55.6	100.0	100.0
Lokalnettet_L3_Trust_DC_VPN	untrust_vr1	6	6	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
any	untrust_vr1	5	0	5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	60.0	0.0	100.0
Kjeller_Kontor_Stue	Kjeller_Kontor_Stue	3	3	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	33.3	100.0
Clientless_VPN_Lokalnettet_L3_VPN	untrust_vr1	3	3	0	100.0	100.0	66.7	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
Clientless_VPN_Lokalnettet_L3_Trust_DC_VPN	untrust_vr1	2	2	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	50.0	100.0	100.0
Lokalnettet_L3_VPN_untrust_vr1	GP.Clientless_Portal_Management_untrust_vr1	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0
untrust_GP	untrust_GP	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0
untrust_GP_untrust_vr1	untrust_GP_untrust_vr1	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
untrust_vr1	untrust_vr1	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Garasje_Kjeller_Kontor_Stue	Garasje_Kjeller_Kontor_Stue	1	1	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0
Grand Total:		77	65	12	98.5	98.5	75.4	96.9	98.5	96.9	98.5	0.0	59.7	74.0	87.7	100.0

Some items cannot realistically be expected to reach 100 percent, such as DNS Sinkhole. DNS Sinkhole should be considered only for traffic that includes DNS queries. Another example is URL Filtering, which typically is implemented only on the perimeter. Also, you should enable Threat Prevention only on rules that allow traffic; there is no point in enabling Threat Prevention on drop or deny rules. You should focus on yellow, orange, and red highlights, which indicate gaps in security.

Zone mapping enables you to determine which traffic you want to analyze by selecting source zone and destination zone pairs, as well as source areas of architecture and destination areas of architecture. After you complete zone mapping, you can import it into the Customer Success tool to create a new Heatmap.

## Zone Mapping Feature Section

Source Area of Architecture	Destination Area of Architecture	Target	Source Zone	Source Zone Type	Destination Zone	Destination Zone Type	Tags
None selected ▾	None selected ▾	None selected ▾	None selected ▾	None selected ▾	None selected ▾	None selected ▾	None selected ▾
<b>Apply Filters</b>	<b>Clear Filters</b>	Includes	Only	Exact Match			

## Example Zone Mapping Report

Source Area of Architecture	Destination Area of Architecture	Target	Source Zone	Source Zone Type	Destination Zone	Destination Zone Type	Tags	Column Filters								
None selected	None selected	None selected	None selected	None selected	None selected	None selected	None selected									
<a href="#">Apply Filters</a> <a href="#">Clear Filters</a> <a href="#">Include</a> <a href="#">Only</a> <a href="#">Exact Match</a>																
Documentation / Help																
Source Area of Architecture	Destination Area of Architecture				WildFire	Threat Prevention (IPS)	URL Filtering									
		Total Rule Count	Allow Rule Count	Deny Rule Count	Wildfire Adoption %	Anti-Spyware Adoption %	OSI Subnet Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL Filtering Adoption %	File Blocking Adoption %	Data Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service Port Adoption %	Login Adoption %
Remote Users / VPNs	Remote Users / VPNs	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0	
Remote Users / VPN	Perimeter Internet	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0	
Perimeter Internet, Remote Users / VPN	Perimeter Internet, Remote Users / VPN	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Perimeter Internet	Perimeter Internet	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Perimeter Internet	3rd party / Vendors, Cloud, Data Center East West, Data Center North South, Guest / BYOD, Internal Core, Out-of-band Management, Perimeter Internet, Remote Office, Remote Users / VPNs	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Out-of-band Management	Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0
Internal Core, Remote Users / VPNs	Perimeter Internet	30	29	1	100.0	100.0	89.7	100.0	100.0	100.0	0.0	0.0	91.3	96.7	91.1	100.0
Internal Core, Remote Users / VPN	Internal Core	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Internal Core, Perimeter Internet, Remote Users / VPN	Out-of-band Management, Perimeter Internet, Remote Users / VPN	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0	100.0
Internal Core	Perimeter Internet	10	14	2	100.0	100.0	74.7	100.0	100.0	100.0	0.0	0.0	20.0	51.4	100.0	100.0
Data Center East West, Internal Core, Remote Users / VPNs	Perimeter Internet	8	8	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	87.5	100.0	100.0
Data Center East West, Internal Core, Remote Users / VPNs	Data Center East West, Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0	100.0
Data Center East West, Internal Core, Out-of-band Management, Remote Users / VPNs	Perimeter Internet	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0	100.0
Data Center East West, Internal Core	Perimeter Internet	1	1	0	100.0	100.0	0.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0
Grand Total:		77	65	12	98.3	98.3	75.4	96.9	96.9	96.3	0.0	51.7	74.0	87.7	100.0	

The figure above shows the output of source architectures and destination architectures in the earlier Heatmap report after zone mapping has been performed. Examples of architectures are Internal, External, Internal Core, Data Center East, and Data Center West.

## Example BPA Report

Best Practice Assessment for NGFW								
Security Rule Checks		Best Practice Check Results						
Rule Enabled	Tags Used	Description Populated	Source/Destination = any/any	Service != any	Not Logging at Start of Session	Log Forwarding	Expired Non-Recurring Schedules	Disable Server Response Inspection
Log Forwarding	Log Non Recurring Schedules	Disable Server Response Inspection	Log at Start of Session					
None selected	None selected	None selected	None selected	None selected	None selected	None selected	None selected	None selected
<a href="#">Apply Filters</a> <a href="#">Clear Filters</a>								
Search: <input type="text"/>								
Rule Name	Rule Enabled	Tags Used	Description Populated	Source/Destination != any/any	Service != any	Not Logging at Start of Session	Log Forwarding	Expired Non-Recurring Schedules
Allow Arlo Client RTSP	true	✓	✗	✓	✓	✓	✓	✓
Allow Arlo Pro	true	✓	✗	✓	✓	✓	✓	✓
Allow Arlo Pro Drop	true	✓	✗	✓	✗	✓	✓	✓
Allow Arlo Pro IP	true	✓	✗	✓	✓	✓	✓	✓
Allow Arlo Pro IP Stun	true	✓	✗	✓	✓	✓	✓	✓
Allow FTP	true	✓	✗	✓	✓	✓	✓	✓
Allow spam email approval	true	✓	✓	✓	✓	✓	✓	✓
Allow_7z	true	✓	✗	✓	✓	✓	✓	✓
Allow_DNS_Internal	true	✓	✓	✓	✓	✓	✓	✓
Allow_GP_Portal	true	✓	✗	✓	✓	✓	✗	✓
Allow_NTP	true	✓	✗	✓	✓	✓	✓	✓
Allow_Outbound	true	✓	✓	✓	✓	✓	✓	✓
Allow_Outbound_AutoFocus	true	✓	✗	✓	✓	✓	✓	✓
Allow_Outbound_YouTube-ban	true	✓	✗	✓	✓	✓	✓	✓
Allow_Outbound_DNS	true	✓	✓	✓	✓	✓	✓	✓
Allow_Outbound_Flash_exception	true	✓	✗	✓	✓	✓	✗	✓
Allow_Outbound_Good_App_Ios	true	✓	✓	✓	✓	✓	✓	✓
Allow_Outbound_Good_App_Ios_web	true	✓	✓	✓	✓	✓	✓	✓
Passing % 91.3% 20.0% 100.0% 67.5% 96.3% 76.3% 100.0% 100.0%								
Showing 1 to 50 of 80 entries <a href="#">Export Data</a>								
Previous <a href="#">1</a> <a href="#">2</a> Next								

## **Example of Best Practices for Security rulebase Checks**

### Security Rulebase Checks

Perform best practice checks against security rulebase for each vsys instance.

Vsys

All ▼ Only show records with warnings

#### Security Rulebase vsys: vsys1

**Best Practice Check Results** ⓘ

- ✓ Regional Deny Rules (Pass)
- ✗ Disabled Rules (Fail): It is recommended to remove disabled rules. (3 disabled rules exist)
- ✗ Interzone Deny Rule with Logging (Fail): It is recommended to have an any/any interzone deny rule with Log at Session End enabled
- ✗ Intrazone Deny Rule with Logging (Fail): It is recommended to have an any/any intrazone deny rule with Log at Session End enabled
- ✓ Malware / Phishing Deny Rule (Pass)
- ✗ HIP Profiles used in Rules (Fail): It is recommended to use HIP Profiles in rulebase
- ✗ User ID Rules without User ID enabled on Zone (Fail): The following zones do not have User ID enabled, but User ID is used on the rule: any (1 rule)

## **Example of Best Practices for Security Best Practice Checks**

### Security Best Practice Checks

X

#### Regional Deny Rules

**Description**  
Ensure there is at least one rule denying traffic from certain regions in security rulebase  
**Rationale**  
Region-based rules help in having control in either allowing or denying traffic from certain region or nation. Regions are prebuilt in the firewall and we can add them in source or destination address fields in the security policy. For instance, if a company has offices in country A, B and C and if the company starts noticing surge in traffic (DoS or flood) from a country X, which they are not expecting, then they can create a region-based policy to deny any traffic coming from the source region X.  
**Reference URL(s)**  
<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Block-Traffic-Based-Upon-Countries/ta-p/52217>

#### Disabled Rules

**Description**  
Ensure no disabled rules exist in security rulebase  
**Rationale**  
Disabled rules are in place only because these security rules were created for temporary reasons, testing reasons, created long time ago which are not in use now or so on and they are currently not necessary to the network. If a security rule is not necessary in the network then it has to be deleted. We should have only the required policies configured.

#### Interzone Deny Rule with Logging

**Description**  
Ensure there is an any/any interzone deny rule with Log at Session End in security rulebase  
**Rationale**  
Firewall has a default security policy at the end of security rulebase for interzone traffic to be denied. This rule is of type interzone. The policy ensures that interzone traffic is not permitted by default and if we have to permit traffic between two different zones then it has to be explicitly configured between those two zones. The default interzone rule does not have 'log at session end' option enabled. Also, we cannot modify this setting for this rule. It is necessary to log traffic that is getting denied if it is interzone to identifies any threat activity. With the default rule, as logging is not enabled, we would not have visibility and hence, this interzone rule has to be configured to log the traffic matching this policy.  
**Reference URL(s)**  
<https://live.paloaltonetworks.com/t5/Management-Articles/What-are-Universal-Intrazone-and-Interzone-Rules/ta-p/57491>

## **1.1.7 References**

VM-Series Plugin and Panorama Plugins:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-plugins/plugins-types>

## **1.1.8 Sample Questions**

1. Which component of the integrated Palo Alto Networks security solution limits network-attached workstation access to a corporate mainframe?
  - a. threat intelligence cloud
  - b. advanced endpoint protection
  - c. next-generation firewall
  - d. tunnel inspection
  
2. Which Palo Alto Networks product is designed primarily to provide threat context with deeper information about attacks?
  - a. Prisma Cloud
  - b. WildFire
  - c. AutoFocus
  - d. Threat Prevention
  
3. Which Palo Alto Networks product is designed primarily to provide normalization of threat intelligence feeds with the potential for automated response?
  - a. MineMeld
  - b. WildFire
  - c. AutoFocus
  - d. Threat Prevention
  
4. Which Palo Alto Networks product is designed primarily to prevent endpoints from successfully running malware programs?
  - a. GlobalProtect
  - b. Cortex XDR – Analytics
  - c. Cortex XDR
  - d. Prisma Cloud
  
5. The Palo Alto Networks Cortex Data Lake can accept logging data from which two products? (Choose two.)
  - a. Cortex XDR
  - b. next-generation firewalls
  - c. Prisma SaaS
  - d. MineMeld
  - e. AutoFocus

6. Which Palo Alto Networks product is a cloud-based storage service designed to hold log information?
- a. Prisma Cloud
  - b. Cortex XDR
  - c. next-generation firewall
  - d. Cortex Data Lake
7. Which product is an example of an application designed to analyze Cortex Data Lake information?
- a. Cortex XDR – Analytics
  - b. Prisma Cloud
  - c. Cortex XDR – Automated Response
  - d. AutoFocus
8. A Heatmap provides an adoption rate for which three features? (Choose three.)
- a. WildFire
  - b. Traps
  - c. File Blocking
  - d. User-ID
  - e. Authentication Profiles
9. What are three Best Practice Assessment tool class summaries? (Choose three.)
- a. Technical
  - b. Operational
  - c. Management
  - d. Risk
  - e. Contingency
10. Which two security features normally do not achieve an adoption rate of 100 percent? (Choose two.)
- a. URL Filtering
  - b. App-ID
  - c. Logging
  - d. DNS Sinkhole
11. Which type of file is used to generate the Heatmap report and the BPA report?
- a. Technical Support
  - b. Configuration
  - c. Statistics
  - d. XML
12. What are two components of the BPA tool? (Choose two.)
- a. Heatmap
  - b. BPA
  - c. XML

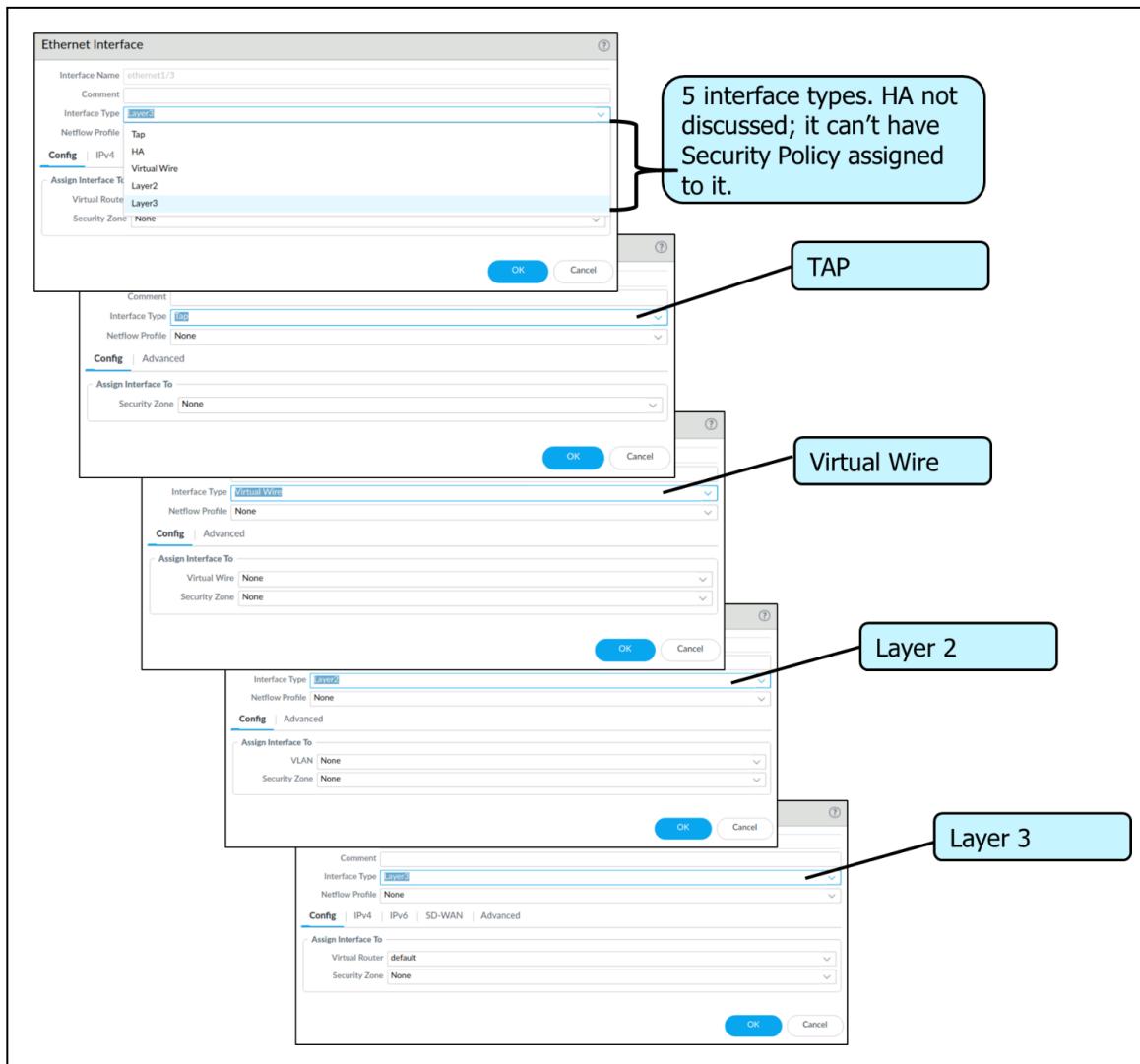
d. Security policy

## 1.2 Determine and assess appropriate interface types for various environments

### *Types of Interfaces*

Palo Alto Networks firewalls support several different interface types: TAP mode, virtual wire mode, Layer 2, Layer 3, and aggregate. A single firewall can freely mix interface types to meet any integration need. The decision about which interface configuration to choose depends on functional need and existing network integration requirements.

The following image shows primary configuration options for interfaces:



### **1.2.1 Layer 2 interfaces**

In a Layer 2 deployment, the firewall provides switching between two or more networks. Devices are connected to a Layer 2 segment; the firewall forwards the frames to the proper port, which is associated with the Media access control (MAC) address that is identified in the frame. Configure a Layer 2 interface when switching is required.

### **1.2.2 Layer 3 interfaces**

In a Layer 3 deployment, the firewall routes traffic between multiple ports using Transmission control protocol/Internet protocol (TCP/IP) addressing. Before you can configure Layer 3 interfaces, you must configure the virtual routers that you want the firewall to use to route the traffic for each Layer 3 interface.

Layer 3 deployments require more network planning and configuration preparation than most other firewall interfaces, but they remain the most widely used in firewall deployments. Palo Alto Networks supports both IPv4 and IPv6 simultaneously through a *dual-stack* implementation when IPv6 is required.

Each Layer 3 interface must be configured with an IPv4 and/or an IPv6 address, zone name assignment, and the attached virtual router that services the traffic on the interface. Options that are available to meet other connectivity requirements include the following:

- NetFlow integration
- Maximum segment size (MSS) adjustment
- Maximum transmission unit (MTU) adjustment
- Binding of firewall services (e.g., ping responses, web management interface availability)
- Neighbor discovery for IPv6
- Manual MAC address assignment
- Link Layer Discovery Protocol (LLDP) enablement
- Dynamic DNS support
- Link negotiation settings

### **1.2.3 Virtual Wire interfaces**

In a virtual wire deployment, you install a firewall transparently on a network segment by binding two firewall ports (interfaces) together. The virtual wire logically connects the two interfaces; hence, the virtual wire is internal to the firewall.

Use a virtual wire deployment only when you want to seamlessly integrate a firewall into a topology and when the two connected interfaces on the firewall do not need to perform any switching or routing. For these two interfaces, the firewall is considered a bump in the wire.

A virtual wire deployment simplifies firewall installation and configuration because you can insert the firewall into an existing topology without assigning MAC or IP addresses to the interfaces, redesigning the network, or reconfiguring surrounding network devices. The virtual wire supports blocking or allowing traffic based on virtual LAN (VLAN) tags. It also supports Security policy rules, App-ID, Content-ID, User-ID, decryption, LLDP, active/passive and active/active high availability (HA), QoS, zone protection (with some exceptions), non-IP protocol protection, denial of service (DoS) protection, packet buffer protection, tunnel content inspection, and NAT.

Each virtual wire interface is directly connected to a Layer 2 or Layer 3 networking device or host. The virtual wire interfaces have no Layer 2 or Layer 3 addresses. When a virtual wire interface receives a frame or packet, it ignores any Layer 2 or Layer 3 addresses for switching or routing purposes; however, it applies your security or NAT policy rules before passing an allowed frame or packet over the virtual wire to the second interface and on to the network device connected to it.

You would not use a virtual wire deployment for interfaces that need to support switching, virtual private network (VPN) tunnels, or routing because they require a Layer 2 or Layer 3 address. A virtual wire interface does not use an Interface Management Profile. This type of profile controls services such as HTTP and ping and therefore requires the interface to have an IP address.

All firewalls that are shipped from the factory have two Ethernet ports (port 1 and port 2) preconfigured as virtual wire interfaces. These interfaces allow all untagged traffic.

#### **1.2.4 Tap interfaces**

A network tap is a device that provides a way to access data that is flowing across a computer network. TAP mode deployment allows you to passively monitor traffic flows across a network using a switch port analyzer (SPAN) or mirror port.

A switch SPAN or mirror port permits the copying of traffic from ports on the switch to the tap interface of the firewall, providing a one-way flow of copied network traffic into the firewall. This configuration allows the firewall to detect traffic and threats but prevents any enforcement action because the traffic does not flow through the firewall back to the environment.

By deploying the firewall in TAP mode, you can get visibility into which applications are running on the network without having to make any changes to your network design. When the firewall is in TAP mode, it also can identify threats on your network. Remember, however, that the traffic is not running through the firewall when the firewall is in TAP mode, so no action can be taken on the traffic, including blocking traffic that includes threats or applying QoS traffic control.

#### **1.2.5 Subinterfaces**

Virtual wire deployments can use virtual wire subinterfaces to separate traffic into zones. Virtual wire subinterfaces provide flexibility in enforcing distinct policies when you need to manage traffic from multiple

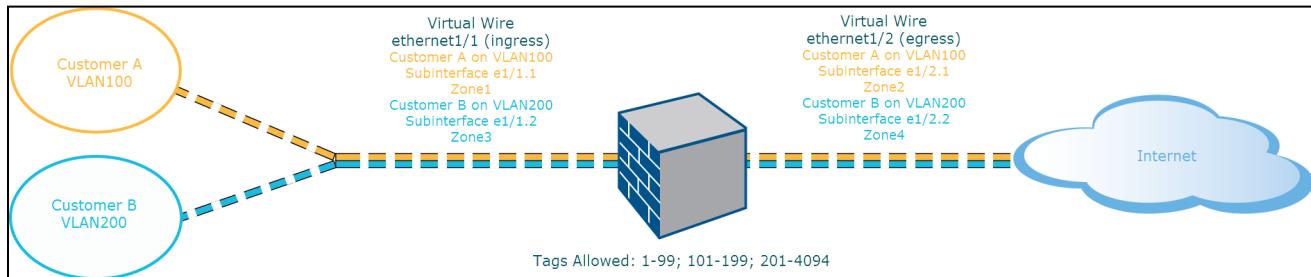
customer networks. The subinterfaces allow you to separate and classify traffic into different zones (the zones can belong to separate virtual systems, if required) using VLAN tags and VLAN tags with IP classifiers.

**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

- Configure two Ethernet interfaces as type virtual wire. Assign these interfaces to a virtual wire.
- Create subinterfaces on the parent virtual wire to separate Customer A and Customer B 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; a virtual wire does not switch VLAN tags.
- 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 subinterface with the VLAN tag “0” and define subinterface(s) with IP classifiers for managing untagged traffic using IP classifiers.



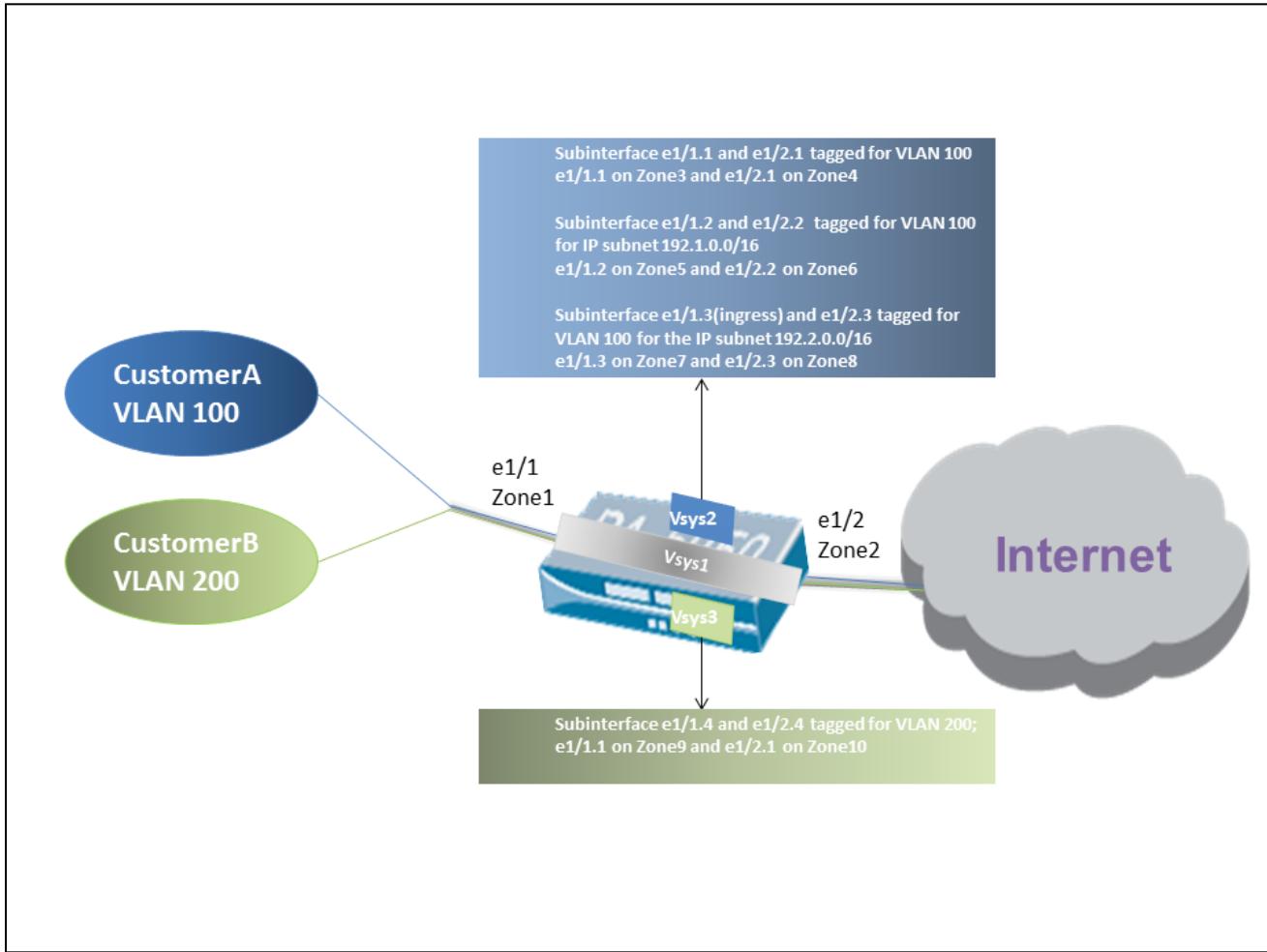
Virtual Wire Deployment with Subinterfaces (VLAN Tags only) depicts Customer A and Customer B connected to the firewall through one physical interface, ethernet1/1, configured as a virtual wire; it is the ingress interface. A second physical interface, ethernet1/2, is also part of the virtual wire; it is the egress interface that provides access to the internet.

For Customer A, you also have subinterfaces ethernet1/1.1 (ingress) and ethernet1/2.1 (egress). For Customer B, you have subinterfaces ethernet1/1.2 (ingress) and ethernet1/2.2 (egress). When configuring the subinterfaces, you must assign the appropriate VLAN tag and zone to apply policies for each customer. In this example, the policies for Customer A are created between Zone1 and Zone2, and policies for Customer B are created between Zone3 and Zone4.

When traffic enters the firewall from Customer A or Customer B, 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.

Virtual Wire Deployment with Subinterfaces (VLAN Tags and IP Classifiers) depicts Customer A and Customer B 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.



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 except VLAN tags 100 and 200, which are assigned to the subinterfaces.

Customer A is managed on vsys2, and Customer B is managed on vsys3. On vsys2 and vsys3, the following virtual wire subinterfaces are created with the appropriate VLAN tags and zones to enforce policy measures.

CUSTOMER	VSYS	VIRTUAL WIRE SUBINTERFACES	ZONE	VLAN TAG	IP CLASSIFIER
A	2	e1/1.1 (ingress) e1/2.1 (egress)	Zone 3 Zone 4	100 100	None
	2	e1/1.2 (ingress) e1/2.2 (egress)	Zone 5 Zone 6	100 100	IP subnet 192.1.0.0/16
	2	e1/1.3 (ingress) e1/2.3 (egress)	Zone 7 Zone 8	100 100	IP subnet 192.2.0.0/16
B	3	e1/1.4 (ingress) e1/2.4 (egress)	Zone 9 Zone 10	200 200	None

When traffic enters the firewall from Customer A or Customer B, the VLAN tag on the incoming packet is first matched against the VLAN tag defined on the ingress subinterfaces. In this case, for Customer A, 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. It then selects the appropriate virtual wire to route traffic through the accurate subinterface.

### 1.2.6 Tunnel interfaces

In a VPN tunnel setup, 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 a proxy ID, the proxy ID is counted toward any Internet protocol security (IPsec) tunnel capacity.

The tunnel interface must belong to a security zone to apply policy, and it must be assigned to a virtual router 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.

The Layer 3 interface that the tunnel interface is attached to typically belongs to an external zone — for example, the untrust zone. Although the tunnel interface can be in the same security zone as the physical interface, you can create a separate zone for the tunnel interface for added security and better visibility. If you create a separate zone for the tunnel interface, such as a VPN zone, you will need to create Security policies to allow traffic to flow between the VPN zone and the trust zone.

A tunnel interface does not require an IP address to route traffic between the sites. An IP address is required only 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 that are configured on it with what is received in the packet to allow a successful Internet key exchange (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 toward the IPsec VPN tunnel capacity of the firewall, and the tunnel capacity varies by the firewall model.

### 1.2.7 Aggregate interfaces

An Aggregate Ethernet (AE) interface group uses IEEE 802.1AX link aggregation to combine multiple Ethernet interfaces into a single virtual interface that connects the firewall to another network device or another firewall. An AE interface group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy: When one interface fails, the remaining interfaces continue to support traffic.

Before you configure an AE interface group, you must configure its interfaces. Hardware media can differ among the interfaces assigned to an aggregate group. For example, you can mix fiber optic and copper. But the bandwidth (e.g., 1Gbps, 10Gbps, 40Gbps, or 100GBps) and interface type (e.g., HA3, virtual wire, Layer 2, or Layer 3) must be the same. You can add at least eight AE interface groups per firewall, although some firewall models support 16, and each group can have up to eight interfaces.

Aggregate interface creation begins with the definition of an Aggregate Interface group, after which individual interfaces are added to the group.

### 1.2.8 Loopback interfaces

Loopback interfaces are Layer 3 interfaces that exist only virtually and connect to virtual routers in the firewall. Loopback interfaces are used for multiple network engineering and implementation purposes. They can be destination configurations for DNS sinkholes, GlobalProtect service interfaces (e.g., portals and gateways), routing identification, and more.

### 1.2.9 Decrypt mirror interfaces

#### *Decryption Mirror*

Decrypt mirror is a special configuration that supports the routing of decrypted traffic copies through an external interface to a data loss prevention (DLP) service. DLP is a product category for products that scan internet-bound traffic for keywords and patterns that identify sensitive information.

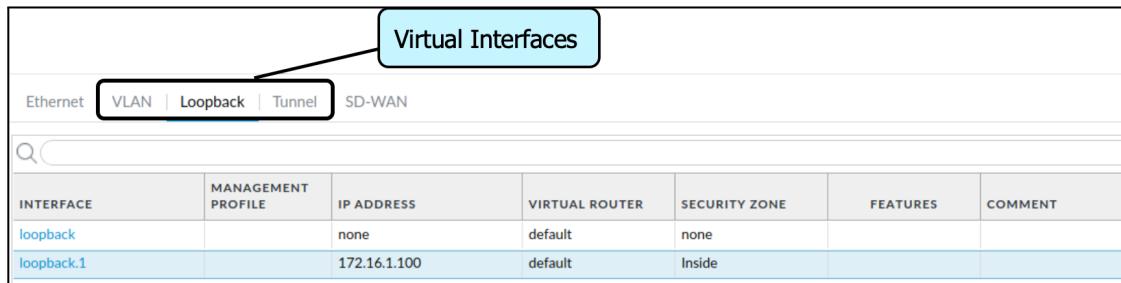
Palo Alto Networks firewalls can automatically send a copy of decrypted traffic to a specified interface using the Decryption Mirroring feature. This option can be licensed at no cost for midrange and high-end firewalls that can automatically forward copies of decrypted traffic to external DLP products.

## ***Special Decryption Implementations***

Palo Alto Networks firewalls also can automatically send a copy of decrypted traffic to a specified interface using the Decryption Mirroring feature. This option is available at no cost to midrange and high-end firewalls that automatically forward copies of decrypted traffic to external DLP products.

## ***Virtual Interfaces***

Palo Alto Networks firewalls also provide several virtual interface types for additional functionality, as shown in the following image.



The screenshot shows a network interface configuration screen. At the top, there are tabs: Ethernet, VLAN (which is selected and highlighted in blue), Loopback, Tunnel, and SD-WAN. Below the tabs is a search bar. The main area displays a table of virtual interfaces:

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
loopback		none	default	none		
loopback.1		172.16.1.100	default	Inside		

VLANs are logical interfaces that specifically serve as interconnects between on-board virtual switches (VLANs) and virtual routers. They allow traffic to move from Layer 2 to Layer 3 within the firewall.

### **1.2.10 VLAN interface**

A VLAN interface can provide routing into a Layer 3 network (IPv4 and IPv6). You can add one or more Layer 2 Ethernet ports (see PA-7000 Series Layer 2 Interface) to a VLAN interface. For details, see [Network > Interfaces > VLAN](#).

### **1.2.11 References**

Virtual Wire Interfaces:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/configure-interfaces/virtual-wire-interfaces>

Configure Layer 3 Interfaces:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/configure-interfaces/layer-3-interfaces/configure-layer-3-interfaces>

Tap Interfaces:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/configure-interfaces/tap-interfaces>

Aggregate Ethernet (AE) Interface Group:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group>

How to Configure a Decrypt Mirror Port:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGDCA0>

Decryption Mirroring:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts/decryption-mirroring>

Network > Interfaces > VLAN:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-interfaces-vlan>

### 1.2.12 Sample Questions

1. Virtual wire does not switch VLAN \_\_\_\_\_.

- a. addresses
- b. subnets
- c. tags
- d. wires

2. 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 \_\_\_\_\_.

- a. service routes
- b. static routes
- c. virtual systems
- d. subinterface

## 1.3 Identify decryption deployment strategies

### 1.3.1 Risks and implications of enabling decryption

#### *Packet Visibility*

The use of encryption for all network applications is growing rapidly. When traffic is encrypted, the Palo Alto Networks firewall loses visibility into packet contents, thus making Content-ID impossible. Because of this lack of visibility, malware might be able to pass unchallenged to an endpoint, at which point it is decrypted and able to attack. Decryption policies maximize the firewall's visibility into packet content to allow for content inspection.

#### *Decryption*

The Secure Sockets Layer (SSL) and Secure Shell (SSH) encryption protocols secure traffic between two entities, such as a web server and a client. SSL encapsulates traffic. It encrypts data so that it is meaningless to anyone other than the client and server with the correct certificates and the keys to decode the data.

#### *Keys and Certificates*

Encryption technology uses keys to transform cleartext strings into ciphertext. These keys are generated using passwords and other shared secrets. Palo Alto Networks firewalls decrypt encrypted traffic by using keys to transform encrypted strings into cleartext. 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 to secure an SSL/TLS connection. Certificates can also be verified when traffic is excluded 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.

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 enable you to specify traffic for decryption according to destination, source, or URL category and 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.

Central to this discussion is the role of digital certificates to secure SSL encrypted data. Your understanding of this role and planning for proper certificate needs and deployment are important considerations in decryption use.

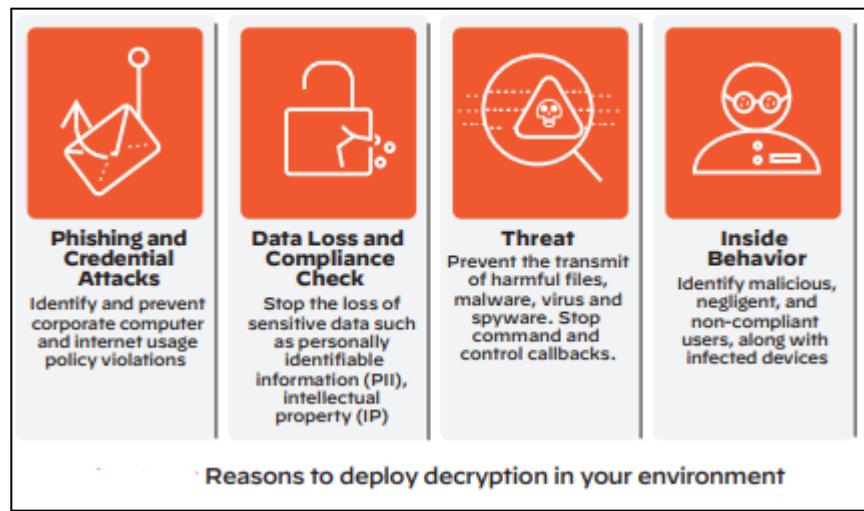
The use of certificates is central to other important firewall functions, in addition to decryption. This need led to the implementation of extensive certificate management capabilities on the firewall.

### ***App-ID and Encryption***

The App-ID scanning engine's effectiveness is often compromised by encrypted traffic that prevents scanning packet contents for identifying elements. This traffic is typically given the App-ID of "SSL." In some cases, the App-ID engine can evaluate elements of the certificate that secure this data for specific identifying components, allowing the App-ID engine to properly assign App-IDs without scanning contents.

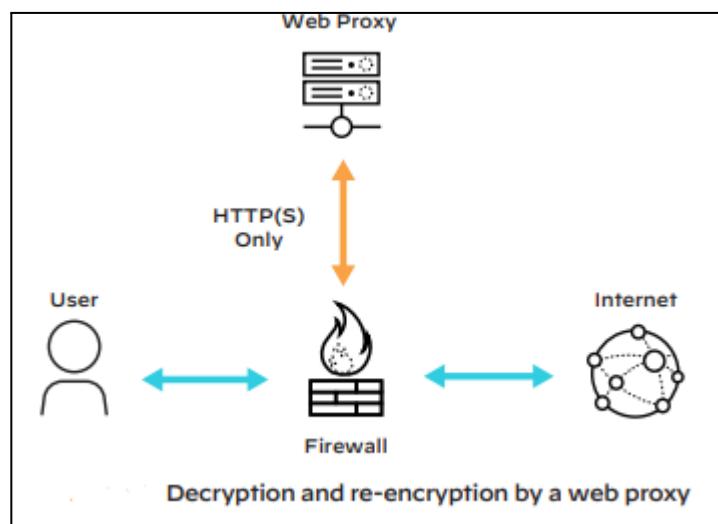
### **1.3.2 Use cases**

Many technical options are available to decrypt traffic on your network, including web proxies, application delivery controllers, SSL visibility and decryption appliances, and NGFWs. Where it's best to decrypt TLS/ SSL traffic depends on which option provides the greatest protection with the least management overhead — in other words, maximum security return on investment.



## Web Proxies

A web proxy acts as a “middleman” by decrypting and inspecting outbound traffic before re-encrypting it and sending it to its destination (see following figure). However, web proxies are limited to inspecting and securing web traffic, which includes HTTP and HTTPS. They are typically deployed on well-known web ports, such as 80 and 443. If an application uses non-web ports or protocols, web proxies can't see the traffic. For example, Office/Microsoft 365 applications work across multiple ports besides 80/443. Regular proxies would miss traffic on these other ports. Moreover, web proxies cannot access non-web traffic, defeating the purpose of gaining complete visibility and control over encrypted traffic on your network. It's like deploying airport security in only one major terminal and leaving the other terminals exposed. Proxies also require you to modify your browser's proxy settings or use a proxy auto-config file, which adds more management overhead and another area to diagnose if users can't access the internet.

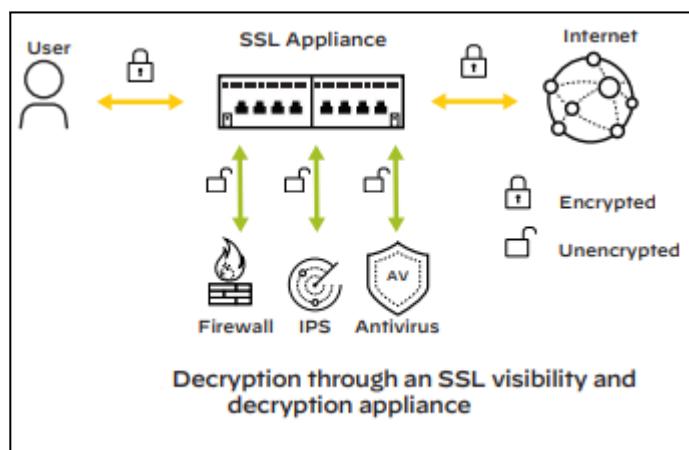


## Application Delivery Controllers

SSL offload is one of the functions performed by Application Delivery Controllers (ADCs). An ADC deployment usually requires two separate appliances: one to decrypt traffic and one to re-encrypt traffic. Given the two-stage operation, the problem with ADC deployments is that, once decrypted, the traffic travels unencrypted between the ADC devices until it hits the encryption device. An adversary can simply sniff the traffic and retrieve sensitive data in cleartext or manipulate the traffic. This undermines one of the fundamental purposes of encryption — the promise of complete confidentiality — and may violate compliance laws in some industries and geographies.

### **SSL Visibility and Decryption Appliances**

SSL visibility appliances decrypt traffic and make it available to all other network security functions that need to inspect it, such as web proxies, DLP systems, and antivirus programs.



### **1.3.3 Decryption Types**

SSL and SSH encryption protocols 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 anyone other than the client and server with the correct certificates and the keys to decode the data. Decrypt SSL and SSH traffic to:

- Prevent malware concealed as encrypted traffic from being introduced into your network. For example, an attacker compromises a website that uses SSL encryption. Employees visit that website and unknowingly download an exploit or malware. The malware then uses the infected employee endpoint to move laterally through the network and compromise other systems.
- Prevent sensitive information from moving outside the network
- Ensure that the appropriate applications are running on a secure network
- Selectively decrypt traffic — for example, create a decryption policy and profile to exclude traffic for financial or healthcare sites from decryption

Palo Alto Networks firewall decryption is policy-based. It can decrypt, inspect, and control inbound and outbound SSL and SSH connections. A decryption policy enables you to specify traffic to decrypt by destination, source, service, or URL category and to block, restrict, or forward the specified traffic according

to the security settings in the associated Decryption Profile. A Decryption Profile controls SSL protocols, certificate verification, and failure checks to prevent traffic that uses weak algorithms or unsupported modes from accessing the network. The firewall uses certificates and keys to decrypt traffic to plaintext and then enforces App-ID and security settings on the plaintext traffic, including Decryption, Antivirus, Vulnerability, Anti-Spyware, URL Filtering, WildFire, and File-Blocking Profiles. After decrypting and inspecting traffic, the firewall re-encrypts the plaintext traffic as it exits the firewall to ensure privacy and security.

The firewall provides three types of decryption policy rules: SSL Forward Proxy to control outbound SSL traffic, SSL Inbound Inspection to control inbound SSL traffic, and SSH Proxy to control tunneled SSH traffic. You can attach a Decryption Profile to a policy rule to apply granular access settings to traffic, such as checks for server certificates, unsupported modes, and failures.

SSL decryption (both forward proxy and inbound inspection) requires certificates to establish the firewall as a trusted third party and to establish trust between a client and a server to secure an SSL/TLS connection. You can also use certificates when excluding servers from SSL decryption for technical reasons (the site breaks decryption for reasons such as certificate pinning, unsupported ciphers, or mutual authentication). SSH decryption does not require certificates.

### 1.3.4 Decryption Profiles and certificates

A Decryption Profile controls SSL protocols, certificate verification, and failure checks to prevent traffic that uses weak algorithms or unsupported modes from accessing the network. The firewall uses certificates and keys to decrypt traffic to plaintext and then enforces App-ID and security settings on the plaintext traffic, including Decryption, Antivirus, Vulnerability, Anti-Spyware, URL Filtering, WildFire, and File Blocking Profiles. After decrypting and inspecting traffic, the firewall re-encrypts the plaintext traffic as it exits the firewall to ensure privacy and security.

#### *Keys and certificates*

Keys are strings of numbers typically generated using a mathematical operation involving random numbers and large primes. Keys transform strings — such as passwords and shared secrets — from unencrypted plaintext to encrypted ciphertext and from encrypted ciphertext to unencrypted plaintext. 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 establish trust between a client and a server 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. These fields include the fully qualified domain name ( 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. A certificate authority (CA) must issue all certificates. After the CA verifies a client or server, the CA issues the certificate and signs it with a private key.

When you apply a decryption policy to traffic, a session between the client and the server is established only if the firewall trusts the CA that signed the server certificate. 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.

The following table describes the certificates Palo Alto Networks firewalls use for decryption.

CERTIFICATES USED WITH DECRYPTION	DESCRIPTION
Forward Trust (used for SSL Forward Proxy decryption)	<p>The certificate the firewall presents to clients during decryption if the site the client is attempting to connect to has a certificate signed by a CA that the firewall trusts. To configure a forward trust certificate on the firewall to present to clients when the server certificate is signed by a trusted CA, see <a href="#">configure SSL forward proxy</a>.</p> <p>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 <a href="#">configure the key size for SSL proxy server certificates</a>. For added security, consider storing the private key associated with the forward trust certificate on a hardware security module (see <a href="#">store private keys on an HSM</a>).</p>
Forward Untrust (used for SSL Forward Proxy decryption)	<p>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="#">configure SSL forward proxy</a>.</p>
SSL Inbound Inspection	<p>The certificates of the servers on your network for which you want to perform SSL Inbound Inspection of traffic destined for those servers. Import the server certificates onto the firewall.</p>

### 1.3.5 Create decryption policy in the firewall

You can configure the firewall to decrypt traffic for visibility, control, and granular security. Decryption policies can apply to SSL, including SSL encapsulated protocols such as Internet Message Access Protocol, Post Office Protocol Version 3, Simple Mail Transfer Protocol, File Transfer Protocol Secure, Secure Shell [IMAP(S), POP3(S), SMTP(S), and FTP(S) and SSH] traffic. SSH decryption can be used to decrypt outbound and inbound

SSH traffic to assure that secure protocols are not being used to tunnel disallowed applications and content. Add a decryption policy rule to define traffic that you want to decrypt (for example, you can decrypt traffic based on URL categorization). Decryption policy rules are compared against the traffic in sequence, so more specific rules must precede the more general ones. SSL forward proxy decryption requires the configuration of a trusted certificate that is presented to the user if the server to which the user is connecting possesses a certificate signed by a CA trusted by the firewall. Create a certificate on the **Device Certificate Management Certificates** page, then click the name of the certificate and select **Forward Trust Certificate**.

Create a decryption policy rule to define traffic for the firewall to decrypt and the type of decryption you want the firewall to perform: SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy decryption. You can also use a decryption policy rule to define Decryption Mirroring.

**Step 1:** Add a new decryption policy rule. Select **Policies > Decryption**, add a new decryption policy rule, and give the policy rule a descriptive **Name**.

**Step 2:** Configure the decryption rule to match to traffic based on network and policy objects:

- **Firewall security zones:** Select **Source** or **Destination**. Match it to traffic based on the source zone or the destination zone.
- **IP addresses, address objects, and address groups:** Select **Source** or **Destination** to match to traffic based on the source address or the destination address. Alternatively, select **Negate** to exclude the source address list from decryption.
- **Users:** Select **Source** and set the **Source User** for whom to decrypt traffic. You can decrypt specific user or group traffic, or decrypt traffic for certain types of users, such as unknown users or pre-logon users (users that are connected to GlobalProtect but are not yet logged in).
- **Ports and protocols:** Select **Service/URL Category** to set the rule to match to traffic based on service. By default, the policy rule is set to decrypt **Any traffic on TCP and UDP ports**. You can add a service or a service group and optionally set the rule to **application-default** to match to applications only on the application default ports.
- **URLs and URL categories:** Select **Service/URL Category** and decrypt traffic based on:
  - An externally hosted list of URLs that the firewall retrieves for policy enforcement (see **Objects > External Dynamic Lists**).
  - Palo Alto Networks predefined URL categories, which make it easy to decrypt entire categories of allowed traffic. This option is also useful when you create policy-based decryption exclusions because you can exclude sensitive sites by category instead of individually. For example, although you can create a custom URL category to group sites that you do not want to decrypt, you can also exclude financial or healthcare-related sites from decryption based on the predefined Palo Alto Networks URL categories. You also can block risky URL categories and create comfort pages to communicate the reason the sites are blocked or enable users to opt out of SSL decryption.

You can use the predefined high-risk and medium-risk URL categories to create a decryption policy rule that decrypts all high-risk and medium-risk URL traffic. Place the rule at the bottom of the rulebase (all decryption exceptions must be above this rule so that you don't decrypt sensitive information) as a safety net to ensure that you decrypt and inspect all risky traffic. However, if high-risk or medium-risk sites to which you allow access contain personally identifiable information or other sensitive information that you don't want to decrypt, either block those sites to avoid allowing encrypted risky traffic while also avoiding privacy issues or create a no decryption rule to handle the sensitive traffic.

- Custom URL categories (see **Objects > Custom Objects > URL Category**). For example, you can create a custom URL category to specify a group of sites you need to access for business purposes but that don't support the safest protocols and algorithms. Then, you can apply a customized Decryption Profile to allow the looser protocols and algorithms for just those sites.

**Step 3:** Set the rule to either decrypt matching traffic or to exclude matching traffic from decryption.

Select **Options**, and set the policy rule **Action**:

To decrypt matching traffic:

1. Set the **Action to Decrypt**.
2. Set the **Type** of decryption for the firewall to perform on matching traffic:
  - **SSL Forward Proxy**
  - **SSL Inbound Inspection** (then, add one or more certificates for the destination internal server of inbound SSL traffic)
  - **SSH Proxy**

To exclude matching traffic from decryption: Set the **Action to No Decrypt**.

**Step 4:** (Optional) Select a Decryption Profile to perform additional checks on traffic that matches the policy rule.

For example, attach a Decryption Profile to a policy rule to ensure that server certificates are valid and to block sessions using unsupported protocols or ciphers. To create a Decryption Profile, select **Objects > Decryption Profile**.

1. Create a decryption policy rule, or open an existing rule to modify it.
2. Select **Options**, and select a Decryption Profile to block and control various aspects of the traffic matched to the rule. The profile rule settings that the firewall applies to matching traffic depends on the policy rule action (decrypt or no Decrypt) and the policy rule type (SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy). This allows you to use the different Decryption Profiles with different types of decryption policy rules that apply to different types of traffic and users.

**Step 5:** Configure decryption logging (configure whether to log both successful and unsuccessful TLS handshakes and configure Decryption log forwarding).

**Step 6:** Click **OK** to save the policy.

**Step 7:** Choose your next step to fully enable the firewall to decrypt traffic:

- Configure [SSL Forward Proxy](#)
- Configure [SSL Inbound Inspection](#)
- Configure [SSH Proxy](#)
- Create policy-based [Decryption Exclusions](#) for traffic you choose not to decrypt, and then add sites that break decryption for technical reasons (e.g., pinned certificates or mutual authentication to the [\*\*SSL Decryption Exclusion\*\*](#) list.

### 1.3.6 Configure SSH proxy

Configuring SSH proxy does not require certificates. The key used to decrypt SSH sessions is generated automatically on the firewall during bootup. With SSH decryption enabled, the firewall decrypts SSH traffic and blocks or restricts SSH traffic based on your decryption policy and Decryption Profile settings. Traffic is re-encrypted as it exits the firewall.

**Step 1:** 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.

View configured interfaces on the **Network > Interfaces > Ethernet** tab. The **Interface Type** column displays if an interface is configured to be a virtual wire, Layer 2, or Layer 3 interface. You can select an interface to modify its configuration, including what type of interface it is.

**Step 2:** Create a decryption policy rule to define traffic for the firewall to decrypt, and then create a Decryption Profile to apply checks to the SSH traffic.

- Select **Policies > Decryption**, **Add** or modify an existing rule, and define traffic to be decrypted.
- Select **Options**, and:
  - Set the rule **Action to Decrypt matching traffic**.
  - Set the rule **Type to SSH Proxy**.
  - (Optional, but a best practice) Configure or select an existing Decryption Profile to block and control various aspects of the decrypted traffic. (For example, create a Decryption Profile to terminate sessions with unsupported versions and unsupported algorithms.)
- Click **OK** to save.

**Step 3:** Commit the configuration.

**Step 4:** (Optional) Continue to **Decryption Exclusions** to disable decryption for certain types of traffic.

### 1.3.7 References

Keys and Certificates for Decryption Policies:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies>

Keys and Certificates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/keys-and-certificate-s>

How Palo Alto Networks Identifies HTTPS Applications Without Decryption:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVSCAQ>

Decryption Exclusions:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions>

Decryption Overview:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-overview>

Decryption: Why, Where, and How:

[https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\\_US/resources/whitepapers/decryption-why-where-and-how](https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/decryption-why-where-and-how)

### 1.3.8 Sample Questions

1. With SSH proxy, PAN-OS firewalls can be configured to detect \_\_\_\_\_. Select all that apply.

- a. SSH traffic
- b. SSH port forwarding
- c. hidden applications inside a SSH tunnel
- d. breached security policies

2. A decryption policy rule allows administrators to:

- a. require certificates
- b. inspect inside encrypted sessions
- c. re-encrypt firewall settings
- d. decrypt VPN traffic

3. Select a use case for a Decryption Profile to block and control various aspects of the decrypted traffic.

- a. terminate idle encrypted user sessions after 300 seconds
- b. search for administrative users after business hours
- c. retrieve a list of user groups from Microsoft Active Directory using TLS
- d. terminate sessions using unsupported versions and unsupported algorithms

## 1.4 Enforce User-ID

### 1.4.1 Methods of building user-to-IP mappings

#### *User-ID and Mapping Users*

The User-ID feature of the Palo Alto Networks NGFW enables you to create policy rules and perform reporting based on users and groups rather than on individual IP addresses.

User-ID seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory and terminal services offerings, thus enabling you to associate application activity and policy rules to users and groups, not just IP addresses. Furthermore, with User-ID enabled, the ACC, App Scope, reports, and logs all include usernames in addition to user IP addresses.

For user-based 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. No other types of directory services are supported for group mapping.

Before the firewall can enforce user-based and group-based policies, it must be able to map the IP addresses based in the packets it receives to usernames. User-ID provides many mechanisms to collect this user-based mapping information.

A User-ID agent process runs either on the firewall (agentless implementation) or is installed as a separate process on a Microsoft Windows-based host. This User-ID agent monitors various network technologies for authentication events and gathers the data, creating a master IP-address-to-user mapping table stored in the firewall. 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 did not map, you can configure the firewall to redirect HTTP requests to a Captive Portal login. You can customize the user mapping mechanisms to suit your environment and even use different mechanisms at different sites.

#### *Mapping IP Addresses to Usernames*

Today's working environment is extremely dynamic. Users no longer are restricted to using just one device: a computer on the network. A user may be using a smartphone, tablet, desktop, and a laptop. Each device is given an IP address dynamically by a Dynamic Host Configuration Protocol (DHCP) server, which makes tracking the user difficult and almost impossible to control. Using a username is easier than using an IP address to control and log a user's activity. The process of mapping a username to an IP address is the function of User-ID.

A user's IP address constantly changes because users use so many devices and laptops provide so much mobility. Capturing that information often is difficult. The firewall needs to be able to monitor multiple sources simultaneously.

For instance, a user's cellphone usually is not in the corporate domain and does not require the user to log in to the domain. However, users often will have their corporate email on their phones. When the phone checks

for new email and authenticates with the Exchange server, the system can capture the IP address from the logs.

The user could be using an iPad or Linux workstation that also is not on the domain. The firewall has a service called Captive Portal that can be used to force the user to authenticate to use the internet. The firewall then has the user's name and IP address.

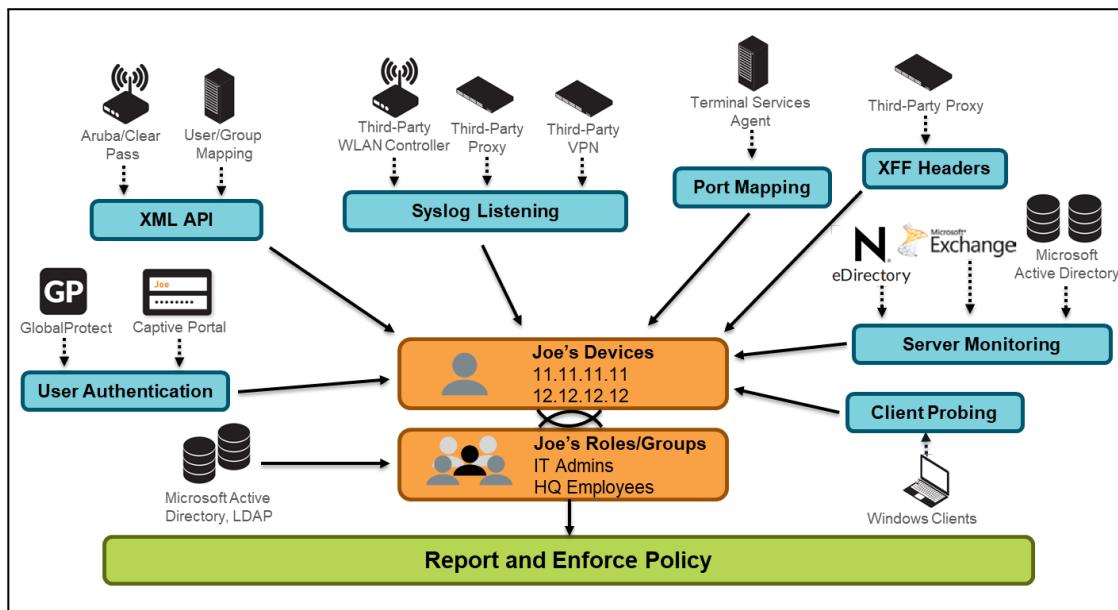
The firewall also has other ways to capture user information. The firewall can use server monitoring to monitor the Security logs on a Windows server for successful authentication events. Syslog monitoring of login events can be used with LDAP and Linux, among others.

The different methods of user mapping include:

- **Server monitoring:** A Windows-based User-ID agent, or the built-in PAN-OS integrated User-ID agent inside the PAN-OS firewall, monitors Security Event logs for successful login and logout events on Microsoft domain controllers, Exchange servers, or Novell eDirectory servers.
- **Port mapping:** For Microsoft Terminal Services or Citrix environments, users might share the same IP address. To overcome this issue, the Palo Alto Networks Terminal Services agent must be installed on the Windows or Citrix terminal server. The Terminal Services agent uses the source port of each client connection to map each user to a session. Linux terminal servers do not support the Terminal Services agent and must use XML API to send user mapping information from login or logout events to User-ID.
- **Syslog:** The Windows-based User-ID agent and the PAN-OS integrated User-ID agent use Syslog Parse Profiles to interpret login and logout event messages that are sent to syslog servers from devices that authenticate users. Such devices include wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, and other network access control devices.
- **XFF headers:** If a proxy server exists between users and a firewall, the firewall might see the source IP address of the proxy server instead of the original source IP address of the host that originated the traffic. Most proxy servers have a feature that allows forwarding of the original source IP address of the host to the firewall within an XFF header. Use of the original client source IP address enables the firewall to map the IP address to a username.
- **Authentication policy and Captive Portal:** The User-ID agent sometimes cannot map an IP address to a username using any of the methods described. In these cases, you can use an Authentication policy and Captive Portal, whereby any web traffic (HTTP or HTTPS) that matches an Authentication policy rule forces the user to authenticate via one of the following three Captive Portal authentication methods:
  - **Browser challenge:** Uses Kerberos or NT LAN Manager (NTLM)
  - **Web form:** Uses multi-factor authentication (MFA), security assertion markup language (SAML) single sign-on (SSO), Kerberos, terminal access controller access control system plus (TACACS+), remote authentication dial-in user service (RADIUS), LDAP, or local authentications
  - Client CA

- **GlobalProtect:** Mobile users have an application running on their endpoint for which they must enter login credentials for VPN access to the firewall. The login information is used for User-ID mapping. GlobalProtect is the most recommended method to map device IP addresses to usernames.
- **XML API:** The PAN-OS XML API is used in cases where standard user mapping methods might not work, such as third-party VPNs or 802.1x-enabled wireless networks.
- **Client probing:** Client probing is used in a Microsoft Windows environment where the User-ID agent probes client systems using Windows Management Instrumentation or NetBIOS. Client probing is not a recommended method for user mapping.

In complex environments, multiple User-ID agents can be deployed to work collaboratively on a master User-ID IP address-to-username mapping table. The following figure shows the main functionality of the User-ID agent.



PAN-OS software can use multiple information sources to map usernames to the IP address of a session.

For more information about the methods used to collect User-ID information, see the following information:

- The “Block Threats by Identifying Users” module in the EDU-210 training Firewall Essentials: Configuration and Management
- The User-ID section in the PAN-OS Administrator’s Guide

#### 1.4.2 Determine if User-ID agent or agentless should be used

##### *Use agentless (PAN-OS)*

- If you have a small to medium deployment with 10 or fewer domain controllers or Exchange servers

- If you wish to share PAN-OS-sourced mappings from Microsoft Active Directory (AD), Captive Portal, or GlobalProtect with other PA devices (maximum 255 devices)

### ***Use User-ID Agent (Windows)***

- If you have medium to large deployment with more than 10 domain controllers
- If you have a multi-domain setup with a large number of servers to monitor

### **1.4.3 Compare and contrast User-ID agents**

#### ***Identifying the User-ID Agent to Deploy***

User-ID has two agents that can be used to monitor servers and gather User-ID information: a built-in agent inside the PAN-OS firewall and a Windows-based client. The built-in agent is called the integrated agent. The Windows-based client can be installed on Windows Server 2008 or later systems. Both agents have the same functionality. Several factors can determine which agent to use.

An organization might choose to use the Windows agent if it has more than 100 domain controllers, because neither type of agent can monitor more than 100 domain controllers or 50 syslog servers. Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

However, if network bandwidth is an issue, you might want to use the PAN-OS integrated agent. It communicates directly with the servers, but the Windows agent communicates with the servers and then communicates User-ID information to the firewall so that it can update the firewall database.

For more information about the different agents and how they are used, see the following information:

- The “Block Threats by Identifying Users” module in the EDU-210 training “Firewall Essentials: Configuration and Management”
- The User-ID section in the PAN-OS Administrator’s Guide

### **1.4.4 Methods of User-ID redistribution**

#### ***Methods of User-ID Redistribution***

Every firewall that enforces user-based policy requires user mapping information. In a large-scale network, instead of configuring all your firewalls to directly query the mapping information sources, you can streamline resource usage by configuring some firewalls to collect mapping information through redistribution.

Redistribution also enables the firewalls to enforce user-based policies when users rely on local sources for authentication (such as regional directory services) but need access to remote services and applications (such as global data center applications). The Data Redistribution feature allows a firewall to be a source of IP user mappings, among other types of data, for any device that is configured to communicate with the agent service of that source firewall or via Panorama.

If you configure an Authentication policy, your firewalls also must redistribute the authentication timestamps that are generated when users authenticate to access applications and services. Firewalls use the timestamps to evaluate the timeouts for Authentication policy rules. The timeouts allow a user who successfully authenticates to later request services and applications without authenticating again within the timeout periods. Redistribution of timestamps enables you to enforce consistent timeouts across all the firewalls in your network.

Firewalls share user mappings and authentication timestamps as part of the same redistribution flow; you do not have to configure redistribution for each information type separately.

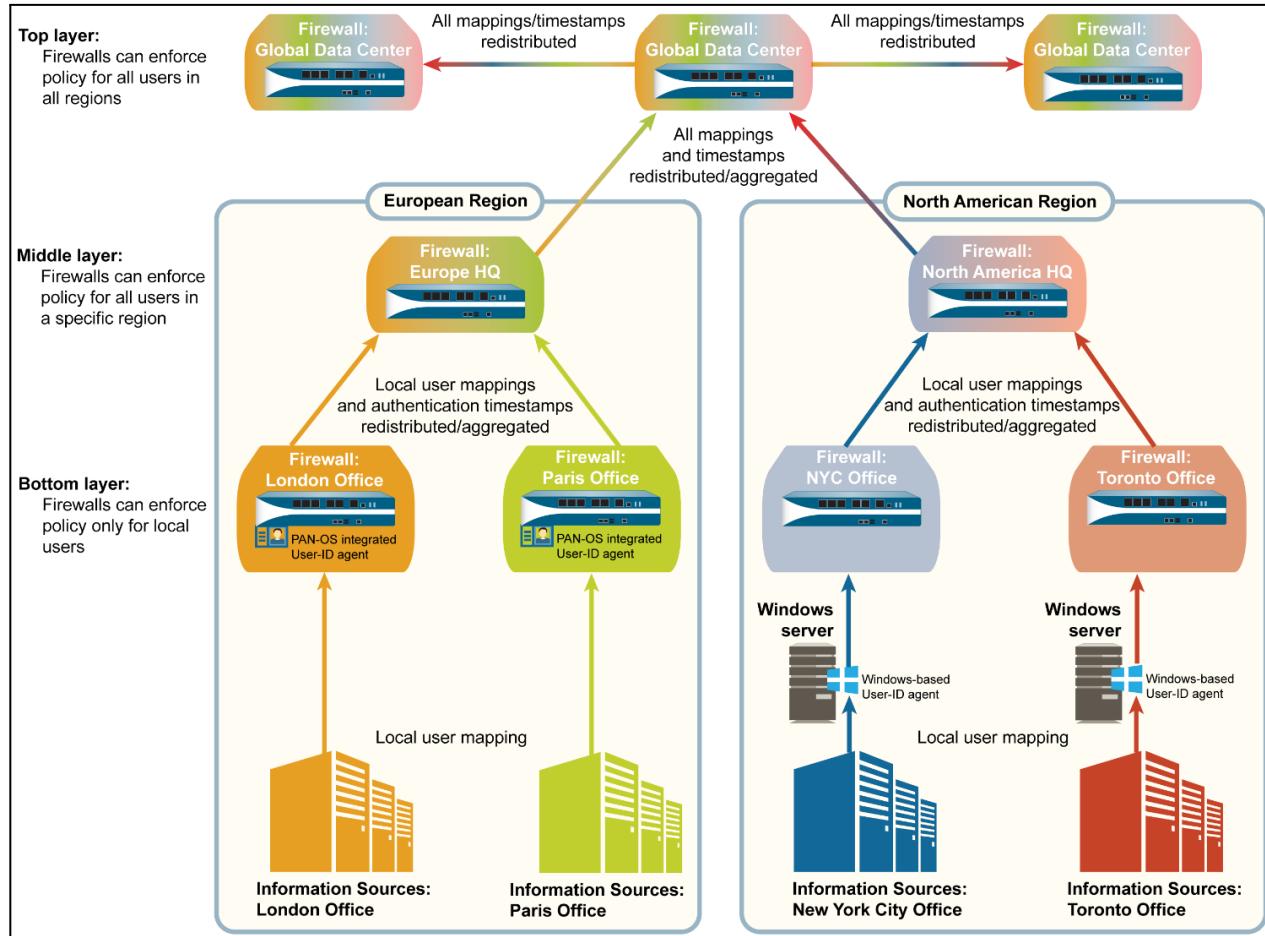
### ***User-ID Table Sharing***

You can enable a firewall or virtual system to serve as a data distribution agent that redistributes user mapping information along with the timestamps associated with authentication challenges. Simply configure Data Redistribution settings to create an agent that will communicate with any firewalls or other devices to share local information.

### ***User-ID Table Consumption***

To map IP addresses to usernames, User-ID agents monitor sources such as directory servers. The agents send the user mappings to firewalls, Log Collectors, or Panorama. Each appliance then can serve as redistribution points that forward the mappings to other firewalls, Log Collectors, or Panorama. Before a firewall or Panorama can collect user mappings, you must configure its connections to the User-ID agents or redistribution points.

## Use Case Example



### 1.4.5 Methods for group mapping

The following are best practices for group mapping in an AD environment:

- If you have a single domain, you need only one group mapping configuration with an LDAP server profile that connects the firewall to the domain controller with the best connectivity. You can add up to four domain controllers to the LDAP server profile for redundancy. Note that you cannot increase redundancy beyond four domain controllers for a single domain by adding multiple group mapping configurations for that domain.
- If you have multiple domains or multiple forests, you must create a group mapping configuration with an LDAP server profile that connects the firewall to a domain server in each domain or forest. Take steps to ensure that you have unique usernames in separate forests.
  - If you have universal groups, create an LDAP server profile to connect to the root domain of the global catalog server on port 3268 or 3269 for SSL. Then, create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that user and group information is available for all domains and subdomains.

- Before using group mapping, configure a primary username for user-based security policies, since this attribute will identify users in the policy configuration, logs, and reports.

## 1.4.6 Server Profile and Authentication Profile

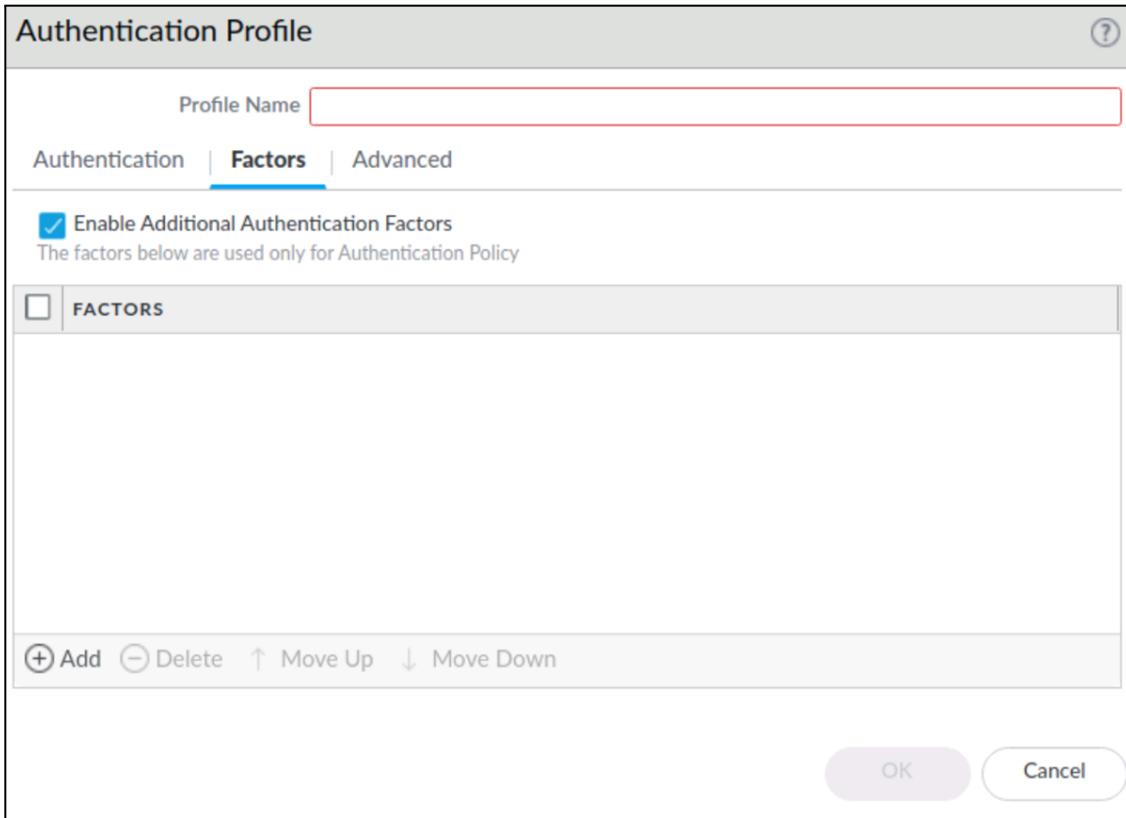
### *Multi Factor Authentication Server Profile*

Defines the access method, location, and authentication for integrated MFA vendors. The **MFA Vendor** drop-down list shows supported vendors. A Certificate Profile is required to support the certificate used to validate the certificate used by the MFA solution to secure its communication with the firewall.

The screenshot shows the 'Multi Factor Authentication Server Profile' dialog box. At the top, there are fields for 'Profile Name' and 'Certificate Profile'. Below that, under 'Server Settings', there is a dropdown for 'MFA Vendor' which is currently set to 'Duo v2'. Other options in the dropdown include 'Okta Adaptive', 'PingID', and 'RSA SecurID Access'. There are also fields for 'NAME', 'API Host', 'Integration Key' (which is highlighted in blue), 'Secret Key', 'Timeout (sec)' (set to 30 [5 - 600]), and 'Base URI' (/auth/v2). At the bottom right, there are 'OK' and 'Cancel' buttons.

### *Authentication Profile*

An Authentication Profile specifies the authentication type and Server Profile for the first Captive Portal-driven authentication. The **Factors** tab incorporates the integrated MFA vendor defined in the Multi Factor Authentication Server Profile. Multiple factors can be added that require the user to pass each challenge from the top down.



#### 1.4.7 References

Map Users to Groups:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-users-to-groups>

Device > User Identification > Group Mapping Settings

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/user-identification/device-user-identification-group-mapping-settings>

Group Mapping:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id-concepts/group-mapping>

User-ID:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id>

Architecting User Identification (User-ID) Deployments Strategies and Tactics Guide PAN-OS 5.0+:

[https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000D8S7AAK&field=Attachment\\_1\\_Body\\_s](https://knowledgebase.paloaltonetworks.com/servlet/fileField?entityId=ka10g000000D8S7AAK&field=Attachment_1_Body_s)

Best Practices for Securing User-ID Deployments:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVPCA0>

Redistribute Data and Authentication Timestamps:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps>

Data Redistribution Using Panorama:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/user-id-redistribution-using-panorama>

Redistribution:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/user-id-agent-setup/user-id-agent-setup-redistribution>

Device > Data Redistribution:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-data-redistribution>

#### 1.4.8 Sample Questions

1. PAN-OS firewalls support the following directory services. Select all that apply.

- a. Microsoft Active Directory
- b. Novell eDirectory
- c. Sun ONE Directory Server
- d. Apache Directory

2. When you enable a user-based or group-based policy, what network security issues could occur if an administrator enables User-ID on an external untrusted zone?

- a. You could disclose internal IP address spacing.
- b. Traffic will be treated as intrazone traffic and by default will be allowed.
- c. Virus/Phishing attacks.
- d. You could allow an attacker to gain unauthorized access to protected services and applications.

3. User-ID maps users to which type of information?

- a. MAC addresses
- b. IP addresses
- c. IP address and port number
- d. port numbers

4. User-ID uses which protocol to map between user identities and groups?

- a. NetBIOS
- b. LDAP
- c. syslog
- d. HTTPS

5. Which format do you use when calling the API to inform the firewall of a new IP address-to-username mapping?
  - a. XML
  - b. JSON
  - c. YAML
  - d. Base64
6. Which configuration must be made on the firewall before it can read user-ID-to-IP-address mapping tables from external sources?
  - a. Group Mapping Settings
  - b. server monitoring
  - c. Captive Portal
  - d. User-ID agents
7. For an external device to consume a local user-ID-to-IP-address mapping table, which data is used for authentication between the devices?
  - a. the source device's data redistribution collector name and preshared key
  - b. the User-ID agent's server monitor account information
  - c. the administrator's account information on the source device with the User-ID role set
  - d. certificates added to the User-ID agent configuration
8. User-ID-to IP-address mapping tables can be read by which product or service?
  - a. Cortex XDR
  - b. Panorama Log Collector
  - c. AutoFocus
  - d. Prisma Cloud

## 1.5 Determine when to use the Authentication policy and methods for doing so

### 1.5.1 Purpose of, and use case for, the Authentication policy

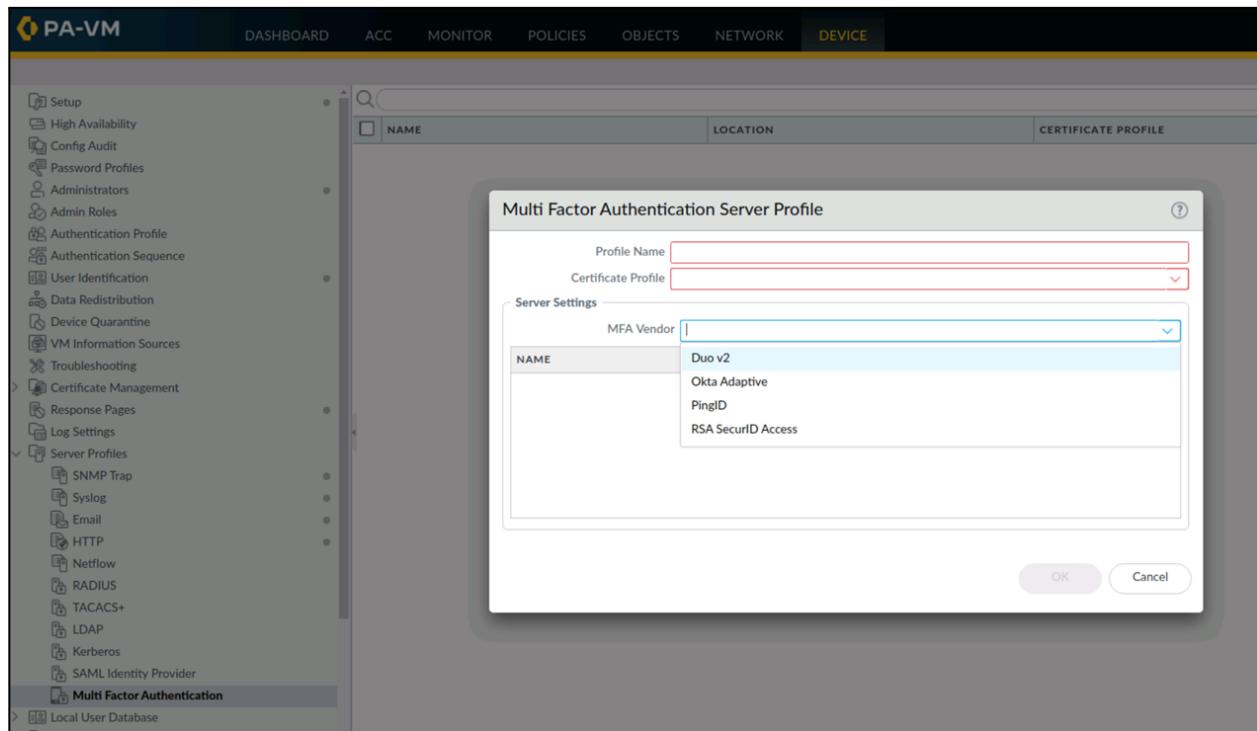
#### *MFA and Authentication Policy*

You can configure MFA to ensure that each user authenticates using multiple methods (factors) when they access highly sensitive services and applications. For example, you can force users to enter a login password and then a verification code that they receive by phone before allowing access to important financial documents. This approach helps to prevent attackers from accessing every service and application in your network just by stealing passwords.

For end-user authentication via Authentication policy, the firewall directly integrates with several MFA platforms (e.g., Duo v2, Okta Adaptive, PingID, and RSA SecurID) and integrates through RADIUS with other MFA platforms.

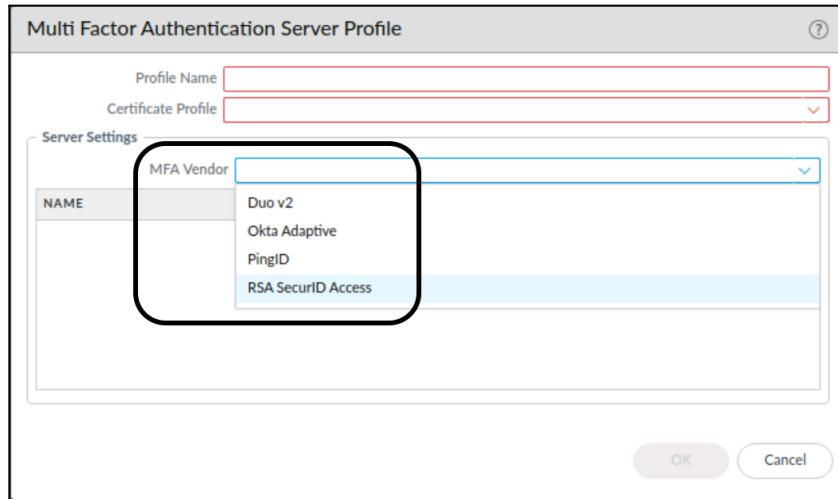
MFA is driven by an Authentication policy that allows precise application of appropriate authentication. These policy rules can invoke simple Captive Portal challenge pages for one-time authentication or can include one (or more) integrated MFA vendor Server Profiles that are included in Authentication Profiles for additional challenges.

After a user successfully completes all challenges, an appropriate Security policy rule will be evaluated that allows access to that protected service.



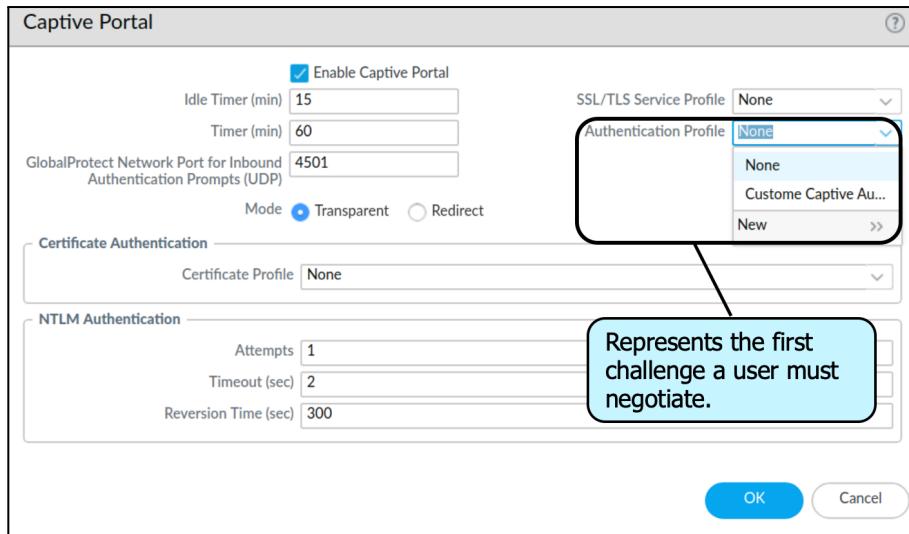
### ***Special Note About MFA***

Palo Alto Networks firewalls support MFA. A Multi Factor Authentication Server Profile is used to natively integrate a firewall with an external third-party MFA solution. MFA factors that the firewall supports include push, Short Message Service (SMS), voice, and one-time password (OTP) authentication. This profile identifies the specific product with its configuration information.



The Multi Factor Authentication Server Profile shown can be a part of multiple authentication challenges that a user must respond to. For example, you can force users to enter a login password and then enter a verification code that they receive by phone before they can access critical financial documents.

The firewall challenges a user with a Captive Portal. Captive Portal configuration includes an Authentication Profile selected for base configuration that represents the first challenge a user must negotiate.



An Authentication Enforcement policy then is used to join the MFA product as a second required authentication. Selection of the MFA product's Authentication Profile adds it as a second authentication requirement for users.

**Authentication Enforcement**

Profile Name:

Authentication Method: **web-form**

Authentication Profile: **None**

Message: This is a customizable authentication message shown to the user to allow customers to provide authentication instructions based on the authentication rule in effect.

OK Cancel

## 1.5.2 Dependencies

### *Dependencies for Implementing MFA*

Before you can use MFA to protect sensitive services and applications, you must configure several settings in the Palo Alto Networks firewall. MFA authentication is triggered when a user requests access to a service that appears in traffic that the firewall processes. The traffic first is evaluated by an Authentication policy rule. When a match is found, the authentication action of the rule is taken.

**Authentication Policy Rule**

General | Source | Destination | Service/URL Category | **Actions**

Authentication Enforcement: **web-form**

Timeout (min): 60

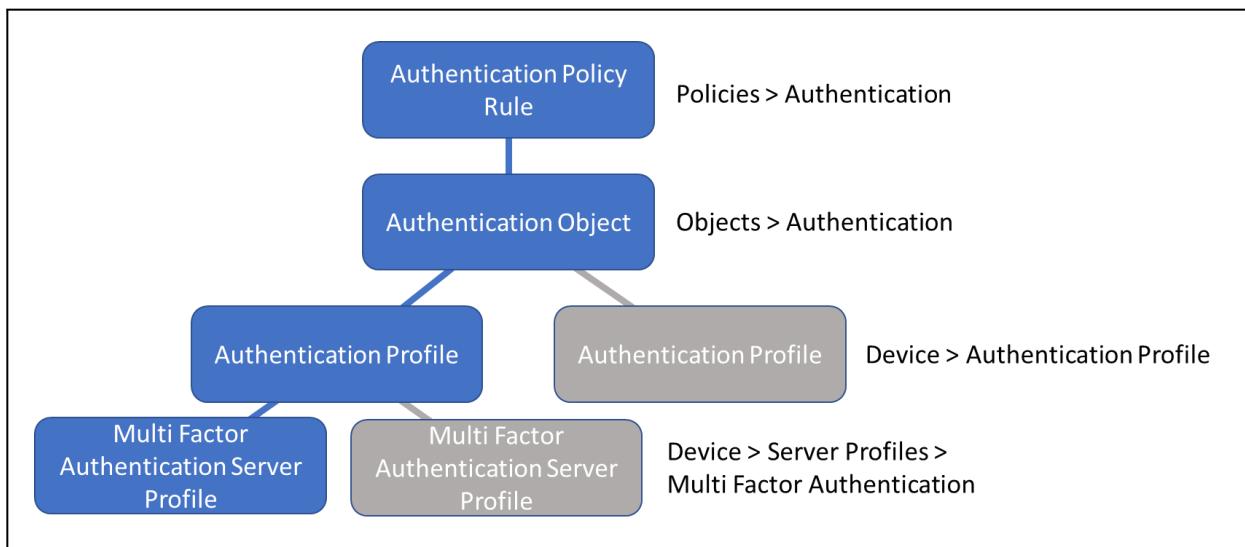
Log Settings

Log Authentication Timeouts

Log Forwarding: **None**

OK Cancel

The following figure shows the relationship of the required objects to configure the Authentication policy rule.

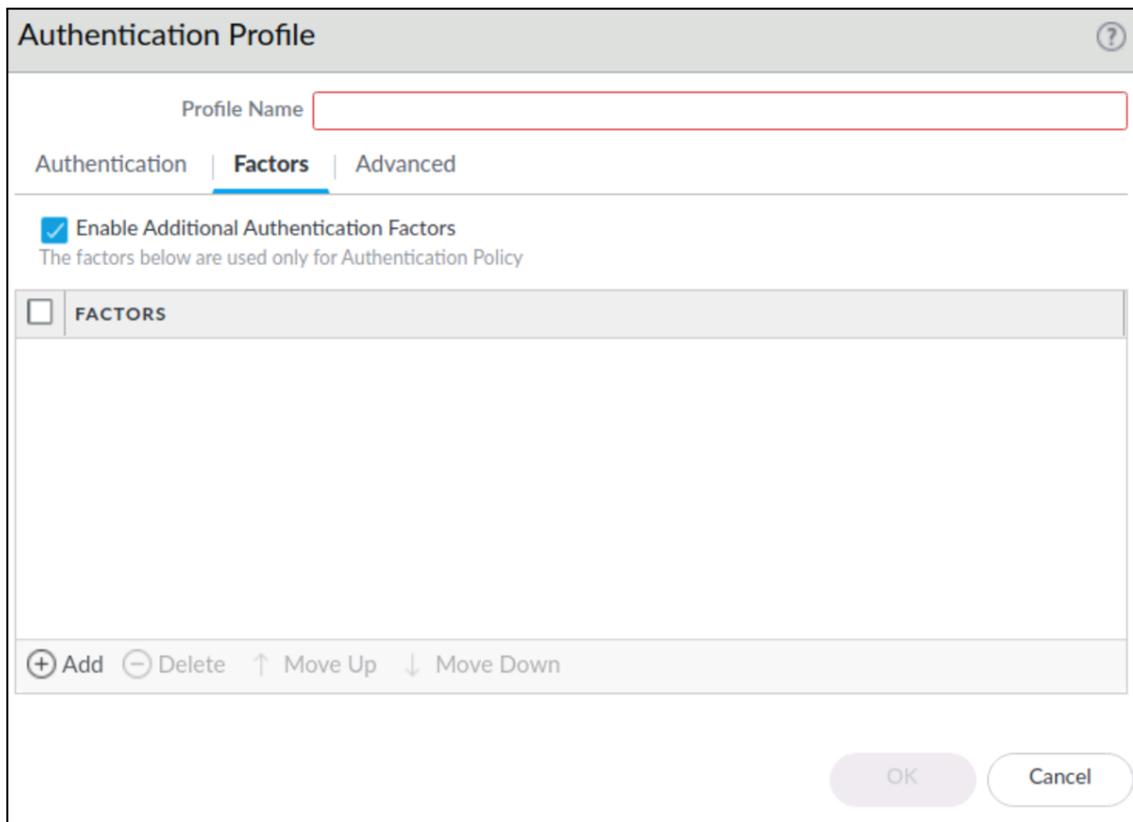


- **Multi Factor Authentication Server Profile:** Defines the access method, location, and authentication for integrated MFA vendors. The **MFA Vendor** drop-down list shows supported vendors. A **Certificate Profile** is required to support the certificate used to validate the certificate used by the MFA solution to secure its communication with the firewall.

Server Settings	
MFA Vendor	Duo v2
NAME	Duo v2
API Host	Okta Adaptive
Integration Key	PingID
Secret Key	RSA SecurID Access
Timeout (sec)	30 [5 - 600]
Base URI	/auth/v2

OK Cancel

- **Authentication Profile:** Specifies the authentication type and Server Profile for the first Captive Portal-driven authentication. The **Factors** tab incorporates the integrated MFA vendor defined in the Multi Factor Authentication Server Profile. Multiple factors can be added that require the user to pass each challenge from the top down.



- **Authentication Enforcement object:** Specifies the Authentication Profile to use and is assigned to an Authentication policy rule. A Captive Portal authentication method also must be specified. A custom message can be included for the user that explains how to respond to the challenge.

### 1.5.3 Captive Portal versus GP Client

#### *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 SSO or NTLM in [Captive Portal 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 client*

The GlobalProtect client software runs on end user systems and enables access to your network resources via the GlobalProtect portals and gateways you have deployed. There are two types of GlobalProtect clients: the GlobalProtect agent and GlobalProtect app.

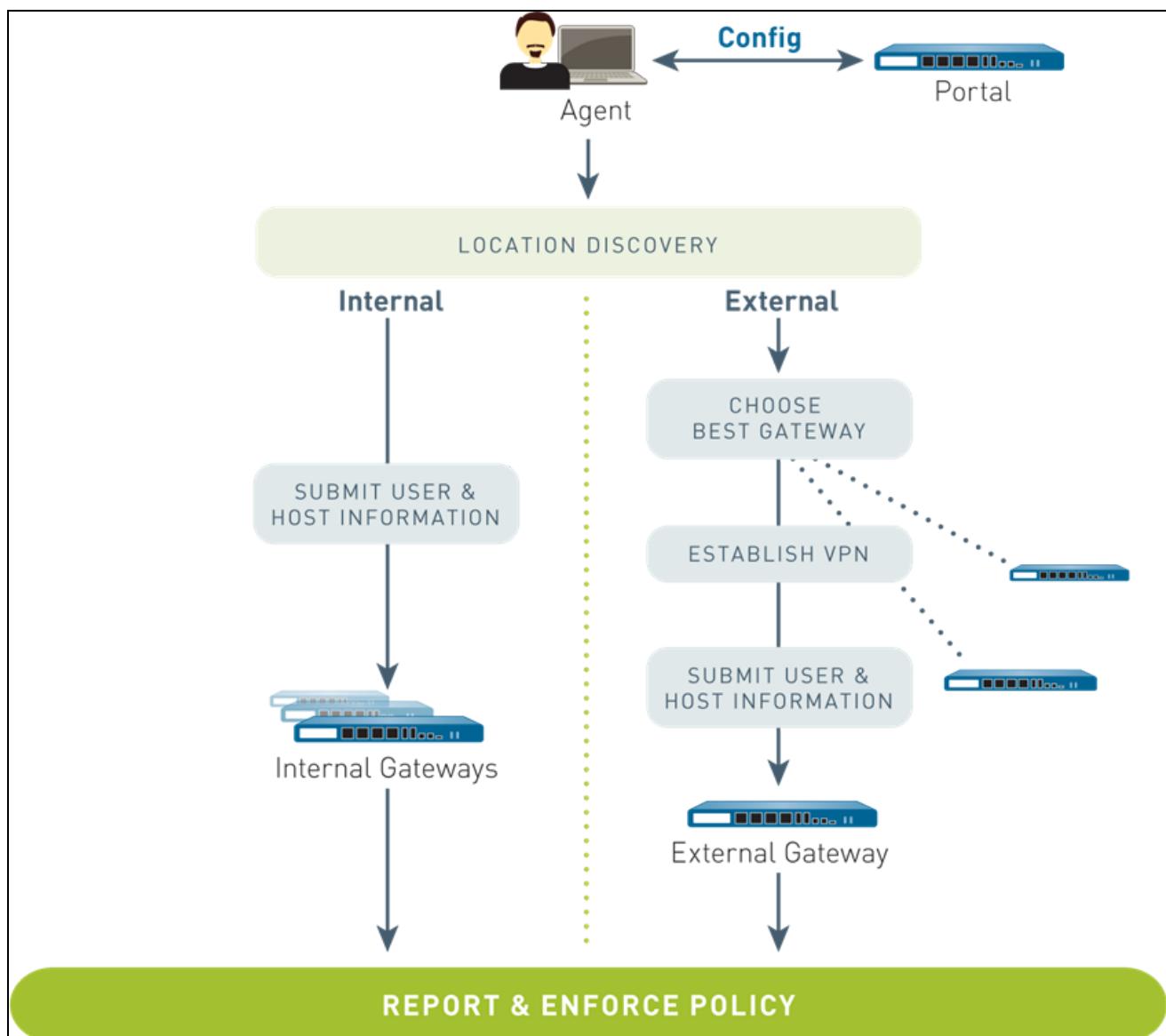
#### **The GlobalProtect Agent**

The **GlobalProtect agent** runs on Windows and macOS systems and is deployed from the GlobalProtect portal. You configure the behavior of the agent — for example, which tabs users can see — in the client configuration(s) you define on the portal. See [Define the GlobalProtect Agent Configurations](#), [Customize the GlobalProtect Agent](#), and [Deploy the GlobalProtect Agent Software](#) for details.

### The GlobalProtect App

The **GlobalProtect app** runs on iOS, Android, Windows Universal window platform (UWP), and Chromebook devices. Users must obtain the GlobalProtect app from the Apple App Store (for iOS), Google Play (for Android), the Microsoft Store (for Windows UWP), or the Chrome Web Store (for Chromebook).

The following diagram illustrates how the GlobalProtect portals, gateways, agents, and apps work together to enable secure access for all your users, regardless of what devices they are using or where they are located.



## 1.5.4 References

Configure Authentication Portal:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal/configure-captive-portal>

Configure Multi-Factor Authentication:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi-factor-authentication>

Map IP Addresses to Usernames Using Authentication Portal:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal>

Authentication Policy:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/authentication-policy>

## 1.5.5 Sample Questions

1. Which firewall configuration object is used to specify more than one external authentication source for a user's login attempt?

- a. multiple Server Profiles configured to failover
- b. Authentication Sequence
- c. local user account set to failover
- d. account sequence

2. Which object links the Captive Portal method with an Authentication Profile when multi-factor authentication is configured?

- a. Multi Factor Authentication Server Profile
- b. Authentication policy rule
- c. Authentication Sequence
- d. Authentication Enforcement object

3. Which four firewall Server Profiles can provide first factor authentication for multi-factor authentication configurations? (Choose four.)

- a. HTTP
- b. Okta v2
- c. PingID
- d. Kerberos
- e. RADIUS
- f. SAML
- g. LDAP
- h. RSA SecurID Access

4. What are the two purposes of multi-factor authentication? (Choose two.)

- a. reduce the value of stolen passwords
- b. simplify password resets
- c. reduce and prevent password sharing
- d. ensure strong passwords
- e. provide single sign-on functionality

5. Which multi-factor authentication factor is *not* supported by the next-generation firewall?

- a. voice
- b. push
- c. SMS
- d. S/Key

6. What is the meaning of setting the source user to known-user in an Authentication policy rule?

- a. The user identity is known (i.e., linked to an IP address), but the resource is sensitive enough to require additional authentication.
- b. The next-generation firewall will demand user authentication, and only then will the resource be available.
- c. The source device is a known device that is used only by a single person.
- d. The firewall attempts to match only users defined in the firewall's local user database.

7. What are the two Captive Portal modes? (Choose two.)

- a. proxy
- b. transparent
- c. web form
- d. certificate
- e. redirect

8. Which action is not required when multi-factor authentication and a SAML Identity Provider are configured?

- a. Create an Authentication policy rule.
- b. Configure NTLM settings.
- c. Create an Authentication object.
- d. Create an Authentication Profile.

9. An Authentication policy rule has a Host Information (HIP) Profile. Where are the users being authenticated coming from?

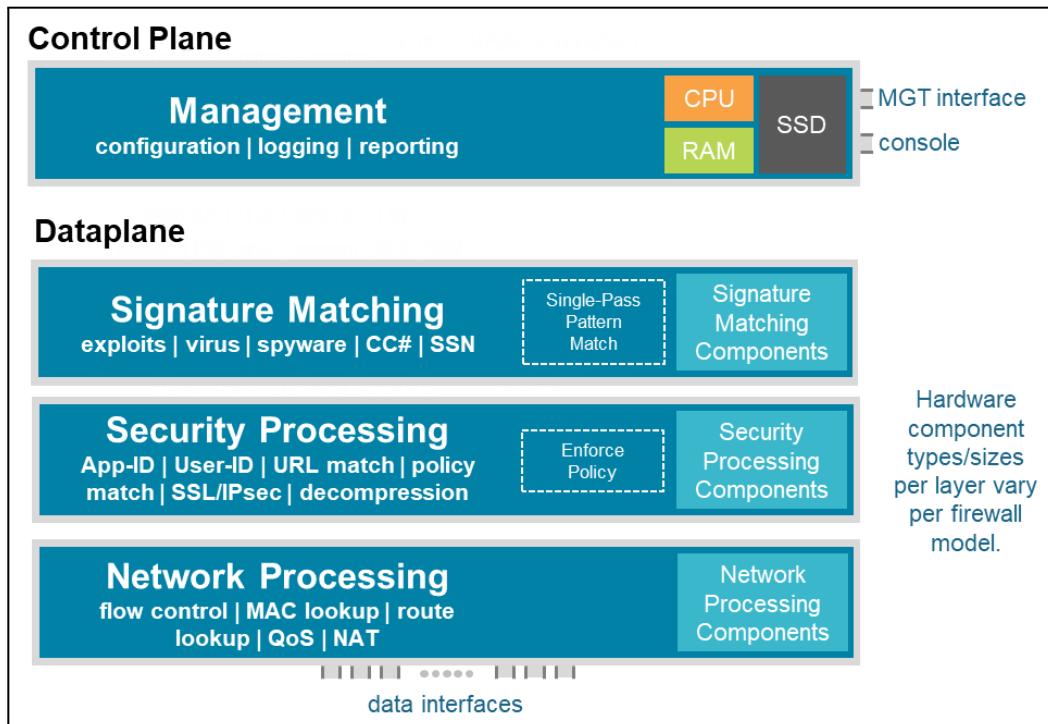
- a. internal devices, such as Linux workstations
- b. external devices belonging to customers of the organization
- c. internal servers running UNIX (e.g., Solaris, HPUX, AIX)
- d. GlobalProtect connections through the internet

## 1.6 Differentiate between the fundamental functions that reside on the management plane and data plane

*Identify functions that reside on the management plane*

### Management Planes and Data Planes

Whether the management plane and data plane functionality is physical or virtual, it is integral to all Palo Alto Networks firewalls. These functions have dedicated hardware resources, which makes them independent of each other. The following figure details the architecture of a PA-220 firewall.



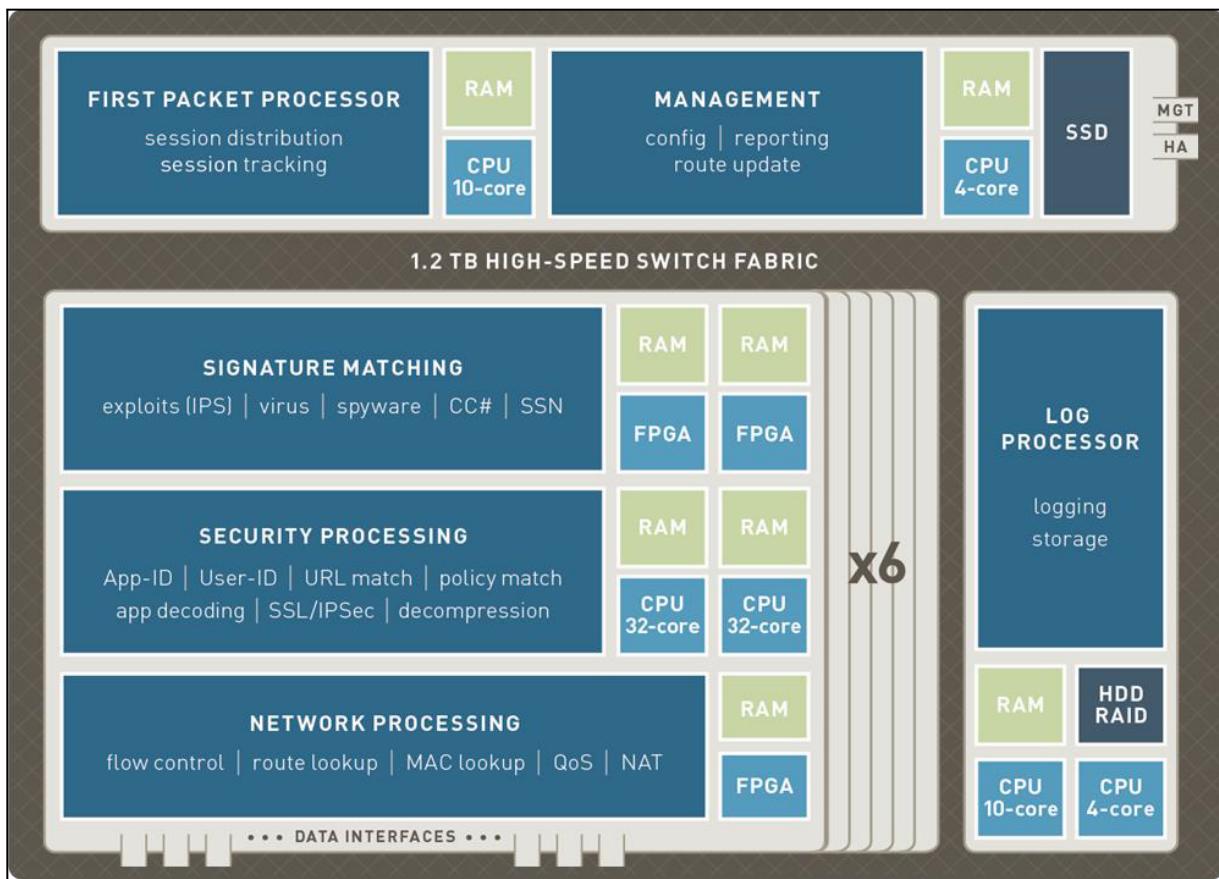
Palo Alto Networks maintains the management plane and data plane separation to protect system resources.

Every Palo Alto Networks firewall assigns a minimum of these functions to the management plane:

- Configuration management
- Logging
- Reporting functions
- User-ID agent process
- Route updates

The management network and console connector terminate directly on this plane.

On the PA-7000 Series firewalls, dedicated log collection and processing is implemented on a separate card. The following figure provides an overview of the PA-7000 Series architecture.



### *Identify functions that reside on the data plane*

The following functions are assigned to the data plane:

- Signature match processor
- All Content-ID and App-ID services
- Security processors
- Session management
- Encryption and decryption
- Compression and decompression
- Policy enforcement
- Network processor
- Route
- Address Resolution Protocol (ARP)
- MAC lookup
- QoS

- NAT
- Flow control

The data plane connects directly to the traffic interfaces. As more computing capability is added to more powerful firewall models, the management planes and data planes gain other functionality as required, sometimes implemented on dedicated cards. Several core functions gain field-programmable gate arrays (FPGAs) or custom application-specific integrated circuits for flexible high-performance processing. Additional management plane functions might include the following:

- First packet processing
- Switch fabric management

### *Scope the impact of using SSL decryption*

When decryption is performed correctly, it enhances security. It prevents adversaries from misusing encrypted traffic to attack your organization. Decrypting traffic can weaken security, but if you follow best practices, decryption will provide your visualization requirements into all traffic. Decryption will also protect you from adversaries that hide threats in encrypted tunnels.

### *Scope the impact of turning logs on for every Security policy*

By default, traffic that hits default policies will not get logged into traffic logs.

#### **1.6.1 References**

SSL Decryption Series: The Security Impact of HTTPS Interception:

<https://blog.paloaltonetworks.com/2018/10/ssl-decryption-series-security-impact-https-interception/>

Size the Decryption Firewall Deployment:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/prepare-to-deploy-decryption/size-the-decryption-firewall-deployment>

Tune or Reduce Firewall Logs:

<https://splunk.paloaltonetworks.com/tune-or-reduce-firewall-logs.html>

#### **1.6.2 Sample Questions**

1. On a PA-7000 Series firewall, which management function runs on a separate, dedicated card?

- configuration management
- logging
- reporting
- management web service

2. Do some next-generation firewall models use FPGA chips?

- no, never

- b. yes, on the data plane, but only on higher-end models
  - c. yes, on the management plane, but only on higher-end models
  - d. on both the data plane and the management plane, but only on higher-end models
3. Which function resides on the management plane?
- a. App-ID matching
  - b. route lookup
  - c. policy match
  - d. logging

# Domain 2- Deploy and Configure Core Components

## 2.1 Configure Management Profiles

Use Interface Management profiles to restrict access. For example, you want to prevent users from accessing the firewall web interface over the ethernet1/1 interface, while allowing this interface to receive Simple Network Management Protocol (SNMP) queries for your IT monitoring system. To do this, you would enable SNMP and disable HTTP/HTTPS in an Interface Management profile and assign the profile to ethernet1/1.

### 2.1.1 Interface Management Profile

To configure an Interface Management Profile, perform the following steps:

1. Navigate to **Network > Network Profiles > Interface Mgmt** and click **Add**.
2. Select the network **protocols** that the interface permits (allows) for management traffic. Choose from **Ping, Telnet, SSH, HTTP, HTTP OCSP, HTTPS, or SNMP**.
3. Select the **services** that the interface permits for management traffic. Choose from the following:
  - a. **Response Pages** (for Authentication Portal or URL Admin Override)
  - b. **User-ID** (to redistribute data and authentication timestamps)
  - c. **User-ID Syslog Listener-SSL** or **User-ID Syslog Listener-UDP** (to configure User-ID to monitor syslog senders for user mapping over SSL or User Datagram Protocol (UDP) traffic)
4. Optionally, add IP addresses to permit access to the interface. If you don't add an IP address, the interface will have no IP address restrictions.
5. Click **OK**.

### 2.1.2 SSL/TLS profile

Palo Alto Networks firewalls and Panorama use SSL/TLS service profiles to specify a certificate and the allowed protocol versions for SSL/TLS services. The firewall and Panorama use SSL/TLS for Authentication 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 the firewall or Panorama to avoid SSL/TLS versions that have known weaknesses. If a service request involves a protocol version that is outside the specified range, the firewall or Panorama downgrades or upgrades the connection to a supported version.

Following are the steps to generate or import a certificate on the firewall for each desired service:

**Step 1:** Select Device > Certificate Management > SSL/TLS Service Profile.

**Step 2:** If the firewall has more than one virtual system (vsys), select the **Location (vsys or Shared)** where the profile is available.

**Step 3:** Click **Add** and enter a **Name** to identify the profile.

**Step 4:** Select the **Certificate** you just obtained.

**Step 5:** 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 6:** Click **OK** and **Commit**.

### 2.1.3 References

Use Interface Management Profiles to Restrict Access:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/configure-interfaces/use-interface-management-profiles-to-restrict-access>

Administrative Access Best Practices:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html>

How to Configure the Management Interface IP:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK>

Network > Network Profiles > Interface Mgmt:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-profiles/network-network-profiles-interface-mgmt>

Configure an SSL/TLS Service Profile:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service-profile>

### 2.1.4 Sample Questions

When configuring the Interface Management Profile, you select the protocols that the interface permits for management traffic. Why is permitting HTTP or Telnet protocols not recommended? Select all that apply.

- HTTP and Telnet protocols transmit in cleartext.
- HTTP and Telnet protocols are vulnerable to sniffing, spoofing, and brute force attacks.
- HTTP and Telnet protocols raise the risk of port stealing.
- HTTP and Telnet protocols are secure and safe.

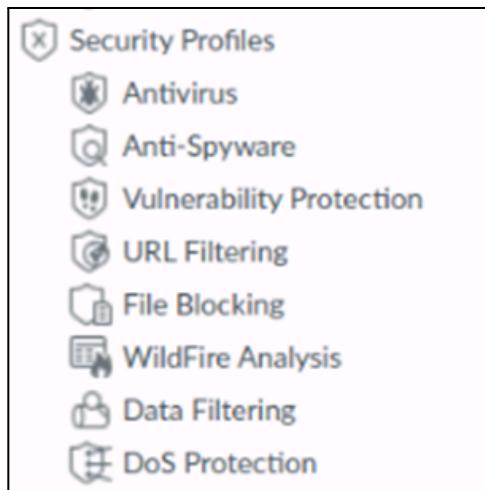
## 2.2 Deploy and configure Security Profiles

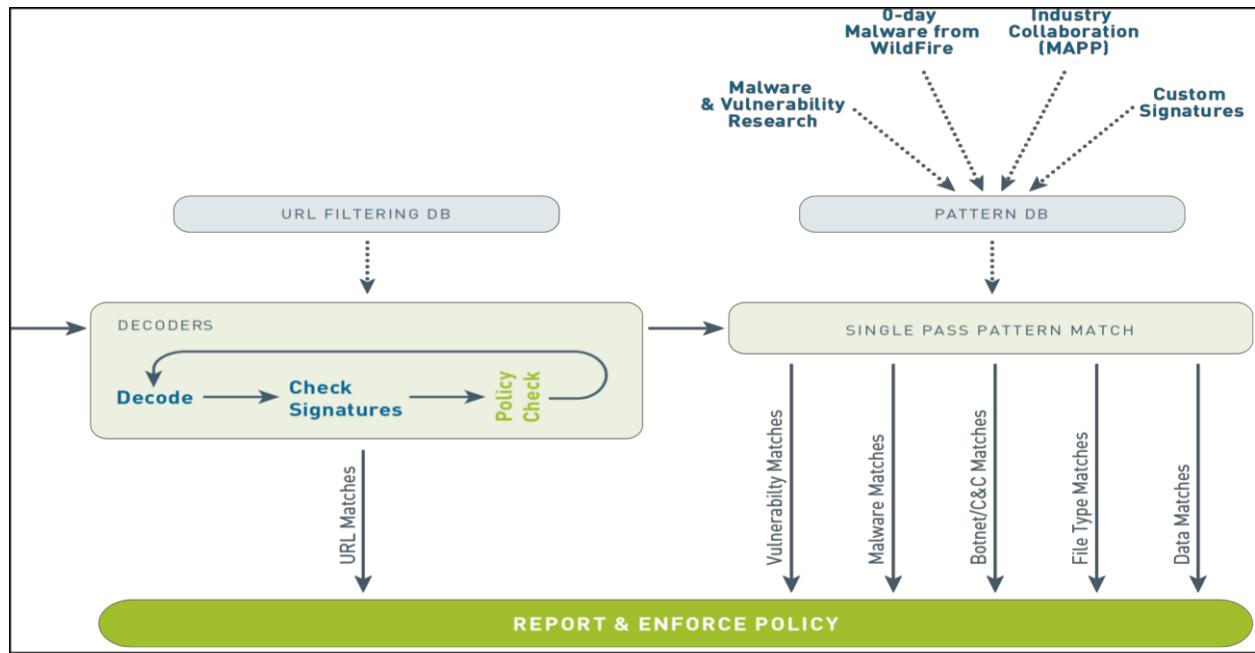
Security Profiles implement specific protections provided by the Palo Alto Networks Content-ID next-generation technology. After Security Profiles are created, they are attached to Security policy rules specifying Content-ID scans to be performed on traffic allowed by a policy rule. These profiles must be attached to Security policy rules to invoke their protections and will be applied only to the traffic handled by that particular rule.

### 2.2.1 Custom configuration of different Security Profiles and Security Profile Groups

#### *Security Profile Overview*

Security Profiles include:





All scanning is done by signature matching on a streaming basis (not a file basis). These signatures are updated based on the configuration and licensing options. For example, with a WildFire license, new virus and malware signatures can be installed as quickly as every 5 minutes. If the firewall has a Threat Prevention license but no WildFire license, signatures from WildFire would be updated only every 24 hours.

Content scanning consumes firewall resources after it is enabled. Consult a firewall comparison chart to identify the model with appropriate “Threat Enabled” throughput.

### ***Identifying Security Profiles for Use***

Although Security policy rules enable you to allow or block traffic on your network, Security Profiles help you define an allow-but-scan rule, which scans allowed applications for threats such as viruses, malware, spyware, and DoS attacks. When traffic matches the allow rule that is defined in the Security policy, the Security Profile(s) attached to the rule are applied for further content inspection, such as antivirus checks and data filtering. Security Profiles are the features that provide the services of the Content-ID feature of PAN-OS software.

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. The Security Profiles attached to Security policy “allow” rules determine the type of threat detection that is performed on the traffic.

You can add Security Profiles that are commonly applied together to create a Security Profile Group; this set of profiles can be treated as a unit and added to Security policy rules in one step (or included in Security policy rules by default, if you choose to set up a default Security Profile Group).

## ***Antivirus Profiles***

Antivirus Profiles protect against viruses, worms, Trojan horses, and spyware downloads. The Palo Alto Networks antivirus solution uses a stream-based malware prevention engine that inspects traffic the moment the first packet is received to provide protection for clients without significantly impacting firewall performance. This profile scans for a wide variety of malware in executables, PDF files, HTML, and JavaScript viruses, and it includes 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 the listed protocol decoders for viruses and generates alerts for SMTP, IMAP, and POP3 protocols while blocking for FTP, HTTP, and Server Message Block (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:** This action permits the application traffic.
- **alert:** This action generates an alert for each application traffic flow. The alert is saved in the Threat log.
- **drop:** This action drops the application traffic.
- **reset-client:** For TCP, this action resets the client-side connection. For UDP, it drops the connection.
- **reset-server:** For TCP, this action resets the server-side connection. For UDP, it drops the connection.
- **reset-both:** For TCP, this action resets the connection on both client and server ends. For UDP, it drops the connection.

Customized profiles can be used to minimize antivirus inspection for traffic between trusted security zones. Customized profiles can also maximize the inspection of traffic received from untrusted zones, such as the internet, along with 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 daily by Threat Prevention subscribers and sub-hourly for WildFire subscribers.

## ***Anti-Spyware Profiles***

Anti-Spyware Profiles block spyware on compromised hosts from trying to phone-home or beacon out to external C2 servers, thus 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 an internet-facing zone.

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 rule:

- **Default:** This profile uses the default action for every signature, as specified by Palo Alto Networks when the signature is created.
- **Strict:** This profile 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 low- and informational-severity signatures.

After 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. The default action typically 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:** This action permits the application traffic.
- **alert:** This action generates an alert for each application traffic flow. The alert is saved in the Threat log.
- **drop:** This action drops the application traffic.
- **reset-client:** For TCP, this action resets the client-side connection. For UDP, it drops the connection.
- **reset-server:** For TCP, this action resets the server-side connection. For UDP, it drops the connection.
- **reset-both:** For TCP, this action resets the connection on both client and server ends. For UDP, it drops the connection.

**Note:** In some cases, when the profile action is set to reset-both, the associated Threat log might display the action as reset-server, which occurs when the firewall detects a threat at the beginning of a session and presents the client with a 503 block page. Because the block page disallows the connection, the client side does not need to be reset, and only the server-side connection is reset.

- **Block IP:** This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

You can also 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, thus 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 then can be easily identified in the Traffic logs and Threat logs because any host that attempts to connect to the sinkhole IP address most likely is infected with malware.

The procedure to configure Anti-Spyware Profiles and Vulnerability Protection Profiles is similar within the management web interface.

### **Vulnerability Protection Profiles**

Vulnerability Protection Profiles stop attempts to exploit system flaws or gain unauthorized access to systems. Although 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 also can create exceptions that allow you to change the response to a specific signature.

After the firewall detects a threat event, you can configure the following actions in an Vulnerability Protection Profile:

- **default:** For each threat signature and anti-spyware signature that is defined by Palo Alto Networks, a default action is specified internally. The default action typically 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:** This action permits the application traffic.
- **alert:** This action generates an alert for each application traffic flow. The alert is saved in the Threat log.
- **drop:** This action drops the application traffic.
- **reset-client:** For TCP, this action resets the client-side connection. For UDP, it drops the connection.
- **reset-server:** For TCP, this action resets the server-side connection. For UDP, it drops the connection.
- **reset-both:** For TCP, this action resets the connection on both client and server ends. For UDP, it drops the connection.

**Note:** In some cases, when the profile action is set to reset-both, the associated Threat log might display the action as reset-server. This occurs when the firewall detects a threat at the beginning of a session and presents the client with a 503-block page. Because the block page disallows the connection, the client side does not need to be reset, and only the server-side connection is reset.

- **Block IP:** This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

### ***URL Filtering Profiles***

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 then can customize the newly added URL Filtering Profiles and add lists of specific websites that always should be blocked or allowed. This information 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 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 Filtering Profile that will have all categories set to allow for visibility into the traffic on your network. You then can customize the newly added

URL Filtering profiles and add lists of specific websites that always should be blocked or allowed, which provides more granular control over URL categories.

URL filtering requires a URL Filtering subscription that keeps URL category classification information current. This subscription provides descriptive data as to which type of information is at a given URL. Profiles can implement various actions against categories that reflect the organization's use policies and risk posture.

### **Data Filtering Profiles**

Data Filtering Profiles prevent sensitive information such as credit card numbers or Social Security numbers from leaving a protected network. The Data Filtering Profile also allows you to filter on keywords, such as a sensitive project name or the word "confidential." It should focus your profile on the desired file types to reduce false-positives. For example, you may want to search only Word documents or Excel spreadsheets. You also may want to scan only web-browsing traffic or FTP.

You can create custom data pattern objects and attach them to a Data Filtering Profile to define the type of information that you want to filter. Create data pattern objects based on the following:

- **Predefined patterns:** Filter for credit card numbers and Social Security numbers (with or without dashes) using predefined patterns
- **Regular expressions:** Filter for a string of characters
- **File properties:** Filter for file properties and values based on file type

**Note:** If you are using a third-party, endpoint DLP solution to populate file properties to indicate sensitive content, this option enables the firewall to enforce your DLP policy.

### **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 or download, and you can specify which applications will be subject to the File Blocking Profile. You also can configure custom response pages that will appear when a user attempts to download the specified file type. This response page allows the user to pause to consider whether to continue and download a file.

You can define your own custom File Blocking Profiles or choose one of the following predefined profiles when applying file blocking to a Security policy rule. The predefined profiles, which are available with content release version 653 and later, allow you to quickly enable best practice file blocking settings:

- **Basic file blocking:** Attach this profile to the Security policy rules that allow traffic to and from less sensitive applications to block files that commonly are included in malware attack campaigns or that have no real use case for upload or download. This profile blocks upload and download of PE files (.scr, .cpl, .dll, .ocx, .pif, .exe), Java files (.class, .jar), Help files (.chm, .hlp), and other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, and .bat. It also prompts users to acknowledge when they attempt to download encrypted-rar or encrypted-zip files. This rule alerts on all other file types to give you complete visibility into all file types entering and leaving your network.

- **Strict file blocking:** Use this stricter profile on the Security policy rules that allow access to your most sensitive applications. This profile blocks the same file types as the basic file blocking profile, plus flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files.

Configure a File Blocking Profile with the following actions:

- **alert:** After the specified file type is detected, a log is generated in the Data Filtering log.
- **block:** After the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log also is generated in the Data Filtering log.
- **continue:** After 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 also is generated in the Data Filtering log. Because this type of forwarding action requires user interaction, it is applicable only 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. This detection is for zero-day threats contained in files. The firewall's anti-virus threat detection finds known viruses based on local resources. Specify files to be forwarded for analysis based on application, file type, and transmission direction (upload or download). Files matched to the profile rule are forwarded to 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. If a profile rule is set to forward files to the WildFire public cloud, the firewall also forwards files that match existing antivirus signatures in addition to unknown files.

You also can use WildFire Analysis Profiles to set up a WildFire hybrid cloud deployment. If you are using a WildFire appliance to locally analyze sensitive files (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. Use of both the WildFire appliance and the WildFire cloud for analysis allows you to benefit from a prompt verdict for files that already have been processed by the cloud and for files that are not supported for appliance analysis. It also frees the appliance capacity to process sensitive content.

The WildFire cloud can scan your organization's files using an appropriately configured WildFire Analysis Profile. A profile includes match conditions describing file characteristics you want to forward to WildFire for analysis. As files matching these conditions are transferred through your firewall, a copy is sent to WildFire for analysis.

**Note:** Files are *not* quarantined pending WildFire evaluation. In cases of positive malware findings, the security engineer must use information collected on the firewall and by WildFire to locate the file internally for remediation.

WildFire Analysis Profiles indicate which files are to be forwarded according to system-wide WildFire configuration settings. WildFire typically renders a verdict on a file within 5 to 10 minutes of receipt.

WildFire analysis results in a detailed report including all aspects of the original file and the contained malware. This report is a valuable tool that describes the exact nature of the detected threat.

### ***DoS Protection Profiles***

DoS Protection profiles provide detailed control for DoS Protection policy rules. DoS Protection profiles 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. Palo Alto Networks firewalls support these two DoS protection mechanisms:

- **Flood protection:** Detects and prevents attacks where the network is flooded with packets, which results in too many half-open sessions or services being unable to respond to each request. In this case, the source address of the attack usually is spoofed.
- **Resource protection:** Detects and prevents session exhaustion attacks. In this type of attack, many 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 Protection profile is used to specify the type of action to take and the details on matching criteria for the DoS policy. The DoS Protection profile defines threshold settings for synchronize (SYN), UDP, and Internet control message protocol (ICMP) floods; can enable resource protection; and defines the maximum number of concurrent connections. After you configure the DoS Protection profile, you attach it to a DoS policy rule.

When you configure DoS protection, you should analyze your environment to set the correct thresholds based on your actual traffic rather than use the default values provided.

### **2.2.2 Relationship between URL filtering and credential theft prevention**

#### ***Phishing Prevention Overview***

The Palo Alto Networks URL filtering solution complements [App-ID](#) by controlling access to web (HTTP and HTTPS) traffic and protecting your network from attack.

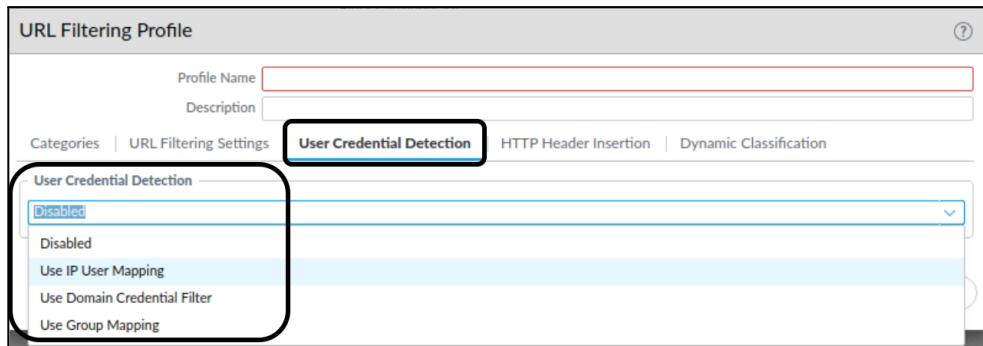
With URL filtering enabled, all web traffic is compared against the URL filtering database, which contains a list of millions of categorized websites. You can use these URL categories as match criteria to enforce Security policy, safely enable web access, and control the traffic that traverses your network. You also can use URL filtering to enforce safe search settings for your users and to prevent credential phishing based on URL category.

Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose which websites you want to allow or block corporate credential submissions based on the URL category of the website. When the firewall detects a user credential being transmitted to a site in a category you have restricted, it either displays a block response page that prevents the user from submitting credentials or presents a continue page that warns users against submitting credentials to sites classified in certain URL categories. The firewall still allows the user to continue with the credential submission. You can customize these block pages to educate users against reusing corporate credentials, even on legitimate, non-phishing sites.

## Credential Detection

Before you configure credential phishing protection, decide which method you want the firewall to use to identify credentials. Each method requires the configuration of User-ID technology. The *IP address-to-username mapping* and *group mapping* methods check for valid username submissions only. In these cases, the firewall blocks or allows the submission based on your settings, regardless of the accompanying password submitted. The *domain credential filter* method checks for valid usernames and passwords submitted to a webpage:

- **IP address-to-username mapping (using PAN-OS-integrated agent):** The firewall uses IP-address-to-user mappings that User-ID collects to check if a username submitted to a webpage matches the username of the logged-in user.
- **Group mapping (using PAN-OS integrated agent):** The User-ID agent collects group mapping information from a directory server and retrieves a list of groups and corresponding group members. It compares usernames submitted to a webpage against the group member usernames.
- **Domain credential filter (using Windows-based agent):** The User-ID agent is installed on a Read-Only Domain Controller. The User-ID agent collects password hashes that correspond to users for which you want to enable credential detection, and it sends these mappings to the firewall. The firewall then checks if the source IP address of a session matches a username and if the password submitted to the webpage belongs to that username. With this mode, the firewall blocks or alerts on the submission only when the password submitted matches a user password.



## Category Selection for Enforcement

After the detection method is chosen for the URL Filtering Profile, the enforcement action must be chosen for each appropriate browsing category. Custom categories can be created when flexibility is required in identifying specific category members. For each category, select how you want to treat user credential submissions:

- **alert:** Allow users to submit credentials to the website, but generate a URL Filtering log each time a user submits credentials to sites in this URL category.
- **allow:** (default) Allow users to submit credentials to the website.

- **block:** Block users from submitting credentials to the website. When a user tries to submit credentials, the firewall displays the Anti Phishing Block page, which prevents the credential submission.
- **continue:** The firewall displays the Anti Phishing Continue page response page when a user attempts to submit credentials. Users must select **Continue** on the response page to continue with the submission.

The screenshot shows the 'URL Filtering Profile' configuration window. On the left, there's a list of categories under 'Pre-defined Categories' such as abortion, abused-drugs, adult, alcohol-and-tobacco, auctions, and business-and-economy. On the right, there are two tables: 'SITE ACCESS' and 'USER CREDENTIAL SUBMISSION'. The 'USER CREDENTIAL SUBMISSION' table has several rows, each with 'allow' in both columns. A callout box points to this table with the text: 'Select how you want to treat user credential submissions for each category.'

SITE ACCESS	USER CREDENTIAL SUBMISSION
allow	allow

When the firewall detects a user attempting to submit credentials to a site in a category that you have restricted, it either displays a block response page that prevents the user from submitting credentials or presents a continue page that warns users against submitting credentials to sites classified in certain URL categories. The firewall still allows the user to continue with the credential submission. You can customize these block pages to educate users against reusing corporate credentials, even on legitimate, non-phishing sites.

### 2.2.3 Use of username and domain name in HTTP header insertion

The firewall supports header insertion for HTTP/1.x traffic only. The firewall does not support header insertion for HTTP/2 traffic. You can create insertion entries based on a predefined HTTP header insertion type, or you can create your own custom type. Header insertion is performed for custom HTTP headers. You can also insert standard HTTP headers.

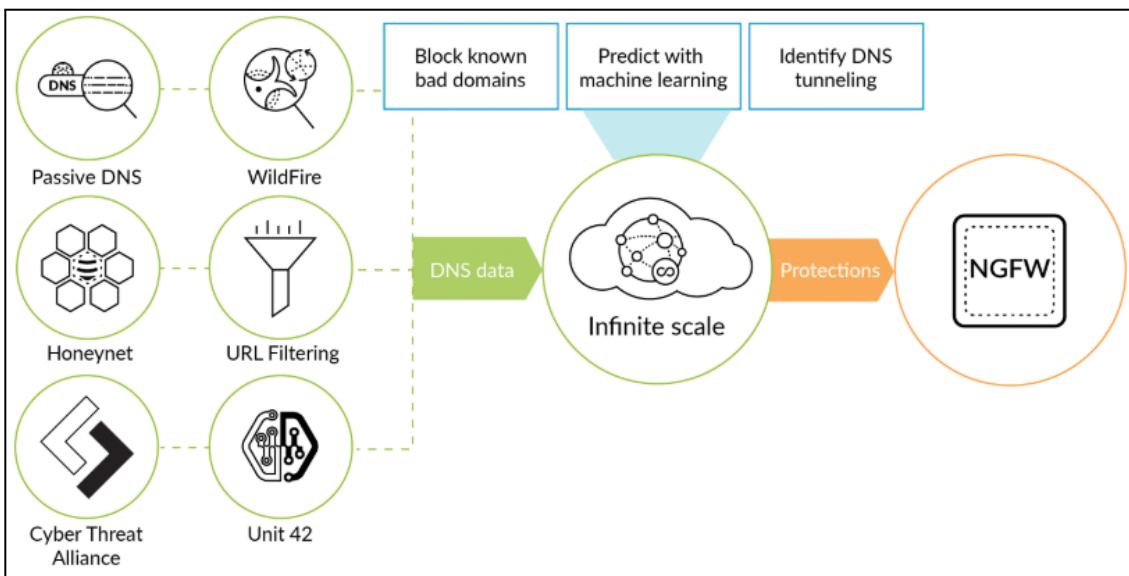
HTTP header insertion can only be performed using the following methods:

- GET
- POST
- PUT

- HEAD

## 2.2.4 DNS Security

DNS Security allows you to apply predictive analytics, ML, and automation to block attacks that use DNS. Tight integration with the NGFW gives you automated protections and eliminates the need for independent tools. Now you can rapidly predict and prevent malicious domains, neutralize threats hidden in DNS tunneling, and apply automation to quickly find and contain infected devices. The following illustration depicts DNS Security sources, intermediate processing of source data, and ultimate delivery to a firewall.



## 2.2.5 How to tune or add exceptions to a Security Profile

Palo Alto Networks defines a recommended default action (such as block or alert) for threat signatures. You can use a threat ID to exclude a threat signature from enforcement or modify the action the firewall enforces for that threat signature. For example, you can modify the action for threat signatures that are triggering false-positives on your network.

Configure threat exceptions for antivirus, vulnerability, spyware, and DNS signatures to change firewall enforcement for a threat. However, before you begin, make sure the firewall is detecting and enforcing threats based on the default signature settings:

- Get the latest Antivirus, Threats and Applications, and WildFire signature updates.
- Set up Antivirus, Anti-Spyware, and Vulnerability Protection subscriptions, and apply these Security Profiles to your Security policy.

**Step 1:** Exclude antivirus signatures from enforcement.

- Select **Objects > Security Profiles > Antivirus**.

- Add or modify an existing Antivirus Profile from which you want to exclude a threat signature, and select **Signature Exceptions**.
- Add the **Threat ID** for the threat signature you want to exclude from enforcement.

THREAT ID	THREAT NAME	
280647	JS/Exploit.pdfka.os	<input type="checkbox"/>

Threat ID **280647**    **+ Add**    **PDF/CSV**

- Click **OK** to save the Antivirus Profile.

**Step 2:** Modify enforcement for vulnerability and spyware signatures. (This does not include DNS signatures; skip to the next option to modify enforcement for DNS signatures, which are a type of spyware signature.)

- Select **Objects > Security Profiles > Anti-Spyware** or **Objects > Security Profiles > Vulnerability Protection**.
- Add or modify an existing Anti-Spyware Profile or Vulnerability Protection Profile from which you want to exclude the threat signature. Then, select either **Signature Exceptions for Anti-Spyware Protection profiles** or **Exceptions for Vulnerability Protection profiles**.
- Show all signatures, then filter to select the signature for which you want to modify enforcement rules.
- Check the box under the **Enable** column for the signature whose enforcement you want to modify.
- Select the **Action** you want the firewall to enforce for this threat signature.

Vulnerability Protection Profile

Name	False Positives																																																																
Description																																																																	
Rules	<a href="#">Exceptions</a>																																																																
<div style="border: 1px solid #ccc; padding: 5px;"> <b>Edit Action</b> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <b>Action</b> <b>Allow</b> <span style="float: right;">Cancel</span> <ul style="list-style-type: none"> <li>Reset Server</li> <li>Reset Client</li> <li>Reset Both</li> <li>Drop</li> <li>Default (Alert)</li> <li>Block IP</li> <li><b>Allow</b></li> <li>Alert</li> </ul> </div> </div>																																																																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2"></th> <th colspan="6">15016 items → X</th> </tr> <tr> <th>ACTION</th> <th>PACKET CAPTURE</th> <th colspan="6"></th> </tr> </thead> <tbody> <tr> <td>(alert)</td> <td></td> <td colspan="6"></td> </tr> <tr> <td>high</td> <td>default (alert)</td> <td>enable</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>informational</td> <td>default (alert)</td> <td>enable</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>high</td> <td>default (alert)</td> <td>enable</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>info-leak</td> <td>default</td> <td>enable</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>informational</td> <td>default</td> <td>enable</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				15016 items → X						ACTION	PACKET CAPTURE							(alert)								high	default (alert)	enable						informational	default (alert)	enable						high	default (alert)	enable						info-leak	default	enable						informational	default	enable					
		15016 items → X																																																															
ACTION	PACKET CAPTURE																																																																
(alert)																																																																	
high	default (alert)	enable																																																															
informational	default (alert)	enable																																																															
high	default (alert)	enable																																																															
info-leak	default	enable																																																															
informational	default	enable																																																															
<input checked="" type="checkbox"/> Show all signatures <a href="#">PDF/CSV</a>																																																																	

- For signatures that you want to exclude from enforcement because they trigger false-positives, set the **Action** to **Allow**.
- Click **OK** to save your new or modified Anti-Spyware Profile or Vulnerability Protection Profile.

### Step 3: Modify enforcement for DNS signatures.

By default, the DNS lookups for malicious hostnames that DNS signatures detect are sinkholed.

- Select **Objects > Security Profiles > Anti-Spyware**.
- Add or modify the Anti-Spyware Profile from which you want to exclude the threat signature, then select **DNS Exceptions**.
- Search for the **DNS Threat ID** for the DNS signature that you want to exclude from enforcement, then select the box of the applicable signature:

DNS Signature Exceptions

DNS Signature Exceptions			
<input type="text" value="64741252"/> 1 item → X			
ENABLE	THREAT ID	DOMAIN/FQDN	THREAT NAME
<input checked="" type="checkbox"/>	64741252	ftp.hinet.dns-dns.com	generic:ftp.hinet.dns-dns.com

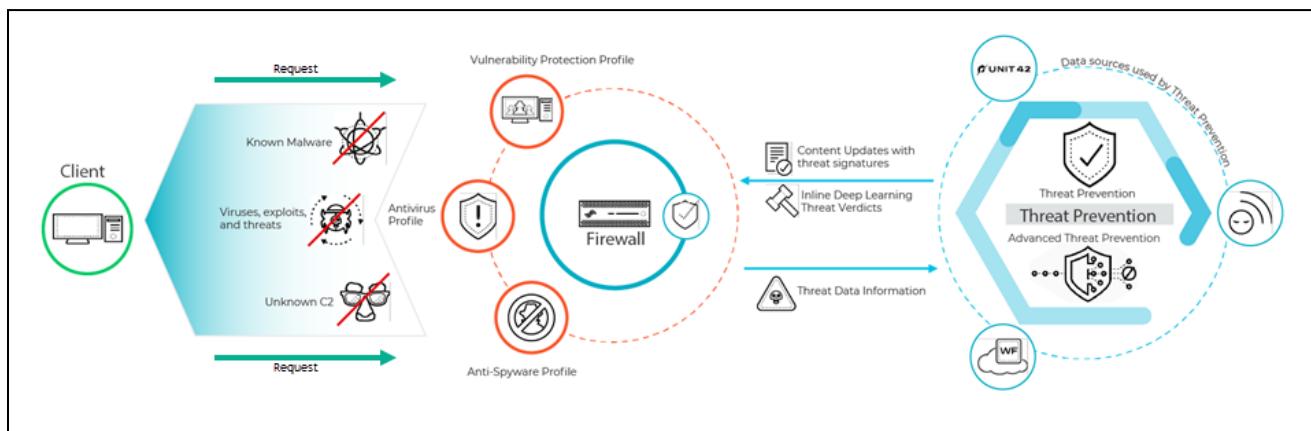
- Click **OK** to save your new or modified Anti-Spyware Profile.

## 2.2.6 Compare and contrast threat prevention and advanced threat prevention

### Threat Prevention

Threat Prevention is an IPS solution that can detect and block malware, vulnerability exploits, and C2 across all ports and protocols. It uses a multilayered prevention system with components operating on the firewall and in the cloud. The Threat Prevention cloud operates a multitude of detection services using combined threat data from Palo Alto Networks services to create signatures, each possessing specific identifiable patterns, that are used by the firewall to enforce security policies when matching threats and malicious behaviors are detected. These signatures are categorized based on the threat type and are assigned unique identifier numbers. To detect threats that correspond with these signatures, the firewall operates analysis engines that inspect and classify network traffic exhibiting anomalous traits.

In addition to the signature-based detection mechanism, Advanced Threat Prevention provides a complementary inline detection system to prevent unknown and evasive C2 threats. The Advanced Threat Prevention cloud operates deep learning models that enable inline analysis on the firewall on a per-request basis to prevent zero-day threats from entering the network.



The threat signatures used by the firewall are broadly categorized into three types: antivirus, anti-spyware, and vulnerability. These types are used by Security Profiles to enforce user-defined policy.

- Antivirus signatures detect various types of malware and viruses, including worms, Trojan horses, and spyware downloads.
- Anti-spyware signatures detect C2 spyware on compromised hosts that try to phone-home or beacon out to an external C2 server.
- Vulnerability signatures detect exploit system vulnerabilities.

Signatures have a default severity level with an associated default action; for example, in the case of a highly malicious threat, a setting of reset both. This setting is based on security recommendations from Palo Alto Networks. In deployments that use specialized internal applications or third-party intelligence feeds with open source SNORT and Suricata rules, custom signatures can be created for purpose-built protection. Firewalls receive signature updates as two update packages: the daily antivirus content update and the

weekly application and threats content update. The antivirus content updates include antivirus signatures and DNS (C2) signatures used by the Antivirus and Anti-Spyware Profiles, respectively. The Applications and Threats content updates include vulnerability and anti-spyware signatures used by the Vulnerability and Anti-Spyware Profiles, respectively. The update packages also include content that is leveraged by other services and subfunctions. For more information, refer to [Dynamic Content Updates](#).

### ***Advanced Threat Prevention***

Advanced Threat Prevention is a cloud-delivered security service that works in conjunction with your existing Threat Prevention license to deliver protections for advanced and evasive C2 threats. Advanced Threat Prevention allows you to prevent unknown threats using real-time traffic inspection and inline detectors. These deep learning, ML-based detection engines in the Advanced Threat Prevention cloud analyze traffic for advanced C2 and spyware threats to protect users against zero-day threats. By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages or operate process-intensive, firewall-based analyzers, which can sap resources. The cloud-based detection engine logic is continuously monitored and updated using C2 traffic datasets from WildFire, with additional support from Palo Alto Networks threat researchers who provide human intervention for highly accurate detection enhancements. Advanced Threat Prevention deep learning engines support analysis of C2-based threats over HTTP, HTTP2, SSL, unknown-UDP, and unknown-TCP applications. Additional analysis models are delivered through content updates; however, enhancements to existing models are performed as a cloud-side update, requiring no firewall update. Advanced Threat Prevention is enabled and configured under [inline cloud analysis](#) in the Anti-Spyware Profile.

## **2.2.7 Compare and contrast URL Filtering and Advanced URL Filtering**

### ***URL Filtering***

- URL Filtering allows you to protect your organization against web-based threats such as phishing, malware, and C2. Inline ML instantly identifies and prevents new and unknown malicious websites before they can be accessed by users. Web Security rules are an extension of your NGFW policy, thus reducing complexity by giving you a single policy set to manage.

URL Filtering provides the following benefits:

- Reduces infection risk from dangerous websites and protects users and data from malware and credential-phishing pages
- Protects across the attack lifecycle through integration with WildFire and the cybersecurity portfolio
- Retains protections synchronized with the latest threat intelligence through the Palo Alto Networks cloud-based URL categorization for phishing, malware, and undesired content
- Provides full visibility and threat inspection into normally opaque web traffic through granular control over SSL decryption

### ***Advanced URL Filtering***

Built in the cloud, Advanced URL Filtering is a subscription service that works natively with your Palo Alto Networks NGFW to secure your network against web-based threats such as phishing, malware, and C2. Advanced URL Filtering uses ML to analyze URLs in real time and classify them into benign or malicious categories, which you can easily build into your NGFW policy for total control of web traffic. These categories trigger complementary capabilities across the NGFW platform, enabling additional layers of protection, such as targeted SSL decryption and advanced logging. Alongside its own analysis, Advanced URL Filtering uses shared threat information from WildFire, Palo Alto Networks industry-leading malware prevention service, and other sources to automatically update protections against malicious sites. Advanced URL Filtering delivers:

- Superior protection against web-based attacks with the combined power of our URL database and cloud-delivered web security engine powered by ML that categorizes and blocks new malicious URLs in real time, even when content is cloaked from crawlers. Advanced URL Filtering prevents 40 percent more threats than traditional web-filtering databases.
- Industry-leading phishing protections that tackle the most common causes of breaches
- Total control of your web traffic through fine-grained controls and policy settings that enable you to automate security actions based on users, risk ratings, and content categories
- Maximum operational efficiency by enabling web protection through the Palo Alto Networks platform

### **2.2.8 References**

Security Profiles:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>

Customize the URL Filtering Response Pages:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/customize-the-url-filtering-response-pages>

URL Filtering:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering>

Configure URL Filtering:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/configure-url-filtering>

WildFire Analysis Reports—Close Up:

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/monitor-wildfire-activity/wildfire-analysis-reportsclose-up>

Objects > Security Profiles > WildFire Analysis:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-security-profiles-wildfire-analysis>

WildFire Administrator's Guide:

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin>

WildFire Subscription:

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-subscription>

Take a Threat Packet Capture:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/take-packet-captures/take-a-threat-packet-capture>

Enable Data Capture for Data Filtering and Manage Data Protection Password:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClvICAC>

Threat Prevention:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention>

Create Threat Exceptions:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/create-threat-exceptions>

## 2.2.9 Sample Questions

1. Which action specifies that Security profiles are relevant in a policy rule?

- a. deny
- b. drop
- c. reset
- d. allow

2. Are files quarantined while WildFire checks if they are malware or legitimate?

- a. always yes
- b. always no
- c. by default, yes, but you can change the settings
- d. by default, no, but you can change the settings

3. Which feature of the next-generation firewall allows you to block websites that are not business-appropriate?

- a. App-ID
- b. File Blocking
- c. Exploit Protection
- d. URL Filtering

4. Which credential phishing prevention action allows users to choose to submit credentials to a site anyway?

- a. alert
- b. allow
- c. block

- d. continue
5. Which user credential detection method works if multiple users share the same client IP address (e.g., because of dynamic address translation done by a device on the internal side of the firewall)?
- a. IP-to-user mapping
  - b. group mapping
  - c. domain credential filter
  - d. IP-and-port-to-user mapping
6. Which type of user credential detection must be used by a firewall administrator who wants to enable credential phishing prevention that blocks an attempt by a user to enter the organization's user ID and password?
- a. IP-to-user mapping
  - b. domain credential filter
  - c. group mapping
  - d. Citrix mapping
7. Which profile do you use for data loss prevention based on file content?
- a. Antivirus
  - b. Anti-Spyware
  - c. Vulnerability Protection
  - d. URL Filtering
  - e. File Blocking
  - f. WildFire Analysis
  - g. Data Filtering
8. Which profile do you use to monitor DNS resolution lookups for sites associated with threat activity?
- a. Antivirus
  - b. Anti-Spyware
  - c. Vulnerability Protection
  - d. URL Filtering
  - e. File Blocking
  - f. WildFire Analysis
  - g. Data Filtering
9. Which profile do you use to analyze files for zero-day malware?
- a. Antivirus
  - b. Anti-Spyware
  - c. Vulnerability Protection
  - d. URL Filtering
  - e. File Blocking
  - f. WildFire Analysis

- g. Data Filtering
10. Which profile do you use to examine browsing traffic for appropriate browsing policy enforcement?
- a. Antivirus
  - b. Anti-Spyware
  - c. Vulnerability Protection
  - d. URL Filtering
  - e. File Blocking
  - f. WildFire Analysis
  - g. Data Filtering
11. Which profile do you use to detect and block an executable file from being transferred through the firewall?
- a. Antivirus
  - b. Anti-Spyware
  - c. Vulnerability Protection
  - d. URL Filtering
  - e. File Blocking
  - f. WildFire Analysis
  - g. Data Filtering

## 2.3 Configure zone protections, packet buffer protection, and DoS protection

### *Implement Zone Protection Profiles*

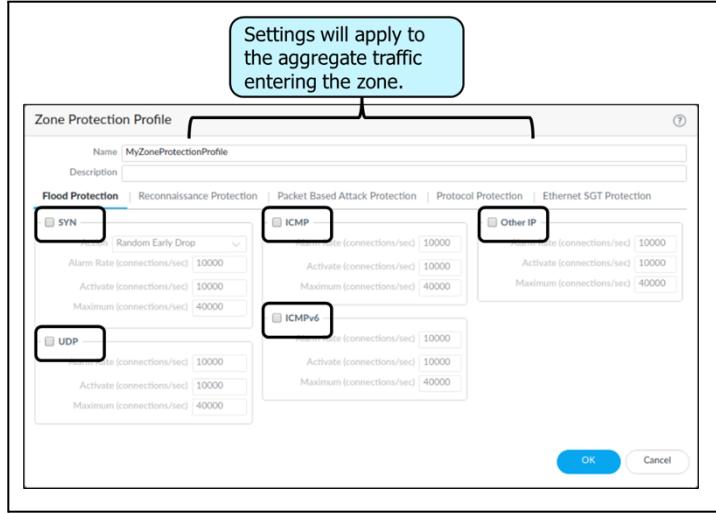
#### **Resource Exhaustion**

Port scans and floods are common causes of resource exhaustion at the interface and system level for protected devices and the firewall interfaces themselves. Although PAN-OS does have powerful protections, none of them are turned on by default. This leaves a firewall and network exposed to DoS attacks until protections are configured. Palo Alto Networks provides two protection mechanisms for resource exhaustion caused by these attacks: Zone Protection profiles and DoS Protection profiles and policies.

#### **Zone Protection Profiles**

Zone Protection profiles defend the zone at the ingress zone edge against reconnaissance port scan and host sweep attacks, IP packet-based attacks, non-IP protocol attacks, and flood attacks. These profiles limit the number of connections per second (CPS) of different packet types. Zone design itself segments networks, boosting the protection of Zone Protection profiles.

Zone Protection profiles provide a broad defense of the entire zone based on the aggregate traffic entering the zone, thus protecting against flood attacks and undesirable packet types and options. Zone Protection profiles do not control traffic between zones; they control traffic only at the ingress zone. Zone Protection profiles do not consider individual IP addresses because they apply to the aggregate traffic entering the zone (DoS Protection policy rules defend individual IP addresses in a zone). This protection occurs early in the traffic processing flow, thus minimizing firewall resource use.



## Implement DoS protections

### DoS Protection Profiles

DoS Protection profiles and DoS Protection policy rules combine to protect specific groups of critical resources and individual critical resources against session floods. Compared to Zone Protection profiles, which protect entire zones from flood attacks, DoS protection can provide granular defense for specific systems, especially critical systems like web servers and database servers that users access from the internet and often are attack targets. You should apply both types of protection; if you apply only a Zone Protection profile, then a DoS attack that targets a particular system in the zone can succeed if the total CPS does not exceed the zone's activate and maximum rates.

DoS protection is resource-intensive, so use it only for critical systems. Like Zone Protection profiles, DoS Protection profiles specify flood thresholds. DoS Protection policy rules determine the devices, users, zones, and services to which DoS Protection profiles apply.

DoS Protection profiles set the protection thresholds to provide DoS protection against flooding of new sessions to provide resource protection and to configure whether the profile applies to aggregate or classified traffic. These profiles define protection thresholds as CPS limits and maximum concurrent session limits for specified endpoints and resources. DoS Protection policy rules control where to apply DoS protection and which action to take when traffic matches the criteria defined in the rule.

Unlike a Zone Protection profile, which protects only the ingress zone, DoS Protection profiles and policy rules can protect specific resources inside a zone, as well as traffic flowing between different endpoints and areas. You also can configure aggregate or classified DoS Protection profiles and policy rules. Zone Protection profiles support only aggregate traffic.



### Differences Between DoS Protection and Zone Protection

A DoS Protection policy can provide some of the same protections as a Zone Protection profile, with a few key differences:

- A DoS policy can be classified or aggregate. Zone Protection profiles are aggregate only.
- With a classified profile, you can create a threshold that applies to only a single source or destination IP address. For example, a per-IP maximum session can be specified for all traffic matching the policy. Then, the firewall can block any single IP address that exceeds the threshold.
- With an aggregate profile, you can create a maximum session rate for all packets matching the policy. The threshold applies to a new session rate for all IPs combined. A triggered threshold would affect all traffic matching the policy.
- Zone Protection profiles allow the use of flood protection and can protect against port scanning, port sweeps, and packet-based attacks. A few examples of packet-based attacks are IP spoofing, fragments, overlapping segments, and reject tcp-non-syn.
- Zone Protection profiles may have less performance impact because they are applied pre-session and do not engage the policy engine.

### *Implement packet buffer protections*

Packet buffer protection is configured globally to protect the entire firewall while enabling packet buffer protection on each zone. Note that VM-Series firewalls do not support packet buffer protection.

To configure packet buffer protection, configure the global session thresholds in **Device > Setup > Session**. Edit the **Session Settings**. Select the **Packet Buffer Protection** checkbox, and configure the following thresholds:

- **Alert (%):** The firewall sends an alert when utilization exceeds this threshold (50 percent threshold by default) for more than 10 seconds.
- **Activate (%):** When utilization exceeds this threshold, the firewall applies RED to abusive sessions.
- **Block Hold Time (sec):** This is the amount of time a RED-mitigated session is allowed to continue before the session is discarded.
- **Block Duration (sec):** This defines how long a session remains discarded or an IP address remains blocked.

### 2.3.1 References

Configure Packet Buffer Protection:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

Understanding DoS Protection:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CLOGCA0>

DoS Protection Profiles and Policy Rules:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules>

Network > Network Profiles > Zone Protection:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection>

Zone Protection Recommendations:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVkCAK>

### 2.3.2 Sample Questions

1. For which two reasons are denial-of-service protections applied by zone? (Choose two.)

- because denial-of-service protections are applied early in processing, before much information is known about the connection but when the ingress interface already is known
- because denial-of-service protections are applied only when manually turned on to avoid quota overload (which would make denial-of-service easier)
- because denial-of-service protections can depend on only the zone and never on port numbers or IP addresses
- because denial-of-service protections on a Layer 3 interface are different from denial-of-service protections available on a Layer 2 interface and interfaces on virtual wires

2. SYN flood protection provides flood protection from which protocol?

- UDP

- b. TCP
  - c. ICMP
  - d. GRE
3. To which two protocols does port scan reconnaissance protection apply? (Choose two.)
- a. UDP
  - b. TCP
  - c. GRE
  - d. ICMP
  - e. IPX
4. In which two places do you configure flood protection? (Choose two.)
- a. DoS Protection profile
  - b. QoS Profile
  - c. Zone Protection profile
  - d. SYN Protection profile
  - e. XOFF Profile
5. Which two firewall features should be used to provide tailored denial-of-service protection to a specific address? (Choose two.)
- a. Zone Protection profiles
  - b. virtual routers
  - c. server profiles
  - d. DoS policy rules
  - e. DoS Protection profiles

## 2.4 Define the initial design/deployment configuration of a Palo Alto Network firewall

### 2.4.1 Considerations for Advanced HA Deployments

Use Panorama to manage HA firewalls. Note the following is not supported in HA deployments:

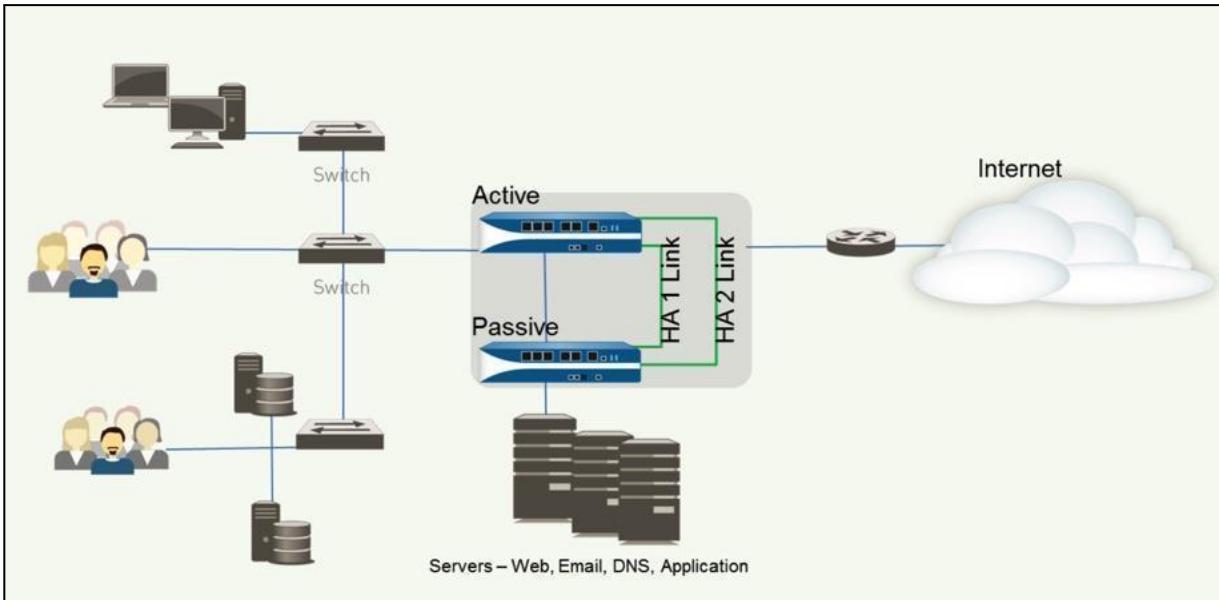
- VM-Series firewalls in Microsoft Azure do not support HA.
- VM-Series firewalls in Amazon Web Services only support active/passive failover.

### 2.4.2 Implement an HA Pair

To set up an active/passive HA pair as shown below, complete the following high-level tasks:

- Connect the HA ports.
- Enable ping on the management port.
- Set the HA mode and group ID.
- Set up the control link connection.

- Enable encryption for the control link connection.
- Set up the backup control link connection.
- Set up the data link connection (HA2) and the backup HA2 connection.
- Enable heartbeat backup.
- Set the device priority, and enable preemption.
- Modify the HA timers.
- Modify the link status of the HA ports on the passive device.
- Enable HA.



### 2.4.3 Implement Zero Touch Provisioning

To set up your firewall for Zero Touch Provisioning (ZTP), perform the following using Panorama:

- Select **Panorama > Plugins to Download**. Install the most recent version of the ZTP plugin.
- Install the Panorama device certificate.
- Register Panorama with the ZTP service.
- Create a default device group and template to connect your ZTP firewalls to Panorama.
- Select **Panorama > Zero Touch Provisioning**. Sync Panorama with the ZTP service.
- Set up the ZTP installer administrative account.
- Add ZTP firewalls to Panorama.

### 2.4.4 Configure Bootstrapping

#### *Bootstrapping*

All Palo Alto Networks firewalls can automatically configure themselves during first boot using the bootstrapping feature. This feature provisions a specifically prepared storage volume (i.e., USB for physical appliances or storage accounts for VM-Series firewalls) containing configuration data, licenses, dynamic updates, and PAN-OS updates. These are all applied automatically during the boot process.

## **VM-Series Bootstrapping**

Bootstrapping enables you to create a repeatable and streamlined process of deploying new VM-Series firewalls on your network. It allows you to create a package with the model configuration for your network and then use that package to deploy VM-Series firewalls anywhere. You can bootstrap the VM-Series firewall off an external device (such as a virtual disk, a virtual CD-ROM, or an Amazon Web Services S3 or Google Cloud bucket) to configure and license the VM-Series firewall. You can bootstrap the firewall with a basic initial configuration and licenses so that the firewall can register with Panorama and then retrieve its full configuration from Panorama. You can also bootstrap the complete configuration so that the firewall is fully configured on boot-up.

### **Bootstrap Package**

The bootstrap process is initiated only when the firewall starts up in a factory default state. After you attach the virtual disk, virtual CD-ROM, or storage bucket to the firewall, the firewall scans for a bootstrap package. If one exists, the firewall uses the settings defined in the bootstrap package. If you have included a Panorama server IP address in the file, the firewall connects with Panorama. If the firewall has internet connectivity, it contacts the licensing server to update the UUID and obtain the license keys and subscriptions. The firewall then is added as an asset in the Palo Alto Networks Support Portal. If the firewall does not have internet connectivity, it either uses the license keys that you included in the bootstrap package or connects to Panorama, which retrieves the appropriate licenses and deploys them to the managed firewalls.

The bootstrap package that you create must include the /config, /license, /software, and /content folders, even if empty, as follows:

- **/config folder:** This folder contains the configuration files. The folder can hold two files: init-cfg.txt and bootstrap.xml.

**Note:** If you intend to pre-register VM-Series firewalls with Panorama with bootstrapping, you must generate a VM authorization key on Panorama and include the generated key in the init-cfg file.

- **/license folder:** This folder contains the license keys or authorization codes for the licenses and subscriptions that you intend to activate on the firewalls. If the firewall does not have internet connectivity, you must either manually obtain the license keys from the Palo Alto Networks Support Portal or use the Licensing API to obtain the keys and then save each key in this folder.

**Note:** You must include an authorization code bundle instead of individual authorization codes so that the firewall or orchestration service can simultaneously fetch all license keys that are associated with a firewall. If you use individual authorization codes instead of a bundle, the firewall will retrieve only the license key for the first authorization code included in the file.

- **/software folder:** This folder contains the software images that are required to upgrade a newly provisioned VM-Series firewall to the desired PAN-OS version for your network. You must include all intermediate software versions between the Open Virtualization Format version and the final PAN-OS software version to which you want to upgrade the VM-Series firewall.
- **/content folder:** This folder contains the Applications and Threats updates and WildFire updates for the valid subscriptions on the VM-Series firewall. You must include the minimum content versions that are

required for the desired PAN-OS version. Without the minimum required content version associated with the PAN-OS version, the VM-Series firewall cannot complete the software upgrade.

- **/plugins folder:** This optional folder contains a single VM-Series plugin image.

## 2.4.5 References

Product Summary Specsheets:

<https://www.paloaltonetworks.com/resources/datasheets/product-summary-specsheet>

Getting Started:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/getting-started>

Internet Gateway Best Practice Security Policy:

<https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices>

Best Practices:

<https://docs.paloaltonetworks.com/best-practices>

Dynamic Content Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/dynamic-content-updates>

Bootstrap the VM-Series Firewall:

<https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm-series-firewall>

## 2.4.6 Sample Questions

1. Which configuration is performed first on a firewall with factory default settings, according to Palo Alto Networks best practices?

- Add licenses.
- Update PAN-OS software.
- Configure the management network port.
- Update dynamic update files.

2. You finished configuring the firewall's basic connectivity in the lab and are ready to put it in the data center. What must you do before you power down the firewall?

- Save the changes.
- Commit the changes.
- Create a restore thumb drive in case the configuration is deleted.
- Verify that the configuration is correct. You do not need to do anything else if it is correct; the configuration is updated automatically.

3. The firewall's MGT port can be configured as which type of interface?

- Layer 2

- b. Layer 3
  - c. virtual wire
  - d. serial
4. When will a firewall check for the presence of bootstrap volume?
- a. each time it cold boots
  - b. each time it boots from a factory default state
  - c. when a firewall is started in maintenance mode
  - d. each time it warm boots
5. Where in the bootstrap volume directories is a required dynamic update file?
- a. /config folder
  - b. /license folder
  - c. /software folder
  - d. /content folder
6. Can a firewall's PAN-OS software be updated by the bootstrap process?
- a. Yes, it can be updated by including a copy of the desired PAN-OS software in the /software folder of the bootstrap volume.
  - b. Yes, it can be updated by including a copy of the desired PAN-OS software in the /content folder of the bootstrap volume.
  - c. No, it must be updated by an administrator after the firewall starts.
  - d. No, the firewall must be licensed before the software can be updated.

## 2.5 Configure authorization, authentication, and device access

### 2.5.1 Role-based access control for authorization

#### *Administrative Accounts and Roles*

Administrators can configure, manage, and monitor Palo Alto Networks firewalls and Panorama using the web interface, command line interface (CLI), and XML API management interface. You can customize role-based administrative access to the management interfaces to delegate specific tasks or permissions to certain administrators.

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

You configure administrator accounts based on the security requirements of your organization, any existing authentication services that your network uses, and the required administrative roles. A role defines the type of system access that is available to an administrator. You can define and restrict access as broadly or granularly as required, depending on the security requirements of your organization. For example, you might

decide that a data center administrator can have access to all device and networking configurations, but a security administrator can control only Security policy definitions, while other key individuals can have limited CLI or XML API access. The role types are as follows:

**Dynamic roles:** These are built-in roles that provide access to Panorama and managed firewalls. After new features are added, the firewall and Panorama automatically update 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 read-write access to Panorama
Superuser (read-only)	Read-only access to Panorama
Panorama administrator	Full access to Panorama except for the following actions: <ul style="list-style-type: none"><li>• Create, modify, or delete Panorama or firewall administrators and roles.</li><li>• Export, validate, revert, save, load, or import a configuration in the <b>Device &gt; Setup &gt; Operations</b> page.</li><li>• Configure <b>Scheduled Config Export</b> functionality in the <b>Panorama</b> tab.</li></ul>

**Admin role profiles:** To provide more granular access control over the functional areas of the web interface, CLI, and XML API, you can create custom roles. After new features are added to the product, you must update the roles with corresponding access privileges; the firewall and Panorama do not automatically add new features to custom role definitions.

## 2.5.2 Different methods used to authenticate

### *Authentication*

Authentication is a method for protecting services and applications by verifying the identities of users so that only legitimate users have access. Several firewall and Panorama features require authentication.

Administrators authenticate to access the web interface, CLI, or XML API of the firewall and Panorama. End users authenticate through Captive Portal or GlobalProtect to access various services and applications through the firewall. You can choose from several authentication services to protect your network and to accommodate your existing security infrastructure while ensuring a smooth user experience.

If you have a public key infrastructure (PKI), you can deploy certificates to enable authentication without requiring users to manually respond to login challenges. Alternatively, or in addition to certificates, you can implement interactive authentication, which requires users to authenticate using one or more methods.

Supported authentication types include the following:

- MFA

- SAML
- SSO
- Kerberos
- TACACS+
- RADIUS
- LDAP
- Local

### ***Protecting Service Access Through the Firewall***

*Authentication policy* enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a webpage), the firewall evaluates the Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, voice, SMS, push, or OTP authentication. For the first factor, users authenticate through a Captive Portal web form. For any additional factors, users authenticate through a MFA login page.

After the user authenticates for all factors, the firewall evaluates Security policy to determine whether to allow access to the service or application.

To reduce the frequency of authentication challenges that interrupt the user workflow, you can specify a timeout period during which a user authenticates only for initial access to services and applications, not for subsequent access. Authentication policy integrates with Captive Portal to record the timestamps used to evaluate the timeout and to enable user-based policies and reports.

Based on user information that the firewall collects during authentication, User-ID creates a new IP address-to-username mapping or updates the existing mapping for that user (if the mapping information has changed). The firewall generates User-ID logs to record the additions and updates. The firewall also generates an Authentication log for each request that matches an authentication rule. If you favor centralized monitoring, you can configure reports based on User-ID or Authentication logs and forward the logs to Panorama or external services as you would for any other log types.

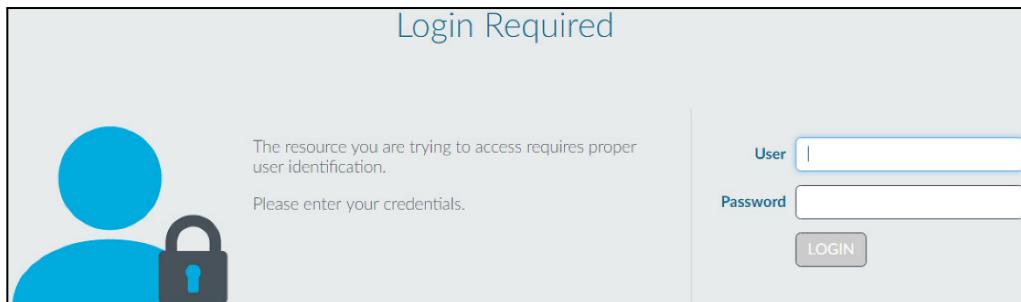
### ***Configuring Authentication Policy***

Perform the following steps to configure Authentication policy for end users who access services through Captive Portal. Before starting, ensure that your Security policy allows users to access the services and URL categories that require authentication.

- Configure Captive Portal. If you use MFA services to authenticate users, you must set the **Mode** to **Redirect**.
- Configure the firewall to use one of the following services to authenticate users:
  - **External Authentication Services:** Configure a Server Profile to define how the firewall connects to the service.

- **Local database authentication:** Add each user account to the local user database on the firewall.
  - **Kerberos SSO:** Create a Kerberos keytab for the firewall. You can configure the firewall to use Kerberos SSO as the primary authentication service and, if SSO failures occur, to fall back to an external service or local database authentication.
- Configure an Authentication Profile, an optional Authentication Sequence for each set of users, and Authentication policy rules that require the same authentication services and settings.
- Select the **Type** of authentication service and related settings:
  - **External service:** Select the **Type** of external server and select the **Server Profile** you created for it.
  - **Local database authentication:** Set the **Type** to **Local Database**. In the **Advanced settings**, **Add** the Captive Portal users and user groups you created.
  - **Kerberos SSO:** Specify the **Kerberos Realm** and **Import the Kerberos Keytab**.
- Configure an Authentication Enforcement object:
  - The object associates each Authentication Profile with a Captive Portal method. The method determines whether the first authentication challenge (factor) is transparent or requires a user response.
  - Select **Objects > Authentication**, and **Add** an object.
  - Enter a **Name** to identify the object.
  - Select an **Authentication Method** for the authentication service type you specified in the Authentication Profile:
    - **browser-challenge:** Select this method if you want the client browser to transparently respond to the first authentication factor instead of having the user enter login credentials. For this method, you must have configured Kerberos SSO in the Authentication Profile or NTLM authentication in the Captive Portal settings. If the browser challenge fails, the firewall falls back to the web-form method.
    - **web-form:** Select this method if you want the firewall to display a Captive Portal web form for users to enter login credentials.
  - Select the Authentication Profile that you configured.
  - Enter the **Message** that the Captive Portal web form will display to tell users how to authenticate for the first authentication factor.
  - Click **OK** to save the object.
- Configure an Authentication policy rule:

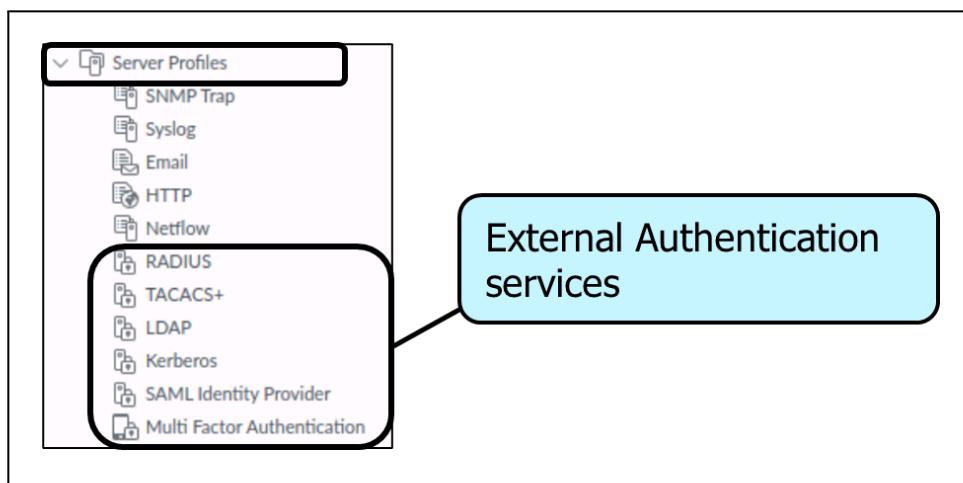
- Create a rule for each set of users, services, and URL categories that requires the same authentication services and settings.
- Select **Policies > Authentication**, and **Add** a rule.
- Enter a **Name** to identify the rule.
- Select **Source**, and **Add** specific zones and IP addresses, or select **Any** zones or IP addresses.
- Select **User**, and select or **Add** the source users and user groups to which the rule applies (default is **any**).
- Select or **Add** the **Host Information Profiles** to which the rule applies (default is **any**).
- Select **Destination**, and **Add** specific zones and IP addresses, or select any zones or IP addresses.
- Select **Service/URL Category**, and select or **Add** the services and service groups for which the rule controls access (default is **service-http**).
- Select or **Add** the **URL Categories** for which the rule controls access (default is **any**). For example, you can create a custom URL category that specifies your most sensitive internal sites.
- Select **Actions**, and select the Authentication Enforcement object you created.
- Specify the **Timeout** period in minutes (default is **60**) during which the firewall prompts the user to authenticate only once for repeated access to services and applications.
- Click **OK** to save the rule.
- (MFA only) Customize the MFA login page:
  - The firewall displays this page so that users can authenticate for any additional MFA factors.
- Verify that the firewall enforces your Authentication policy:
  - Log in to your network as one of the source users specified in an Authentication policy rule.
  - Request a service or URL category that matches one specified in the rule. The firewall displays the Captive Portal web form for the first authentication factor. Here is an example:



- End the session for the service or URL that you just accessed.
  - Start a new session for the same service or application. Be sure to perform this step within the timeout period that you configured in the Authentication rule.
  - The firewall allows access without re-authenticating.
  - Wait until the timeout period expires. Request the same service or application.
  - The firewall prompts you to re-authenticate.
- (Optional) Redistribute user mappings and authentication timestamps to other firewalls that enforce Authentication policy to ensure that they all apply timeouts consistently for all users.

### 2.5.3 The Authentication Sequence

When user or administrative access is configured, one or more authentication methods must be specified. A user or administrator definition typically requires an Authentication Profile that specifies the desired authentication method. When more than one method is desired, you can instead use an Authentication Sequence, which is a list of Authentication Profiles. The first profile will be accessed. If it is not available, the next option will be tried. An Authentication Profile specifies a single Server Profile. A Server Profile contains specific configuration and access information that is necessary to reach the external authentication service.



### 2.5.4 The device access method

#### *Panorama Access Domains*

Panorama access domains control the access that device group and template administrators have to specific device groups (to manage policies and objects), to templates (to manage network and device settings), and to the web interface of managed firewalls (through context switching). You can define up to 4,000 access domains, and you can manage them locally or by using RADIUS Vendor-Specific Attributes (VSAs), TACACS+ VSAs, or SAML attributes.

## 2.5.5 References

Configure an Authentication Profile and Sequence:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-an-authentication-profile-and-sequence>

Panorama > Access Domains:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-access-domains>

## 2.5.6 Sample Questions

1. Which three configuration pieces must be addressed to configure multi-factor authentication for users accessing services through the firewall? (Choose three.)

- a. GlobalProtect Portal
- b. Captive Portal
- c. Authentication Enforcement Profile
- d. Authentication Profile
- e. response pages

2. Which firewall configuration component is used to configure access to an external authentication service?

- a. Local User Database
- b. Server Profiles
- c. VM information source
- d. admin roles
- e. Authentication policy rules

3. Which two firewall functions are reserved only for administrators assigned the superuser dynamic role? (Choose two.)

- a. managing certificates
- b. managing firewall admin accounts
- c. editing the management interface settings
- d. creating virtual systems within a firewall
- e. accessing the configuration mode of the command line interface

## 2.6 Configure and manage certificates

### 2.6.1 Certificate Usage

#### *Certificate Background*

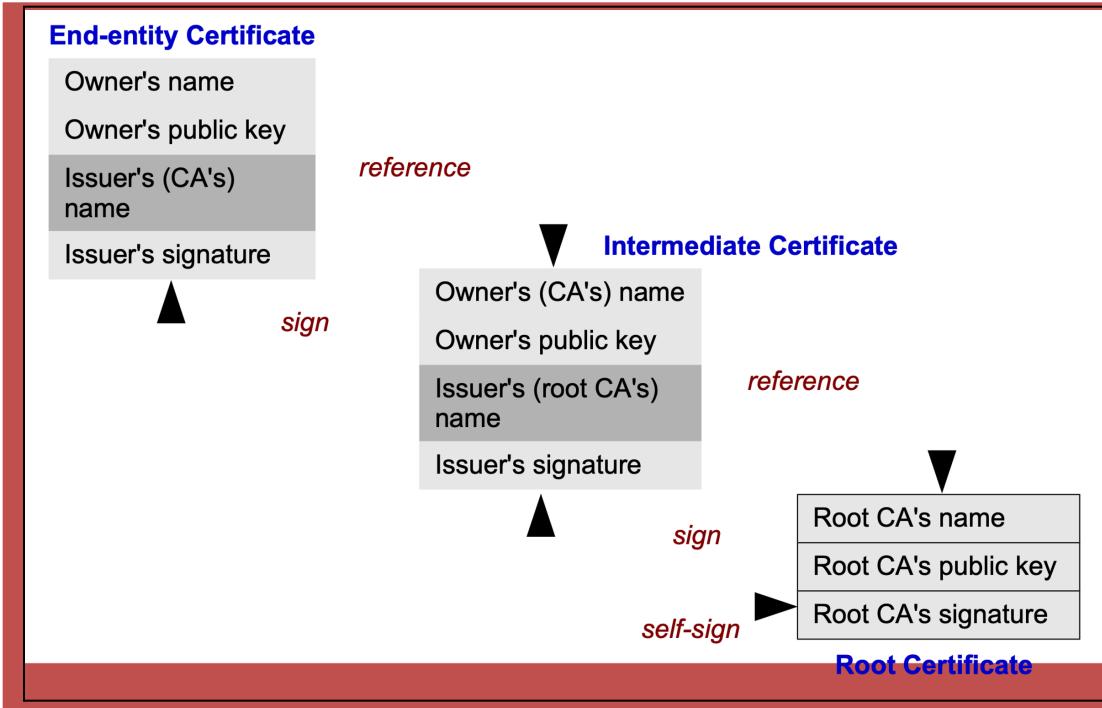
In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity

that has verified the certificate's contents (called the issuer). If the signature is valid and the software examining the certificate trusts the issuer, then the software can use that key to communicate securely with the certificate's subject. In email encryption, code signing, and e-signature systems, a certificate's subject typically is a person or organization. However, in Transport Layer Security (TLS), a certificate's subject typically is a computer or other device, though TLS certificates may identify organizations or individuals in addition to their core role in identifying devices. TLS, sometimes called by its older name SSL, is notable for being a part of HTTPS, a protocol for securely browsing the web.

In a typical PKI scheme, the certificate issuer is a CA, usually a company that charges customers to issue certificates for them. CAs also can be created and managed by individuals and organizations requiring certificates for internal use.

A CA is responsible for signing certificates. These certificates act as an introduction between two parties, which means that a CA acts as a trusted third party. A CA processes requests from people or organizations requesting certificates (called subscribers), verifies the information, and potentially signs an end-entity certificate based on that information. To perform this role effectively, a CA needs to have one or more broadly trusted root certificates or intermediate certificates and the corresponding private keys. CAs may achieve this broad trust by having their root certificates included in popular software or by obtaining a cross-signature from another CA delegating trust.

A receiving entity is responsible for validating the information contained in a certificate presented to it. Among the potential verification tests is a validation that the certificate was issued by the issuing CA information contained in the certificate. This verification requires the CA's signing key contained in its Root Certificate used to sign all issued certificates. This certificate must be locally available to the receiving entity to run the validation test. These CA Root Certificates often are kept in locally stored certificate caches in the hosting operating system or a browser- or program-managed certificate cache. The firewall also contains a CA Root Certificate cache.



CAs also are responsible for maintaining up-to-date revocation information about certificates they have issued that indicates whether certificates still are valid. They provide this information through Online Certificate Status Protocol (OCSP) or certificate revocation lists.

## 2.6.2 Certificate Profiles

Certificate profiles define user and device authentication for Authentication Portal, MFA, GlobalProtect, site-to-site IPsec VPN, external dynamic list validation, Dynamic DNS, User-ID agent and Terminal Services agent access, and web interface access to Palo Alto Networks firewalls or Panorama. The profiles specify which certificates to use, how to verify certificate revocation status, and how that status limits access. Configure a certificate profile for each application.

## 2.6.3 Certificate Chains

Not all websites send their complete certificate chain, even though the RFC 5246 TLSv1.2 standard requires authenticated servers to provide a valid certificate chain leading to an acceptable CA. When you enable decryption and apply a Forward Proxy Decryption Profile that enables block sessions with untrusted issuers in the decryption policy, if an intermediate certificate is missing from the certificate list the website's server presents to the firewall, the firewall can't construct the certificate chain to the top (root) certificate. In these cases, the firewall presents its forward untrust certificate to the client because the firewall cannot construct the chain to the root certificate and trust cannot be established without the missing intermediate certificate.

If a website you need to communicate with for business purposes has one or more missing intermediate certificates and the decryption policy blocks sessions with untrusted issuers, then you can find and download the missing intermediate certificate and install it on the firewall as a trusted root CA so that the firewall trusts

the site's server. (The alternative is to contact the website owner and ask them to configure their server so that it sends the intermediate certificate during the handshake.)

## 2.6.4 References

Certificate profiles:

[Configure a Certificate Profile \(paloaltonetworks.com\)](https://paloaltonetworks.com/configure-a-certificate-profile)

Certificate status:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs/repair-incomplete-certificate-chains>

Keys and Certificates for Decryption Policies:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies>

Certificate Management:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management>

How to Install a Chained Certificate Signed by a Public CA:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClkoCAC>

Resource List: SSL Certificates Configuring and Troubleshooting:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5YCAS>

## 2.6.5 Sample Questions

1. Which condition could be a symptom of a certificate chain-of-trust issue?

- a. The firewall no longer decrypts HTTPS traffic.
- b. The firewall no longer decrypts HTTPS traffic from a specific site.
- c. The firewall still decrypts HTTPS traffic from all sites, but it re-encrypts it using the forward untrust certificate instead of the forward trust certificate.
- d. The firewall still decrypts HTTPS traffic from a specific site, but it re-encrypts it using the forward untrust certificate instead of the forward trust certificate.

2. Which field is mandatory in the subject field of a certificate?

- a. Organization
- b. Organizational Unit
- c. Common Name
- d. Locale

3. Which field in a certificate must include a value known to the firewall for the certificate to be considered valid by the firewall?

- a. Issuer

- b. Subject
- c. Key
- d. Object

4. A Palo Alto Networks firewall can obtain a certificate for its internal use through which three methods?  
(Choose three.)

- a. import a certificate file generated by an external CA
- b. reference an externally stored certificate by a URL configured in an SSL/TLS Service Profile
- c. generate a certificate directly by manually entering certificate data
- d. obtain a certificate from an Simple certificate enrollment protocol (SCEP) server using an SCEP Profile
- e. import a certificate from an external CA by using an Authentication Profile

5. Which two resources must be available to successfully run certificate validation tests on a certificate received from an external source? (Choose two.)

- a. root certificate of the issuing CA
- b. public key for the received certificate
- c. OCSP connection address
- d. existing Certificate Profile that matches the received certificate's CA identity

6. How are updates made to the cache of root certificates that is used for certificate verification purposes and maintained by Palo Alto Networks?

- a. The administrator reviews certificate status and replaces them manually.
- b. The firewall automatically updates the certificates as it updates the associated certificate revocation list.
- c. The administrator installs PAN-OS software and dynamic content updates.
- d. The firewall automatically installs new certificates using OCSP.

7. How does a firewall administrator who creates a certificate on the firewall mark it for use in an SSL Forward Proxy configuration?

- a. adds a certificate tag in the decryption policy rule
- b. configures a trust certificate in the Decryption Profile
- c. sets the forward trust certificate property of the certificate itself
- d. maps the certificate to the URL in the SSL/TLS Service Profile

8. Administrators within the enterprise want to replace the default certificate that is used by the firewall to secure the management web interface traffic with a certificate that is generated by their existing CA. Which certificate property must be set for their new certificate to function?

- a. The certificate CN must be set to a domain name that resolves to any traffic port address of the firewall.
- b. The certificate must be signed by the firewall root certificate.
- c. The certificate must have the forward trust certificate property set.
- d. The CN must be set to the management port of the firewall.

9. A Palo Alto Networks firewall can forward DHCP packets to servers connected to which two kinds of networks? (Choose two.)

- a. virtual wire
- b. Layer 2
- c. Layer 3
- d. aggregate

10. How does a Palo Alto Networks firewall that is configured to forward DHCP packets to multiple server destinations choose which reply to forward to the sender?

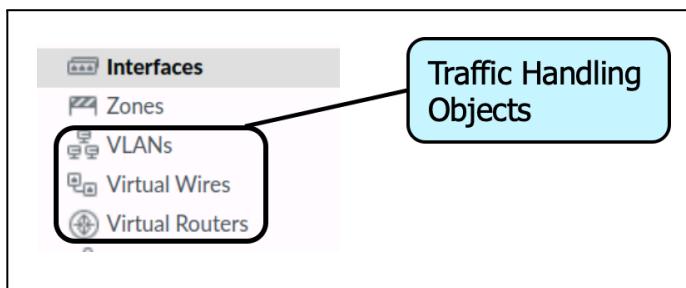
- a. The first server listed in the server priority DHCP configuration is forwarded until it fails to respond, then the next one is chosen.
- b. A request is sent to all servers on the list, and the first responder is forwarded.
- c. All DHCP server responses are forwarded, and the receiving client chooses which response to accept.
- d. The server that is the fewest network hops from the requesting client is chosen. When more than one server has the same hop count, all packets from the servers are forwarded to the client.

## 2.7 Configure routing

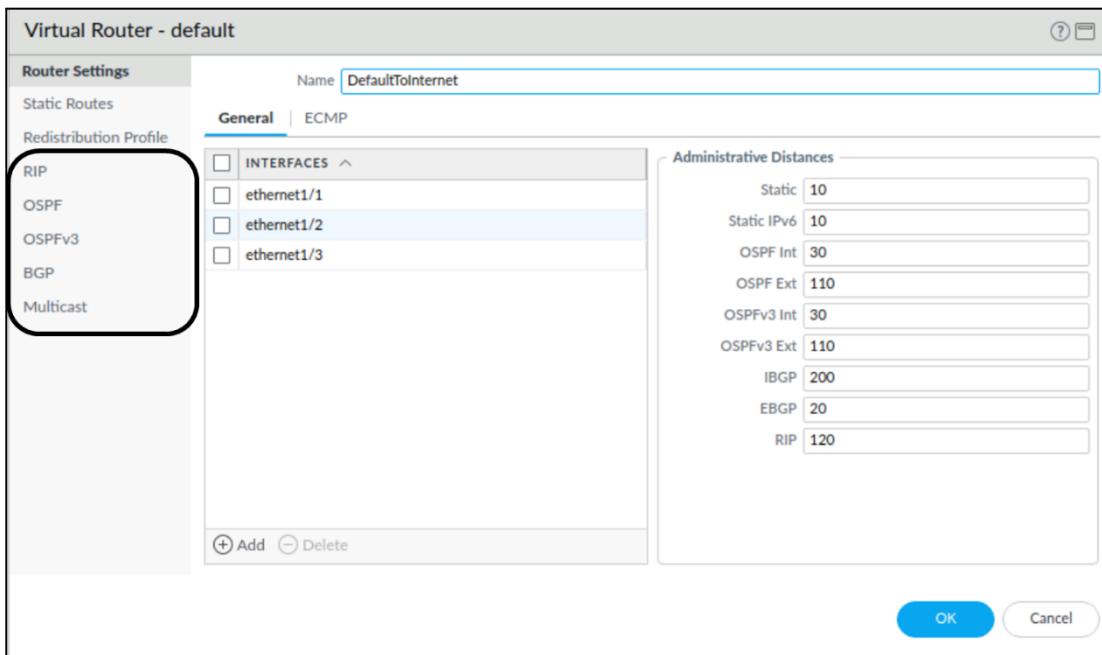
### 2.7.1 Dynamic routing

#### *Traffic Forwarding*

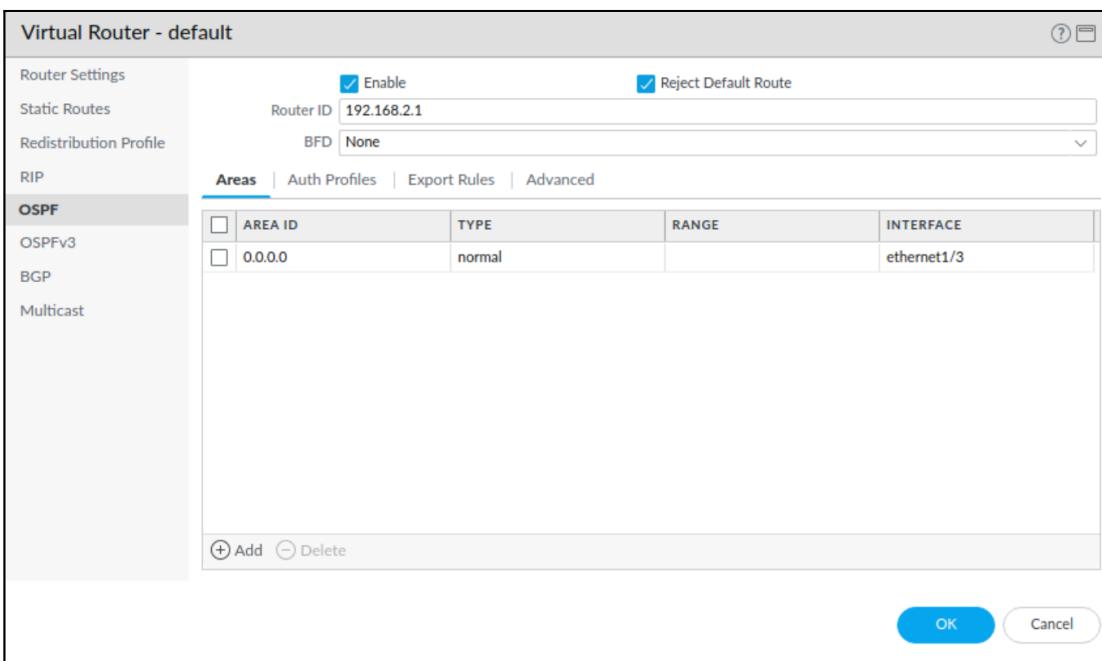
All traffic that arrives at the firewall will be delivered either to an internal firewall process (destination traffic) or be passed through a traffic interface (transit traffic). All transit traffic must be handed off to the egress interface by a traffic handling object that matches the interface type. Examples of these objects are VLAN objects (VLANs) for Layer 2 traffic, virtual routers for Layer 3 traffic, and virtual wires for virtual wire interfaces.



Simultaneous implementations of multiple traffic handler types in multiple quantities are possible. Each object contains configuration capabilities that are appropriate to its protocol-handling needs. Legacy virtual routers can implement various dynamic routing support, if desired. The Advanced Route Engine of virtual routers supports the Border Gateway Protocol (BGP) dynamic routing protocol and static routes.



Each Layer 3 dynamic routing protocol includes appropriate specific configuration options. Here is an example of the Open Shortest Path First (OSPF) protocol in the Legacy Route Engine:

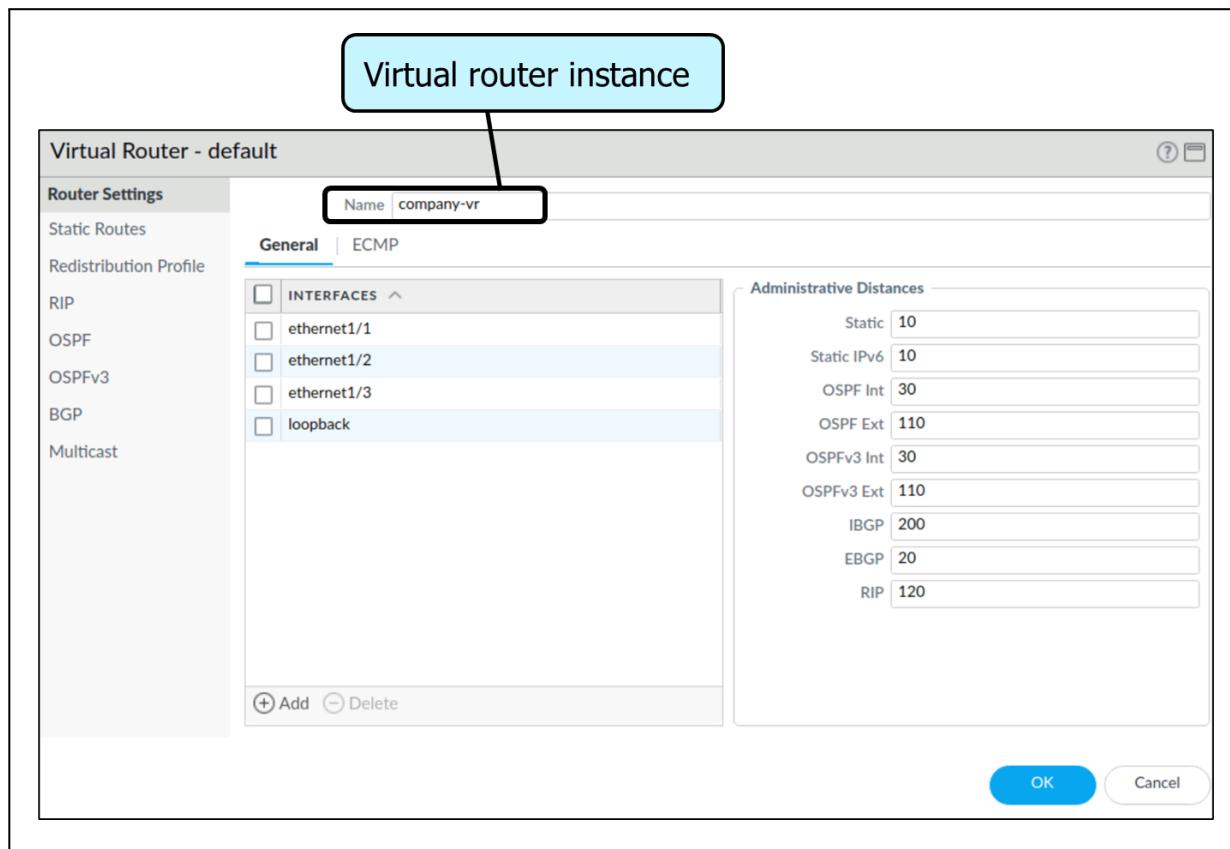


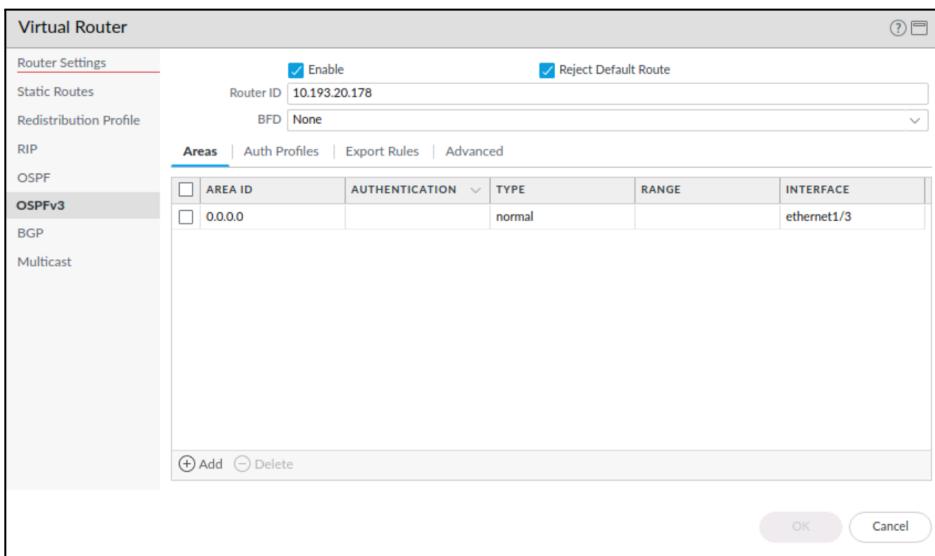
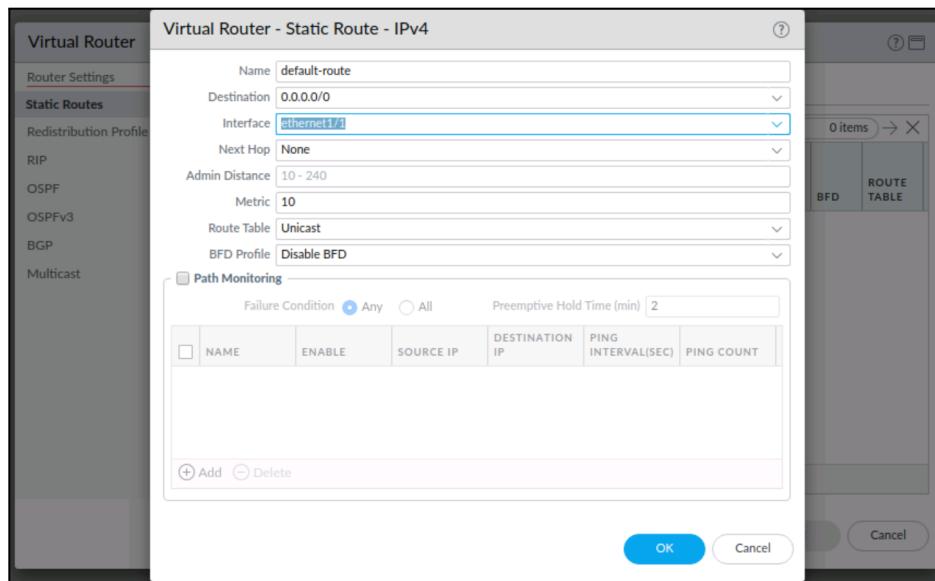
IPsec tunnels are considered Layer 3 traffic segments for implementation purposes and are handled by virtual routers, as are any other network segments. Forwarding decisions are made by destination address, not by VPN policy.

## Routing Configuration

PAN-OS supports static routes, BGP, OSPF, Routing Information Protocol (RIP), and multicast routing configured in two routing engines, only one of which can be active at a time. The Legacy Routing Engine is the continuation of the virtual routing features in previous PAN-OS versions. It supports multiple dynamic routing protocols and can support more than one virtual routing instance, with the limit being determined by the firewall model. The Advanced Routing Engine supports BGP and static routes only and can support a single virtual router instance regardless of firewall model. There are limitations for the number of entries in the forwarding tables (i.e., forwarding information bases [FIBs]) and routing tables (i.e., routing information bases [RIBs]) in either routing engine.

The virtual router configuration is meant to match the existing routing infrastructure. In addition to protocol configuration, Redistribution Profiles can support protocol interoperability.





<input checked="" type="checkbox"/> company-vr	ethernet1/1	Static Routes: 1				More Runtime Stats
	ethernet1/2					
	ethernet1/3					
	loopback					

## Virtual Routers

Because Layer 3 interfaces and their virtual routers are the most widely used deployment options, a review of virtual routers follows.

The firewall has two routing engines, one of which can be enabled at a time. The Legacy Route Engine is a continuation of the routing engine from previous PAN-OS versions and is still the default. The Legacy Route

Engine supports BGP, OSPF, OSPFv3, and RIP dynamic routing protocols, plus static routes, route monitoring, and Redistribution Profiles. Several virtual router instances can be created and managed simultaneously. The Advanced Route Engine is also available in some firewall models and supports the BGP dynamic routing protocol only with static routes. The Advanced Route Engine allows for only a single virtual router instance. A firewall must be rebooted when the type of route engine is changed. Firewalls that use the Advanced Route Engine are appropriate for large data centers, enterprises, ISPs, and cloud services.

A virtual router is a function of the firewall that participates in Layer 3 routing. The firewall uses virtual routers to obtain routes to other subnets after you manually define static routes or through participation in one or more Layer 3 routing protocols (dynamic routes). The routes that the firewall obtains through these methods populate the IP RIB on the firewall. When a packet is destined for a different subnet than the one it arrived on, the virtual router obtains the best route from the RIB, places it in the FIB, and forwards the packet to the next hop router that is defined in the FIB. The firewall uses Ethernet switching to reach other devices on the same IP subnet. (An exception to adding only a single optimal route to the FIB occurs if you are using Equal-Cost Multi-Path [ECMP] routing, in which case all equal-cost routes go in the FIB.)

The Ethernet, VLAN, and tunnel interfaces that are defined on the firewall receive and forward Layer 3 packets. The destination zone is derived from the outgoing interface based on the forwarding criteria, and the firewall consults policy rules to identify the Security policies that it applies to each packet. 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 Layer 3 interfaces on a virtual router to participate with dynamic routing protocols (i.e., BGP, OSPFv2, OSPFv3, or RIP) and add static routes with the routing protocol configured in the routing engine. You can also create multiple virtual routers in the Legacy Route Engine; each router maintains a separate set of routes that are not shared between the other virtual routers, which enables you to configure different routing behaviors for different interfaces.

Each Layer 3 Ethernet, loopback, VLAN, and tunnel interface defined on the firewall must be associated with a virtual router. Although each interface can belong to only one virtual router, you can configure multiple routing protocols and static routes for a virtual router.

A firewall can have more than one router instance when it is using the Legacy Route Engine, with each model supporting a different maximum. An interface can be attached to one virtual router at a time. Virtual routers can route directly to each other within the firewall.

### ***Administrative Distance***

Within the virtual router configuration, set administrative distances for types of routes as required for your network. A virtual router that has two or more different routes to the same destination uses administrative distance to choose the best path from different routing protocols and static routes by preferring a lower distance.

### ***ECMP Routing***

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, the virtual router would select only a single route to a destination from the routing table and add it to its forwarding table; it will not use any of the other routes unless there is an outage in the chosen route.

Enablement of ECMP functionality on a virtual router allows the firewall to have up to four equal-cost paths to a destination in its forwarding table, which allows the firewall to perform these actions:

- 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 wait for the routing protocol or RIB table to elect an alternative path/route, which helps reduce downtime

### **2.7.2 Redistribution Profiles**

#### ***Route Redistribution***

Route redistribution on the firewall is the process of making routes that the firewall learned from one routing protocol (or a static or connected route) available to a different routing protocol, thereby increasing the number of reachable networks. Without route redistribution, a router or virtual router advertises and shares routes only with other routers that run the same routing protocol. You can redistribute IPv4 or IPv6 BGP, connected, or static routes into the OSPF RIB and redistribute OSPFv3, connected, or static routes into the BGP RIB.

Route distribution means, for example, that you can make specific networks that were once available only by manual static route configuration on specific routers available to BGP autonomous systems or OSPF areas. You can also advertise locally connected routes — such as routes to a private lab network — into BGP autonomous systems or OSPF areas.

You might want to give users on your internal OSPFv3 network access to BGP so they can access devices on the internet. In this case, you would redistribute BGP routes into the OSPFv3 RIB.

Conversely, you might want to give your external users access to some parts of your internal network, so you can make internal OSPFv3 networks available through BGP by redistributing OSPFv3 routes into the BGP RIB.

### **2.7.3 Static routes**

When you configure static routes, they are normally used with dynamic routing protocols. Typically, you configure a static route for a location that a dynamic routing protocol can't reach.

## 2.7.4 Route monitoring

When you configure path monitoring for a static route, the firewall uses path monitoring to detect when the path to the monitored destination has gone down. The firewall then reroutes traffic using alternative routes.

## 2.7.5 Policy-based forwarding

The firewall in most cases uses the destination IP address in a packet to determine the egress 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. You can specify the egress interface based set parameters (such as destination IP address) or type of traffic.

When you create a PBF rule, you must specify:

- A name for the rule
- A source zone or interface
- An egress interface

You can specify the source and destination addresses using an IP address, an address object, or a FQDN. Note that application-specific rules are not recommended for use with PBF because PBF rules may be applied before the firewall has determined the application.

## 2.7.6 Virtual routers versus logical routers

### *Virtual Routers*

Because Layer 3 interfaces and their associated virtual routers are the most widely used deployment options, a review of virtual routers follows.

The firewall has two routing engines, one of which can be enabled at a time. The Legacy Route Engine is a continuation of the routing engine from previous PAN-OS versions and is still the default. The Legacy Route Engine supports BGP, OSPF, OSPFv3, and RIP dynamic routing protocols, plus static routes, route monitoring, and Redistribution Profiles. Several virtual router instances can be created and managed simultaneously. The Advanced Route Engine is also available in some firewall models and supports the BGP dynamic routing protocol only with static routes. The Advanced Route Engine allows for only a single virtual router instance. A firewall must be rebooted when the type of route engine is changed. Firewalls that use the Advanced Route Engine are appropriate for large data centers, enterprises, ISPs, and cloud services.

A virtual router is a function of the firewall that participates in Layer 3 routing. The firewall uses virtual routers to obtain routes to other subnets after you manually define static routes or through participation in one or more Layer 3 routing protocols (dynamic routes). The routes that the firewall obtains through these methods populate the IP RIB on the firewall. When a packet is destined for a different subnet than the one it arrived on, the virtual router obtains the best route from the RIB, places it in the FIB, and forwards the packet to the next hop router that is defined in the FIB. The firewall uses Ethernet switching to reach other devices

on the same IP subnet. (An exception to adding only a single optimal route to the FIB occurs if you are using ECMP, in which case all equal-cost routes go in the FIB.)

The Ethernet, VLAN, and tunnel interfaces that are defined on the firewall receive and forward Layer 3 packets. The destination zone is derived from the outgoing interface based on the forwarding criteria, and the firewall consults policy rules to identify the Security policies that it applies to each packet. 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 Layer 3 interfaces on a virtual router to participate with dynamic routing protocols (i.e., BGP, OSPFv2, OSPFv3, or RIP) and add static routes with the routing protocol configured in the routing engine. You can also create multiple virtual routers in the Legacy Route Engine; each router maintains a separate set of routes that are not shared between the other virtual routers, which enables you to configure different routing behaviors for different interfaces.

Each Layer 3 Ethernet, loopback, VLAN, and tunnel interface defined on the firewall must be associated with a virtual router. Although each interface can belong to only one virtual router, you can configure multiple routing protocols and static routes for a virtual router.

A firewall can have more than one router instance when it is using the Legacy Route Engine, with each model supporting a different maximum. An interface can be attached to one virtual router at a time. Virtual routers can route directly to each other within the firewall.

### ***Logical Routers***

The firewall uses logical routers to obtain Layer 3 routes to other subnets when you manually define static routes or through participation in one or more Layer 3 routing protocols (dynamic routes). The routes that the firewall obtains through these methods populate the IP RIB on the firewall. When a packet is destined for a different subnet than the one it arrived on, the logical router obtains the best route from the RIB, places it in the FIB, and forwards the packet to the next hop router defined in the FIB. The firewall uses Ethernet switching to reach other devices on the same IP subnet. (An exception to one best route going in the FIB occurs if you are using ECMP, in which case all equal-cost routes go in the FIB.)

The Ethernet, VLAN, and tunnel interfaces defined on the firewall receive and forward Layer 3 packets. The destination zone is derived from the outgoing interface based on the forwarding criteria, and the firewall consults policy rules to identify the Security policies that it applies to each packet. In addition to routing to other network devices, logical routers can route to other logical routers within the same firewall if a next hop is specified to point to another logical router.

You can configure Layer 3 interfaces to participate with dynamic routing protocols (BGP, OSPF, OSPFv3, or RIP) as well as add static routes. You can also create multiple logical routers, each maintaining a separate set of routes that aren't shared between logical routers, enabling you to configure different routing behaviors for different interfaces.

You can configure dynamic routing from one logical router to another by configuring a loopback interface in each logical router, creating a static route between the two loopback interfaces, and then configuring a dynamic routing protocol to peer between these two interfaces.

Each Layer 3 Ethernet, loopback, VLAN, and tunnel interface defined on the firewall must be associated with a logical router. While each interface can belong to only one logical router, you can configure multiple routing protocols and static routes for a logical router. Regardless of the static routes and dynamic routing protocols you configure for a logical router, one general configuration is required.

### 2.7.7 References

Configure a Static Route:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/static-routes/configure-a-static-route>

Static Route Removal Based on Path Monitoring:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/static-routes/static-route-removal-based-on-path-monitoring>

Service Versus Applications in PBF:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/policy-based-forwarding/pbf/service-versus-applications-in-pbf>

How to Configure PBF in Multi Vsyst Configuration:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000000ClKsCAK>

Network > Virtual Routers:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-virtual-router>

ECMP:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/ecmp>

### 2.7.8 Sample Questions

1. How do two legacy virtual routers on a firewall forward traffic to each other?
  - a. Virtual router traffic is sent to an external router that routes it back to the second virtual router.
  - b. Both virtual routers pass traffic via a dedicated VLAN routing interface.
  - c. Both virtual routers pass traffic via a configurable shared routing interface.
  - d. Virtual routers forward traffic directly to each other within the firewall using routing table lookups.
2. A firewall's virtual router can connect to which three types of interfaces? (Choose three.)
  - a. virtual wire
  - b. management

- c. Layer 3 traffic
  - d. HA1
  - e. HA2
  - f. loopback
  - g. tunnel
3. Without having to make network address configuration changes, you would use which type of network interface to insert a Palo Alto Networks firewall in front of a legacy port-based firewall to collect application information from incoming network traffic?
- a. VLAN
  - b. tunnel
  - c. tap
  - d. virtual wire
  - e. Layer 2
  - f. Layer 3
4. Which type of interface do you use to connect Layer 2 and Layer 3 interfaces?
- a. VLAN
  - b. tunnel
  - c. tap
  - d. virtual wire
  - e. Layer 2
  - f. Layer 3
5. Which three types of interfaces can the firewall's management web interface be bound to? (Choose three.)
- a. VLAN
  - b. tunnel
  - c. tap
  - d. virtual wire
  - e. Layer 2
  - f. Layer 3
6. Which three types of interfaces connect to a virtual router? (Choose three.)
- a. VLAN
  - b. tunnel
  - c. tap
  - d. virtual wire
  - e. Layer 2
  - f. Layer 3
7. Which dynamic routing protocol is *not* supported by the Palo Alto Networks firewall?
- a. RIP

- b. OSPF
  - c. OSPFv3
  - d. IGRP
  - e. BGP
8. Which action is *not* compatible with aggregate interface configuration?
- a. aggregating 18 Layer 3 interfaces
  - b. aggregating four virtual wire interfaces
  - c. aggregating interfaces in an HA pair
  - d. aggregating two 10Gbps optical and two 10Gbps copper Ethernet ports

## 2.8 Configure NAT

### 2.8.1 NAT policy rules

NAT allows the organization to use internal IP addresses that are not exposed to the internet. NAT rules are based on source and destination zones, source and destination addresses, and application services (such as HTTP). As is the case with Security policy rules, NAT policy rules are compared against incoming traffic in sequence, and the first rule that matches the traffic is applied.

### 2.8.2 Security rules

A Security policy allows you to enforce rules and actions. It can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same.

Security policy rules are matched from the top down. Up to two processing steps are in each Security policy match. Step 1 confirms that a match has been made based on the matching conditions provided in the Security policy. If a match is found in Step 1, the traffic is logged (based on that policy rule's configuration) and the chosen action (deny, allow, drop, reset) is performed. Once processing is complete, there will be no further matching in the Security policy rulebase.

### 2.8.3 Source NAT

Source NAT is typically used by internal users to access the internet; the source address is translated and kept private. There are three types of source NAT: dynamic IP and port (DIPP), dynamic IP, and static IP.

#### DIPP

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. 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

**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

**Static IP** allows the one-to-one, 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.

## 2.8.4 No-NAT Policies

No-NAT rules are configured to allow exclusion of IP addresses defined within the range of NAT rules defined later in the NAT policy. To define a no-NAT policy, specify all of the match criteria and select **No Source Translation** in the source translation column.

You can verify the NAT rules processed by selecting **Device > Troubleshooting** and testing the traffic matches for the NAT rule. For example:

Test Configuration		Test Result	Result Detail	
		NAT Policy Match Result	Name	Value
Select Test	NAT Policy Match		Result	access-corp
From	13-vlan-trust			
To	13-untrust			
Source	10.54.21.28			
Destination	8.8.8.8			
Source Port	[1 - 65535]			
Destination Port	445			
Protocol	6			
To Interface	None			
Ha Device ID	[0 - 1]			
		Execute	Reset	

## 2.8.5 Use session browser to find NAT rule name

This topic describes various settings for sessions other than timeouts values. Perform these tasks if you need to change the default settings.

### Step 1: Change the session settings.

Select **Device > Setup > Session** and edit the Session Settings.

### Step 2: Specify whether to apply newly configured Security policy rules to sessions that are in progress.

Select Rematch all sessions on config policy change to apply newly configured Security policy rules to sessions that are already in progress. This capability is enabled by default. If you clear this check box, any policy rule changes you make apply only to sessions initiated after you commit the policy change.

For example, if a Telnet session started while an associated policy rule 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.

### Step 3: Configure IPv6 settings.

- **ICMPv6 Token Bucket Size**—Default: 100 tokens. See the section [ICMPv6 Rate Limiting](#).
- **ICMPv6 Error Packet Rate (per sec)**—Default: 100. See the section [ICMPv6 Rate Limiting](#).
- **Enable IPv6 Firewalling**—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 **IPv6 Firewalling** setting must also be enabled for IPv6 to function.

### Step 4 : Enable jumbo frames and set the MTU.

- Select **Enable Jumbo Frame** to enable jumbo frame support on Ethernet interfaces. Jumbo frames have a maximum transmission unit (MTU) of 9,216 bytes and are available on certain models.
- Set the **Global MTU**, depending on whether or not you enabled jumbo frames:
  - If you did not enable jumbo frames, the **Global MTU** defaults to 1,500 bytes; the range is 576 to 1,500 bytes.
  - If you enabled jumbo frames, the **Global MTU** defaults to 9,192 bytes; the range is 9,192 to 9,216 bytes.

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.

### Step 5: Tune NAT session settings.

- **NAT64 IPv6 Minimum Network MTU**—Sets the global MTU for IPv6 translated traffic. The default of 1,280 bytes is based on the standard minimum MTU for IPv6 traffic.

- **NAT Oversubscription Rate**—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 firewall model.
- A rate of 1 means no oversubscription; each translated IP address and port pair can be used only once at a time.
- If the setting is **Platform Default**, user configuration of the rate is disabled and the default oversubscription rate for the model applies.

Reducing the oversubscription rate decreases the number of source device translations, but provides higher NAT rule capacities.

#### **Step 6 :** Tune accelerated aging settings.

Select Accelerated Aging to enable faster aging-out of idle sessions. You can also change the threshold (%) and scaling factor:

- **Accelerated Aging Threshold**—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 Accelerated Aging Scaling Factor to the aging calculations for all sessions.
- **Accelerated Aging Scaling Factor**—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.

#### **Step 7:** Enable packet buffer protection.

- Select **Packet Buffer Protection** to enable the firewall to take action against sessions that can overwhelm the its packet buffer and causes legitimate traffic to be dropped.
- If you enable packet buffer protection, you can tune the thresholds and timers that dictate how the firewall responds to packet buffer abuse.
  - **Alert (%)**: When packet buffer utilization exceeds this threshold, the firewall creates a log event. The threshold is set to 50% by default and the range is 0% to 99%. If the value is set to 0%, the firewall does not create a log event.
  - **Activate (%)**: When a packet buffer utilization exceeds this threshold, the firewall applies random early drop (RED) to abusive sessions. The threshold is set to 50% by default and the range is 0% to 99%. If the value is set to 0%, the firewall does not apply RED.
  - **Block Hold Time (sec)**: The amount of time a RED-mitigated session is allowed to continue before it is discarded. By default, the block hold time is 60 seconds. The range is 0 to 65,535 seconds. If the value is set to 0, the firewall does not discard sessions based on packet buffer protection.

- **Block Duration (sec):** This setting defines how long a session is discarded or an IP address is blocked. The default is 3,600 second with a range of 0 seconds to 15,999,999 seconds. If this value is set to 0, the firewall does not discard sessions or block IP addresses based on packet buffer protection.

**Step 8:** Enable buffering of multicast route setup packets.

- Select Multicast Route Setup Buffering to enable the firewall to preserve the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not yet exist for the corresponding multicast group. By default, the firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. You only need to enable multicast route setup buffering if your content servers are directly connected to the firewall and your custom application cannot withstand the first packet in the session being dropped. This option is disabled by default.
- If you enable buffering, you can also tune the Buffer Size, which specifies the buffer size per flow. The firewall can buffer a maximum of 5,000 packets.

**Step 9:** Save the session settings.

Click **OK**.

**Step 10:** Tune the Maximum Segment Size (MSS) adjustment size settings for a Layer 3 interface.

- Select **Network > Interfaces**, select **Ethernet**, **VLAN**, or **Loopback**, and select a Layer 3 interface.
- Select **Advanced >Other Info**.
- Select **Adjust TCP MSS** and enter a value for one or both of the following:
  - **IPv4 MSS Adjustment Size** (range is 40-300 bytes; default is 40 bytes).
  - **IPv6 MSS Adjustment Size** (range is 60-300 bytes; default is 60 bytes).
- Click **OK**.

**Step 11:** Commit your changes.

Click **Commit**.

**Step 12:** Reboot the firewall after changing the jumbo frame configuration.

- Select **Device > Setup > Operations**.
- Click **Reboot Device**.

## 2.8.6 U-Turn NAT

The term “U-Turn” is used when the logical path of a connection traverses the firewall from inside to outside and back in by connecting to an internal resource using its external IP address. U-Turn NAT is a configuration trick to accommodate a deployment where the external IP needs to reach an internal resource.

## Use of U-turn NAT

In some environments, an internal host may require an external IP address to run a certain service — for example, a locally hosted web server or mail server. Internal hosts may need to use the external IP address due to the absence of an internal DNS server or other requirements specific to the service.

In this example, using regular destination NAT configuration, any connections originating from the laptop directed to the server on its external IP address, 198.51.100.230, are directed to the default gateway, as the IP address is not in the local subnet. Connections then get translated to destination IP address 192.168.0.97 without applying source NAT, which causes the web server to send return packets directly to the workstation, resulting in an asymmetric flow.

With U-Turn NAT configured, outbound packets from the laptop also have source NAT applied to them.

The source NAT causes the server to send reply packets directly to the firewall rather than to the laptop. Sending packets directly to the firewall prevents asymmetry and allows the firewall to still apply content scanning to the session.

## Configuring U-Turn NAT

The Security policy has an inbound rule that allows inbound connections from the internet onto the internal web server with application web browsing, which is default port 80. Further, we have a simple outbound Security policy that allows any users to go to the internet on any application. Finally, we have the two implied rules that allow intrazonal traffic — for example, trust to trust — and the denied intranet zone that prevents sessions from reaching other zones without an explicit policy permitting it.

The NAT policy has an inbound rule to allow connections from anywhere to the external IP address to be translated to the server's internal IP address. It also has a hide-NAT rule to allow internal connections to go out to the internet and get source-translated behind the firewall's external interface IP address.

When we look at the client PC, trying to access 198.51.100.230 (the internet-facing IP address of the internal server) will result in a page not loading. Wireshark shows a syn packet being sent to the external IP, a syn/ack being received from the internal IP address 192.168.0.97, and a reset being sent because the client doesn't understand what's going on.

If we now go back to the firewall and open the NAT policy, we see that the inbound NAT rule has been set up to accept any source zone and translate that to the proper internal server IP address.

### Creating a New NAT Rule Details:

- **Name:** internal access
- **Source zone:** trust
- **Destination zone:** untrust
- **Destination address:** 198.51.100.230

### Under the Translated Packet tab:

- **Destination address:** 192.168.0.97 (IP address of the web server in question)
- **Source address translation:** Dynamic IP/Port
- **Switch address type:** Interface
- **Interface:** ethernet1/2 (internal interface of the firewall)
- **IP address:** 192.168.0.230/24

Name this new rule internal access. Go to the **Original Packet** tab, and set the **Source Zone** to **trust**, the **Destination Zone** to **untrust**, and the **Destination Address** to **198.51.100.230**. In the **Translation Packet** tab, set the **Destination Address**, just like the regular rule, to **192.168.0.97**. Enable source address translation by setting it to **Dynamic IP and Port**, and switch the **Address Type** to **interface address**.

You also can set the **Address Type** to **translated address** and choose an address in the IP range assigned to the interface. In this example, we'll stick with the IP address assigned to the interface for ease of use.

Select the trust zone interface from the drop-down, set its IP, then click **OK**.

**NOTE:** Be sure to place the new NAT rule above the inbound rule. Otherwise, the original NAT rule will take precedence over the newly created rule.

Commit the configuration, and return to the client PC.

### Verifying and Testing U-Turn NAT

If we open the webpage now, the internet information server 7 default page loads, and the web server is accessible from the inside on its external IP address.

If we take a look at the Wireshark packet capture, the client is receiving its returning packets from the external IP, because the firewall can now perform NAT on both directions of the flow.

### 2.8.7 Check HIT counts

View the number of times a Security, NAT, QoS, policy-based forwarding (PBF), Decryption, Tunnel Inspection, Application Override, Authentication, or DoS protection rule matches traffic to help keep your firewall policies up to date as your environment and security needs change. To prevent attackers from exploiting over-provisioned access, such as when a server is decommissioned or when you no longer need temporary access to a service, use the policy rule hit count data to identify and remove unused rules.

Policy rule usage data enables you to validate rule additions and rule changes and to monitor the time frame when a rule was used. For example, when you migrate port-based rules to app-based rules, you create an app-based rule above the port-based rule and check for any traffic that matches the port-based rule. After migration, the hit count data helps you determine whether it is safe to remove the port-based rule by confirming whether traffic is matching the app-based rule instead of the port-based rule. The policy rule hit count helps you determine whether a rule is effective for access enforcement.

You can reset the rule hit count data to validate an existing rule or to gauge rule usage within a specified period of time. Policy rule hit count data is not stored on the firewall or Panorama so that data is no longer available after you reset (clear) the hit count.

After filtering your policy rulebase, administrators can take action to delete, disable, enable, and tag policy rules directly from the policy optimizer. For example, you can filter for unused rules and then tag them for review to determine whether they can be safely deleted or kept in the rulebase. By enabling administrators to take action directly from the policy optimizer, you reduce the management overhead required to further assist in simplifying your rule lifecycle management and ensure that your firewalls are not over-provisioned.

#### Step 1: Launch the Web Interface.

1. Navigate to Policy Rulebase Settings (**Device > Setup > Management**).

#### Step 2: Verify that **Policy Rule Hit Count** is enabled.

The screenshot shows the 'Policy Rulebase Settings' page. At the top, there is a gear icon. Below it, several checkboxes are present: 'Require Tag on policies' (unchecked), 'Require description on policies' (unchecked), 'Fail commit if policies have no tags or description' (unchecked), 'Require audit comment on policies' (unchecked), 'Audit Comment Regular Expression' (empty input field), 'Policy Rule Hit Count' (checked with a green checkmark), and 'Policy Application Usage' (checked with a blue checkmark).

#### Step 3: Select Policies.

#### Step 4: View the policy rule usage for each policy rule:

- **Hit Count**—The number of times traffic matched the criteria you defined in the policy rule. Persists through reboot, dataplane restarts, and upgrades unless you manually reset or rename the rule.
- **Last Hit**—The most recent timestamp for when traffic matched the rule.
- **First Hit**—The first instance when traffic was matched to this rule.
- **Modified**—The date and time the policy rule was last modified.
- **Created**—The date and time the policy rule was created.

NAME	Source				Rule Usage			MODIFIED	CREATED
	T...	Z...	A...	U...	HIT COUNT	LAST HIT	FIRST HIT		
/ideo	n...	a...	a...	a...	2424328	2020-09-22 11:33:00	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Video Streaming	n...	a...	a...	a...	14337228	2020-09-22 16:26:58	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
`cavenger	n...	a...	a...	a...	321760616	2020-09-22 16:27:10	2019-07-30 10:12:57	2020-07-27 13:27:16	2019-07-30 09:50
Web Traffic	n...	a...	a...	a...	1509584361	2020-09-22 16:27:10	2019-07-30 10:12:02	2020-07-27 13:27:16	2019-07-30 09:50
iperf	n...	a...	a...	a...	5	2019-10-15 14:54:31	2019-10-11 13:08:28	2020-07-27 13:27:16	2019-07-30 09:50

Step 5: In the Policy Optimizer dialog, view the **Rule Usage** filter.

Step 6: Filter rules in the selected rulebase.

1. Select the **Timeframe** you want to filter on or specify a **Custom** time frame.
2. Select the rule **Usage** on which to filter.
3. (Optional) If you have reset the rule usage data for any rules, check for **Exclude rules reset during the last <number of days> days** and decide when to exclude a rule based on the number of days you specify since the rule was reset. Only rules that were reset before your specified number of days are included in the filtered results

The screenshot shows the PA-VM interface with the Policies tab selected. On the left, there's a sidebar with various security and optimization categories like NAT, QoS, Policy Based Forwarding, etc. Under the Policy Optimizer section, there are filters for 'No App Specified' and 'Unused Apps'. The main area is titled 'Rule Usage' with a sub-section 'Unused in 30 days' showing 31 items. A table lists rules with columns: NAME, HIT COUNT, LAST HIT, FIRST HIT, RESET DATE, MODIFIED, and CREATED. The first few rows include 'Deny\_Malicious', 'Block\_Quic', 'Allow\_DNS', and 'Block\_PasteBin\_Redd...'. The interface includes a search bar, a toolbar with 'Commit', 'Save', 'Print', and 'Search' buttons, and a footer with object selection and filtering options.

NAME	Rule Usage				MODIFIED	CREATED
	HIT COUNT	LAST HIT	FIRST HIT	RESET DATE		
1 Deny_Malicious	75211831	2020-06-24 10:58:26	2019-08-13 14:38:29	-	2020-07-27 13:27:16	2019-07-30 09:50:23
2 Block_Quic	2809657	2020-09-11 00:15:57	2019-08-22 08:14:02	-	2020-07-27 13:27:16	2019-07-30 09:50:23
3 Allow_DNS	433179426	2020-09-22 16:35:47	2019-08-13 14:39:37	-	2020-07-27 13:27:16	2019-07-30 09:50:23
4 Block_PasteBin_Redd...	18290041	2020-09-22 16:33:45	2020-04-15 18:00:36	-	2020-07-27 13:27:16	2020-04-15 17:29:12
5 Block_Social_Media	0	-	-	-	2020-07-27 13:27:16	2020-06-30 16:37:15
6 Temp_Allow_for_Conf...	0	-	-	-	2020-07-27 13:27:16	2020-05-22 17:35:44
7 Allow_Fetch	161307	2020-08-13 09:34:46	2020-04-15 18:45:07	-	2020-07-27 13:27:16	2020-04-15 18:44:46
8 Allow_SCADA_Traffic	357362	2020-09-22 16:35:09	2020-04-09 11:34:44	-	2020-07-27 13:27:16	2020-04-09 11:34:48
9 Zoom	0	-	-	-	2020-07-27 13:27:16	2020-04-16 11:43:49
10 Allow_Gsuite	4976276	2020-09-22 16:18:20	2020-04-16 11:48:02	-	2020-07-27 13:27:16	2020-04-16 11:43:49
11 Allow_Office365_Core	235	2020-09-22 13:19:47	2020-05-22 17:49:50	-	2020-07-27 13:27:16	2020-05-22 17:28:26
12 Allow_Office365_Infra	0	-	-	-	2020-07-27 13:27:16	2020-05-22 22:46:44
13 Allow_Office365_ssl...	29597	2020-09-22 16:33:01	2020-05-22 22:55:02	-	2020-07-27 13:27:16	2020-05-22 22:46:44
14 Allow_March_Madness	13980	2020-08-11 08:54:17	2020-04-09 15:22:46	-	2020-07-27 13:27:16	2020-04-09 14:47:09
15 Allow_ssl_http	33526300	2020-09-22 16:33:45	2020-04-09 15:22:46	-	2020-07-27 13:27:16	2020-04-09 14:47:09
16 Known_Device_Ping	151859	2020-08-13 09:36:37	2020-04-13 16:57:45	-	2020-07-27 13:27:16	2020-04-13 16:39:40
17 Allow_Office_Interne...	30	2020-08-13 09:36:56	2020-04-22 11:26:54	-	2020-07-27 13:27:16	2020-04-22 11:26:20

4. (Optional) Specify search filters based on rule data

- Hover your cursor over the column header and **Columns**.
- Add any additional columns you want to display or use for filter.

NAME
<input checked="" type="checkbox"/> Location
<input type="checkbox"/> Service
<input type="checkbox"/> Tags
<input type="checkbox"/> Type
<input type="checkbox"/> Source Zone
<input type="checkbox"/> Source Address
<input type="checkbox"/> Source User
<input type="checkbox"/> Source
<input type="checkbox"/> Destination Zone
<input type="checkbox"/> Destination Address
<input type="checkbox"/> Application
<input type="checkbox"/> URL Category
<input type="checkbox"/> Action
<input type="checkbox"/> Profile
<input type="checkbox"/> Options
<input type="checkbox"/> Rule UUID
<input type="checkbox"/> Target
<input type="checkbox"/> Description
<input type="checkbox"/> Traffic (Bytes, 30 days)
<input type="checkbox"/> App Usage Apps Allowed
<input type="checkbox"/> App Usage Apps Seen
<input type="checkbox"/> App Usage Days with No New Apps
<input type="checkbox"/> App Usage Compare
<input checked="" type="checkbox"/> Rule Usage
<input checked="" type="checkbox"/> Modified
<input checked="" type="checkbox"/> Created

- Hover your cursor over the column data that you would like to filter on **Filter**. For data that contain dates, select whether to filter using **This date**, **This date or earlier**, or **This date or later**.
- **Apply Filter ( → ).**

NAME	Rule Usage				MODIFIED	CREATED
	HIT COUNT	LAST HIT	FIRST HIT	RESET DATE		
Allow_DNS	43317426	2020-09-22 16:35:47	2019-08-13 14:39:37	-	2020-07-27 13:27:16	2019-07-30 09:51
Block_PasteBin_Redir...	18290041	2020-09-22 16:33:45	2020-04-15 18:00:36	-	2020-07-27 13:27:16	2020-04-15 17:29:12
Block_Social_Media	0	-	-	-	2020-07-27 13:27:16	2020-06-30 16:37:15
Temp Allow for Cont...	0	-	-	-	2020-07-27 13:27:16	2020-05-22 17:35:44
Allow_Fetch	161307	2020-08-13 09:34:46	2020-04-15 18:45:07	-	2020-07-27 13:27:16	2020-04-15 18:44:46
Allow_SCADA_Traffic	357362	2020-09-22 16:35:09	2020-04-09 11:34:44	-	2020-07-27 13:27:16	2020-04-09 11:34:48
Zoom	0	-	-	-	2020-07-27 13:27:16	2020-04-16 11:43:49
Allow_CoAule	4976276	2020-09-22 16:18:20	2020-04-16 11:48:02	-	2020-07-27 13:27:16	2020-04-16 11:43:49
Allow_Office365_Con...	235	2020-09-22 13:19:47	2020-05-22 17:49:50	-	2020-07-27 13:27:16	2020-05-22 17:28:26
Allow_Office365_Infra	0	-	-	-	2020-07-27 13:27:16	2020-05-22 22:24:44
Allow_Office365_ssl...	29597	2020-09-22 16:33:01	2020-05-22 22:55:02	-	2020-07-27 13:27:16	2020-05-22 22:46:44
Allow_March_Madness	13980	2020-08-11 08:54:17	2020-04-09 15:22:46	-	2020-07-27 13:27:16	2020-04-09 14:47:09
Allow_wi_ttp	33526300	2020-09-22 16:33:45	2020-04-09 15:22:46	-	2020-07-27 13:27:16	2020-04-09 14:47:09
Known_Device_Plug	151859	2020-08-10 09:36:37	2020-04-13 16:57:45	-	2020-07-27 13:27:16	2020-04-13 16:39:40
Allow_Office_Interne...	30	2020-08-13 09:36:56	2020-04-22 11:26:54	-	2020-07-27 13:27:16	2020-04-22 11:26:20
Block_Plug	109924	2020-07-18 00:08:59	2020-04-13 16:16:38	-	2020-07-27 13:27:16	2020-04-13 16:44:55
File-sharing	1138834	2020-09-22 16:26:08	2020-05-22 19:26:02	-	2020-07-27 13:27:16	2020-05-22 19:23:17

### Step 7: Take action on one or more unused policy rules.

1. Select one or more unused policy rules.
2. Perform one of the following actions:
  - **Delete**—Delete one or more selected policy rules.
  - **Enable**—Enable one or more selected policy rules when disabled.
  - **Disable**—Disable one or more selected policy rules.
  - **Tag**—Apply one or more group tags to one or more selected policy rules. The group tag must already exist in order to tag policy rule.
  - **Untag**—Remove one or more group tags from one or more selected policy rules.
3. **Commit** your changes.

### 2.8.7 Reference

View policy rule usage:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-policy-rule-usage>

Palo Alto Networks #1: Initial Configuration (for beginners):

<https://rtodto.net/palo-alto-networks-1-initial-configuration/>

NAT Policy overview:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/nat/nat-policy-rules/nat-policy-overview>

Configure NAT:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/nat/configure-nat>

NAT Configuration Examples:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/nat/nat-configuration-examples>

Policies > NAT

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/policies/policies-nat>

Configure Session Settings:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/session-settings-and-timeouts/configure-session-settings>

## 2.8.8 Sample Questions

1. Which two source address translation types can use a single IP address to NAT multiple IP addresses? (Choose two.)

- a. static IP
- b. dynamic IP
- c. dynamic IP and port
- d. translated address
- e. address override

2. Which NAT type can be used to translate between IPv4 and IPv6?

- a. IPv4
- b. NAT64
- c. NPTv6
- d. IPv6

3. How does a firewall process a packet that has more than one NAT policy rule that matches the packet?

- a. Each matching rule in the list is applied from the top down, with cumulative changes being processed at the end of the list.
- b. The first rule matching the packet is applied and processed, skipping the others.
- c. The firewall issues an error when committing NAT policy rules that can affect the same packet.
- d. The last matching rule in the list is applied and processed.

## 2.9 Configure site-to-site tunnels

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.

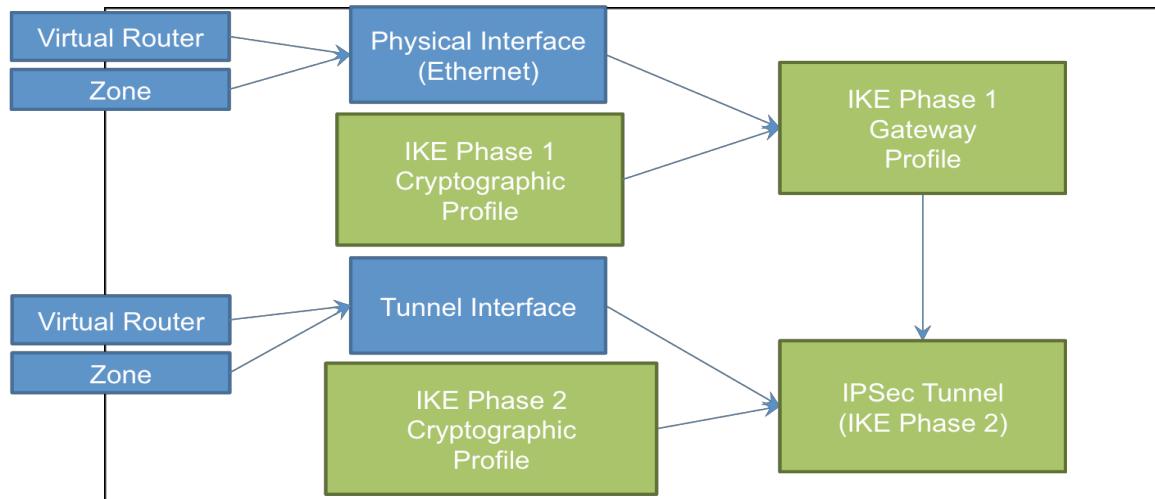
To route traffic between the sites, a tunnel interface does not require an IP address. An IP address is only required if you want to enable tunnel monitoring or if you are using a dynamic routing protocol to route traffic across the tunnel. With dynamic routing, the tunnel IP address serves as the next 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.

### 2.9.1 IPsec components

#### *IPsec Tunnel Interfaces*

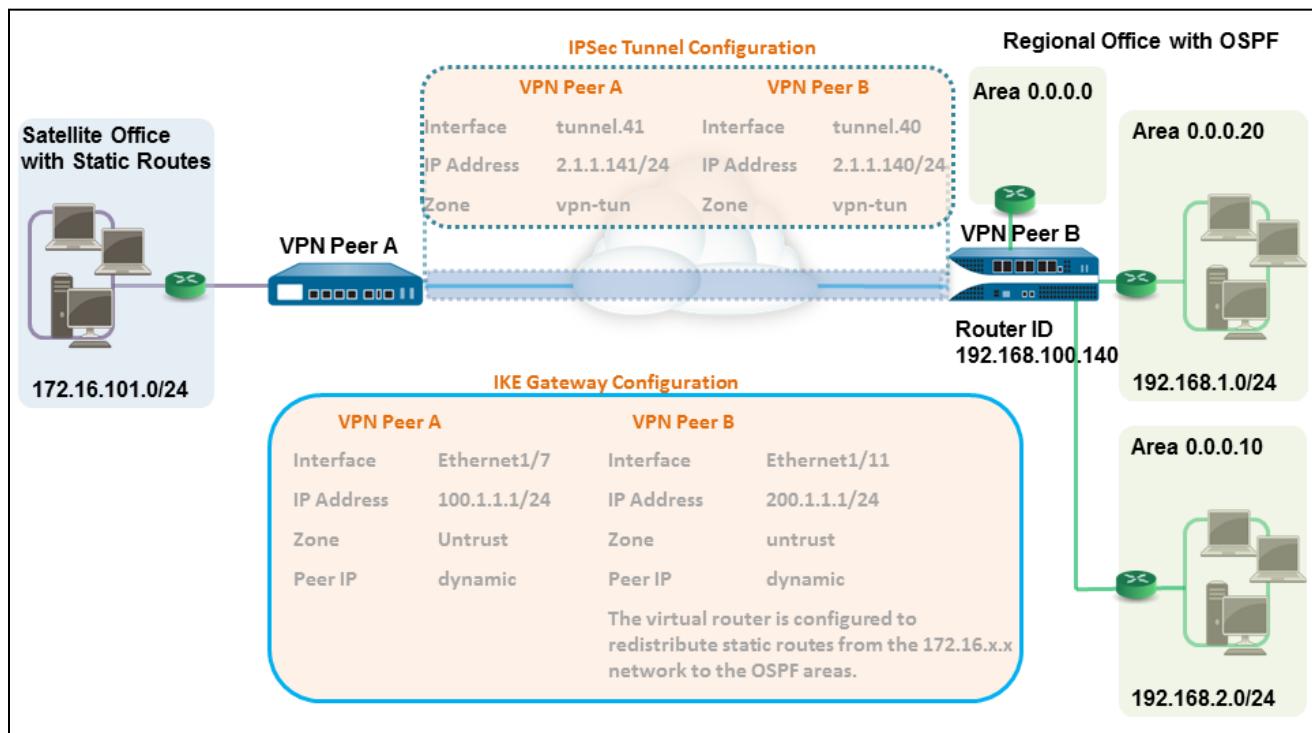
IPsec VPNs are terminated on Layer 3 tunnel interfaces. (These tunnel interfaces can be put into separate zones, thus allowing a specific Security policy per zone.) These tunnels require IPsec and Crypto Profiles for Phase 1 and Phase 2 connectivity. PAN-OS supports route-based VPNs, which means that the decision to route traffic through the VPN is made by the virtual router. Palo Alto Networks firewalls support connection to alternative policy-based VPNs requiring the use of proxy IDs for compatibility. The following figure shows the various objects involved in IPsec tunnel definitions.



## 2.9.2 Static peers and dynamic peers for IPsec

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 to propagate (export) the static routes to the OSPF autonomous system.



### 2.9.3 IPsec tunnel Monitor Profiles

A Monitor Profile is used to monitor IPsec tunnels and to monitor a next-hop device for PBF rules. In both cases, the Monitor Profile is used to specify an action to take when a resource (IPsec tunnel or next-hop device) becomes unavailable. Monitor Profiles are optional, but they can be very useful for maintaining connectivity between sites and ensuring that PBF rules are maintained. The following settings are used to configure a Monitor Profile.

FIELD	DESCRIPTION
Name	Enter a name to identify the Monitor Profile (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Action	<p>Specify an action to take if the tunnel is not available. If the threshold number of heartbeats is lost, the firewall takes the specified action.</p> <ul style="list-style-type: none"> <li><b>wait-recover:</b> Wait for the tunnel to recover; do not take additional action. Packets will continue to be sent according to the PBF rule.</li> <li><b>fail-over:</b> Traffic will fail over to a backup path, if one is available. The firewall uses routing table lookup to determine routing for the duration of this session.</li> </ul> <p>In both cases, the firewall tries to negotiate new IPsec keys to accelerate recovery.</p>

Interval	Specify the time between heartbeats (range is 2 to 10; default is 3).
Threshold	Specify the number of heartbeats to be lost before the firewall takes the specified action (range is 2 to 10; default is 5).

## 2.9.4 IPsec tunnel testing

Perform this task to test VPN connectivity.

**Step 1:** 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>
```

**Step 2:** Enter the following command to test if IKE phase 1 is set up:

```
show vpn ike-sa gateway <gateway_name>
```

In the output, check whether the Security Association displays. If it doesn't, review the syslog messages to interpret the reason for failure.

**Step 3:** 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>
```

**Step 4:** Enter the following command to test if IKE phase 2 is set up:

```
show vpn ipsec-sa tunnel <tunnel_name>
```

In the output, check whether the Security Association displays. If it doesn't, review the syslog messages to interpret the reason for failure.

**Step 5:** To view the VPN traffic flow information, use the following command:

```
show vpn flow
total tunnels configured: 1
filter - type IPSec, state any

total IPSec tunnel configured: 1
total IPSec tunnel shown: 1

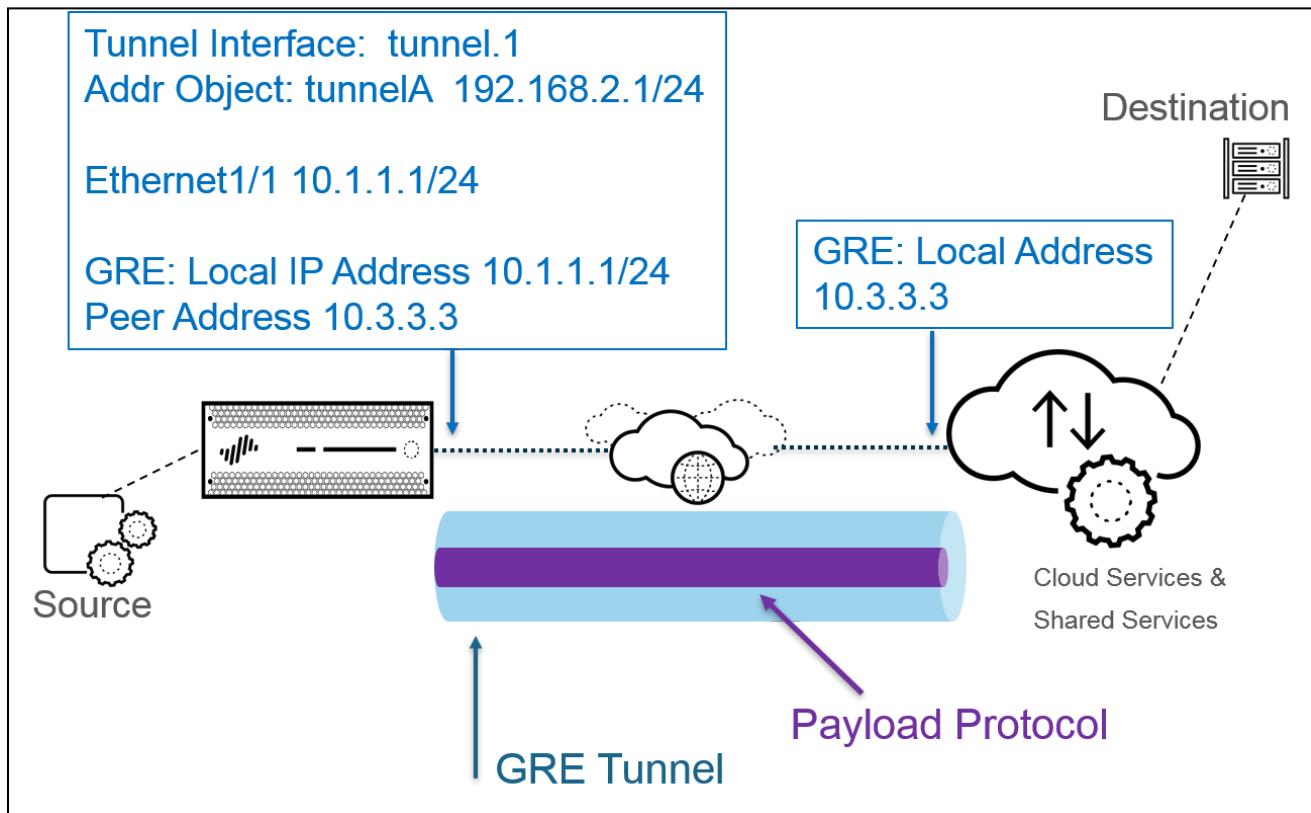
name          id      state    local-ip      peer-ip      tunnel-i/f
-----
vpn-to-siteB  5      active   100.1.1.1    200.1.1.1    tunnel.41
```

## 2.9.5 Generic Routing Encapsulation

A Generic Routing Encapsulation (GRE) tunnel connects two endpoints (a firewall and another appliance) in a point-to-point, logical link. The firewall can terminate GRE tunnels; you can route or forward packets to a GRE tunnel. GRE tunnels are simple to use and often the tunneling protocol of choice for point-to-point connectivity, especially to services in the cloud or to partner networks.

Create a GRE tunnel when you want to direct packets that are destined for an IP address to take a certain point-to-point path — for example, to a cloud-based proxy or to a partner network. The packets travel through the GRE tunnel (over a transit network such as the internet) to the cloud service while on their way to the destination address. This enables the cloud service to enforce its services or policies on the packets.

The following figure is an example of a GRE tunnel connecting the firewall across the internet to a cloud service.



When the firewall allows a packet to pass (based on a policy match) and the packet egresses to a GRE tunnel interface, the firewall adds GRE encapsulation; it doesn't generate a session. The firewall does not perform a Security policy rule lookup for the GRE-encapsulated traffic, so you don't need a Security policy rule for the GRE traffic that the firewall encapsulates. However, when the firewall receives GRE traffic, it generates a session and applies all policies to the GRE IP header in addition to the encapsulated traffic. The firewall treats the received GRE packet like any other packet. Therefore:

- If the firewall receives the GRE packet on an interface that has the same zone as the tunnel interface associated with the GRE tunnel (for example, tunnel.1), the source zone is the same as the destination zone. By default, traffic is allowed within a zone (intrazone traffic), so the ingress GRE traffic is allowed by default.
- However, if you configured your own intrazone Security policy rule to deny such traffic, you must explicitly allow GRE traffic.
- Likewise, if the zone of the tunnel interface associated with the GRE tunnel (for example, tunnel.1) is a different zone from that of the ingress interface, you must configure a Security policy rule to allow the GRE traffic.

Because the firewall encapsulates the tunneled packet in a GRE packet, the additional 24 bytes of GRE header automatically result in a smaller MSS in the MTU. If you don't change the IPv4 MSS adjustment size for the interface, the firewall reduces the MTU by 64 bytes by default (40 bytes of IP header + 24 bytes of GRE header). This means that if the default MTU is 1,500 bytes, the MSS will be 1,436 bytes ( $1,500 - 40 - 24 = 1,436$ ). If you configure an MSS adjustment size of 300 bytes, for example, the MSS will be only 1,176 bytes ( $1,500 - 300 - 24 = 1,176$ ).

The firewall does not support routing a GRE or IPsec tunnel to a GRE tunnel, but you can route a GRE tunnel to an IPsec tunnel. Additionally:

- A GRE tunnel does not support QoS.
- The firewall does not support a single interface acting as both a GRE tunnel endpoint and a decryption broker.
- GRE tunneling does not support NAT between GRE tunnel endpoints.

## 2.9.6 One-to-one and one-to-many tunnels

Palo Alto Networks supports the following VPN deployments:

- **Site-to-site VPN:** This deployment provides a simple VPN that connects a central site and a remote site. This is also commonly referred to as a hub-and-spoke VPN that connects a central (gateway) site with multiple remote (branch) sites.
- **Remote-user-to-site VPN:** This deployment provides an endpoint client to use GlobalProtect agent for a secure remote user access connection through the firewall gateway.
- **Large scale VPN (LVPN):** This deployment uses Palo Alto Networks GlobalProtect LVPN. It provides a scalable mechanism to provide hub-and-spoke VPN for up to 1,024 branch offices.

## 2.9.7 Determine when to use proxy IDs

### Symptom

When configuring IPsec VPNs, Proxy IDs are a requirement with a peer that supports Policy Based VPNs.

Sometimes multiple local and remote subnets need to communicate over VPN for the same peer. If peer side is a policy based VPN you will need to setup multiple proxy IDs on the Palo Alto firewall Tunnel configuration to match with peer's policies.

Even with the correct configuration, the traffic may fail because of the way proxy IDs are stored in the Dataplane (DP). This article highlights best practices to be used when configuring multiple Proxy IDs with the same peer which are for overlapping subnets.

## Environment

- Any PAN-OS.
- Palo Alto Firewall.
- IPSEC VPN configured with Proxy IDs.

## Cause

When multiple Proxy IDs are configured, naming of Policy IDs is important as order of proxy ID matching depends on the string order of the proxy id name.

Example:

Let's say there are 4 Proxy IDs configured under the tunnel configuration:

```
TestProxyID-1      : Local = 10.1.1.0/24,    Remote = 192.168.30.0/24
ProxyID-10_8_0_0   : Local = 10.8.1.0/24,           Remote =
192.168.30.0/24
proxy-id-10_123_0_0 : Local     = 10.123.1.0/24,     Remote =
192.168.30.0/24
AllNetworks        : Local     = 10.0.0.0/8,          Remote =
192.168.30.0/24
```

When the proxy IDs are stored in DP, they are sorted using String Comparison (ASCII sorting)

To determine the sort order, we can use any sorting tools such as <https://www.textfixer.com/tools/alphabetical-order.php>

Using the above, the string sort order for the above proxy ID names:

```
AllNetworks        : Local     = 10.0.0.0/8,          Remote =
192.168.30.0/24
proxy-id-10_123_0_0 : Local     = 10.123.1.0/24,     Remote =
192.168.30.0/24
```

```
ProxyID-10_8_0_0      : Local = 10.8.1.0/24,    Remote =
192.168.30.0/24

TestProxyID-1        : Local = 10.1.1.0/24,    Remote =
192.168.30.0/24
```

IPSEC Security SA's will be stored in this order in DP. This will affect traffic processing as when a certain traffic needs to be encrypted using one of the proxy IDs, it will look from top to bottom for the first matching proxy ID.

In the above example, even though "**AllNetworks**" proxy ID is defined on bottom in the configuration, but in DP it will be the first in order.

In the above example, if any traffic is going from source 10.123.1.0/24 via this IPSEC tunnel to a remote IP, it will not be send via "**proxy-id-10\_123\_0\_0**" but via "**AllNetworks**". So this may fail on the remote side, who is checking incoming traffic against proxy IDs.

### Resolution

For proxy IDs with overlapping subnets, define the proxy ID names so that more specific proxy ID name is above the broader Proxy ID name as per String Sorting.

## 2.9.8 References

Tunnel interface:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/site-to-site-vpn-concepts/tunnel-interface>

Site-to-Site VPN with static and dynamic routing:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/site-to-site-vpn-quick-configs/site-to-site-vpn-with-static-and-dynamic-routing>

VPN Deployments:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/vpn-deployments>

Site-to-Site VPN Overview:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/site-to-site-vpn-overview>

GlobalProtect Administrator's Guide:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin.html>

Large Scale VPN (LSVPN):

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/large-scale-vpn-lsvpn>

Network > Network Profiles > Monitor:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor.html>

Test VPN Connectivity:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/test-vpn-connectivity.html>

Configure Multiple Proxy IDs in VPN Tunnel with Overlapping Subnet Ranges:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PLTICAO>

## 2.9.9 Sample Questions

1. Why is tunnel interface used?
  - a. to configure proxy IDs
  - b. to deliver traffic between two endpoints
  - c. to set up a VPN tunnel
  - d. to apply policy
  
2. Which command is used to test the IKE phase 1 set up?
  - a. show vpn ike-sa gateway <gateway\_name>
  - b. show vpn ipsec-sa tunnel <tunnel\_name>
  - c. test vpn ike-sa gateway <gateway\_name>
  - d. test vpn ipsec-sa tunnel <tunnel\_name>
  
3. Which profile is used to monitor IPsec tunnels and next-hop device?
  - a. Redistribution Profile
  - b. monitor profile
  - c. Layer 3 tunnel
  - d. Logical interface
  
4. Which technique is used to sort proxy IDs when they are stored in DP?
  - a. Unicode sorting
  - b. String comparison or ASCII sorting
  - c. random sorting
  - d. a and b

## 2.10 Configure service routes

Configure service routes globally for the firewall. 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.

## 2.10.1 Default service routes

Perform the following tasks to configure static routes or a default route for a virtual router on the firewall.

### Step 1: Configure a static route.

- Select **Network > Virtual Router**, and select the virtual router you are configuring, such as **default**.
- Select the **Static Routes** tab.
- Select **IPv4** or **IPv6**, depending on the type of static route you want to configure.
- Add a **Name** for the route. The name must start with an alphanumeric character, and it can contain a combination of alphanumeric characters, underscores (\_), hyphens (-), dots (.), and spaces. Beginning with PAN-OS 10.0.8, the name can be a maximum of 63 characters.
- For **Destination**, enter the route and netmask (for example, 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address). If you're creating a default route, enter the default route (0.0.0.0/0 for an IPv4 address or ::/0 for an IPv6 address). Alternatively, you can create an address object of type IP Netmask.
- (Optional) For **Interface**, specify the outgoing interface for packets to use to go to the next hop. Use this for stricter control over which interface the firewall uses rather than the interface in the route table for the next hop of this route.
- For **Next Hop**, select one of the following:
  - **IP Address:** Enter the IP address (for example, 192.168.56.1 or 2001:db8:49e:1::1) when you want to route to a specific next hop. You must enable IPv6 on the interface (when you configure Layer 3 interfaces) to use an IPv6 next hop address. If you're creating a default route, for **Next Hop** you must select **IP Address** and enter the IP address for your internet gateway (for example, 192.168.56.1 or 2001:db8:49e:1::1). Alternatively, you can create an address object of type IP Netmask. The address object must have a netmask of /32 for IPv4 or /128 for IPv6.
  - **Next VR:** Select this option and then select a virtual router if you want to route internally to a different virtual router on the firewall.
  - **FQDN:** Enter an FQDN or select an address object that uses an FQDN. You can also create a new address object of type FQDN.

If you use an FQDN as a static route next hop, that FQDN must resolve to an IP address that belongs to the same subnet as the interface you configured for the static route; otherwise, the firewall rejects the resolution, and the FQDN remains unresolved.

The firewall uses only one IP address (from each IPv4 or IPv6 family type) from the DNS resolution of the FQDN. If the DNS resolution returns more than one address, the firewall uses the preferred IP address that matches the IP family type (IPv4 or IPv6) configured for the next hop. The preferred IP address is the first address the DNS server returns in its initial response. The firewall retains this address as preferred as long as the address appears in subsequent responses, regardless of its order.

- **Discard:** Select to drop packets that are addressed to this destination.

- **None:** Select if there is no next hop for the route. For example, a point-to-point connection does not require a next hop because there is only one way for packets to go.
- Enter an **Admin Distance** for the route to override the default administrative distance set for static routes for this virtual router (range is 10 to 240; default is 10).
- Enter a **Metric** for the route (range is 1 to 65,535).

**Step 2:** Choose where to install the route.

Select the RIB into which you want the firewall to install the static route:

- **Unicast:** Install the route in the unicast route table. Choose this option if you want the route used only for unicast traffic.
- **Multicast:** Install the route in the multicast route table (available for IPv4 routes only). Choose this option if you want the route used only for multicast traffic.
- **Both:** Install the route in the unicast and multicast route tables (available for IPv4 routes only). Choose this option if you want either unicast or multicast traffic to use the route.
- **No Install:** Do not install the route in either route table.

**Step 3:** (Optional) If your firewall model supports Bidirectional forwarding detection (BFD), you can apply a BFD Profile to the static route so that if the static route fails, the firewall removes the route from the RIB and FIB and uses an alternative route. Default is None.

**Step 4:** Click **OK** twice.

**Step 5:** Commit the configuration.

## 2.10.2 Custom service routes

When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you will want to create different service routes for each virtual system.

One use case for configuring service routes at the virtual system level is an ISP that needs to support multiple individual tenants on a single Palo Alto Networks firewall.

## 2.10.3 Destination service routes

On the **Global** tab, when you click **Service Route Configuration > Customize**, the **Destination** tab appears. Destination service routes are available under the Global tab only (not the **Virtual Systems** tab) so that the service route for an individual virtual system cannot override route table entries that are not associated with that virtual system. You can use a destination service route to add a customized redirection of a service that is not supported on the customized list of services. A destination service route is a way to set up routing to override the FIB route table. Any settings in the destination service routes override the route table entries. They could be related or unrelated to any service.

The Destination tab is for the following use cases:

- When a service does not have an application service route.
- Within a single virtual system, when you want to use multiple virtual routers or a combination of a virtual router and management port.

DESTINATION SERVICE ROUTE SETTINGS	DESCRIPTION
Destination	Enter the <b>Destination IP address</b> . An incoming packet with a destination IP address that matches this address will use as its source the <b>Source Address</b> you specify for this service route.
Source Interface	To limit the drop-down for <b>Source Address</b> , select a <b>Source Interface</b> . Selecting <b>Any</b> causes all IP addresses on all interfaces to be available in the Source Address drop-down. Selecting <b>MGT</b> causes the firewall to use the MGT interface for the service route.
Source Address	Select the <b>Source Address</b> for the service route; this address will be used for packets returning from the destination. You do not need to enter the subnet for the destination address.

## 2.10.4 Custom routes for different virtual systems versus destination routes

### *Virtual Systems*

When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you'd want to create different service routes for each virtual system.

One use case for configuring service routes at the virtual system level is if you are an ISP who needs to support multiple individual tenants on a single Palo Alto Networks firewall. Each tenant requires custom service routes to access service such as DNS, Kerberos, LDAP, NetFlow, RADIUS, TACACS+, Multi-Factor Authentication, email, SNMP trap, syslog, HTTP, User-ID Agent, VM Monitor, and Panorama (deployment of content and software updates). 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.

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.

- [Customize Service Routes to Services for Virtual Systems](#)
- [Configure a PA-7000 Series Firewall for Logging Per Virtual System](#)
- [Configure Administrative Access Per Virtual System or Firewall](#)

### ***Destination Routes***

On the **Global** tab, when you click **Service Route Configuration > Customize**, the **Destination** tab appears. Destination service routes are available under the Global tab only (not the **Virtual Systems** tab) so that the service route for an individual virtual system cannot override route table entries that are not associated with that virtual system. You can use a destination service route to add a customized redirection of a service that is not supported on the customized list of services. A destination service route is a way to set up routing to override the FIB route table. Any settings in the destination service routes override the route table entries. They could be related or unrelated to any service.

The Destination tab is for the following use cases:

- When a service does not have an application service route.
- Within a single virtual system, when you want to use multiple virtual routers or a combination of a virtual router and management port.

DESTINATION SERVICE ROUTE SETTINGS	DESCRIPTION
Destination	Enter the <b>Destination IP address</b> . An incoming packet with a destination IP address that matches this address will use as its source the <b>Source Address</b> you specify for this service route.
Source Interface	To limit the drop-down for <b>Source Address</b> , select a <b>Source Interface</b> . Selecting <b>Any</b> causes all IP addresses on all interfaces to be available in the Source Address drop-down. Selecting <b>MGT</b> causes the firewall to use the MGT interface for the service route.

Source Address	Select the <b>Source Address</b> for the service route; this address will be used for packets returning from the destination. You do not need to enter the subnet for the destination address.
----------------	--

## 2.10.5 How to verify service routes

Configure service routes globally for the firewall. 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.

## 2.10.6 References

Configure a Static Route:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/static-routes/configure-a-static-route>

Service Routes:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service-routes>

## 2.10.7 Sample Questions

1. Which protocol is supported for traffic decryption matching a decryption policy rule?
  - a. IPsec
  - b. SP3
  - c. SSH
  - d. NLSP
  
2. Where do you specify that a certificate is to be used for SSL Forward Proxy?
  - a. certificate properties
  - b. Decryption Profile
  - c. decryption policy
  - d. Security policy
  
3. Which feature must be configured to exclude sensitive traffic from decryption?
  - a. Security policy rule that includes the specific URL with an “allow” action
  - b. decryption policy rule with the specific URL and “no decrypt” action
  - c. application override policy that matches the application URL and port number
  - d. Decryption Profile that includes the site’s URL

## 2.11 Configure application-based QoS

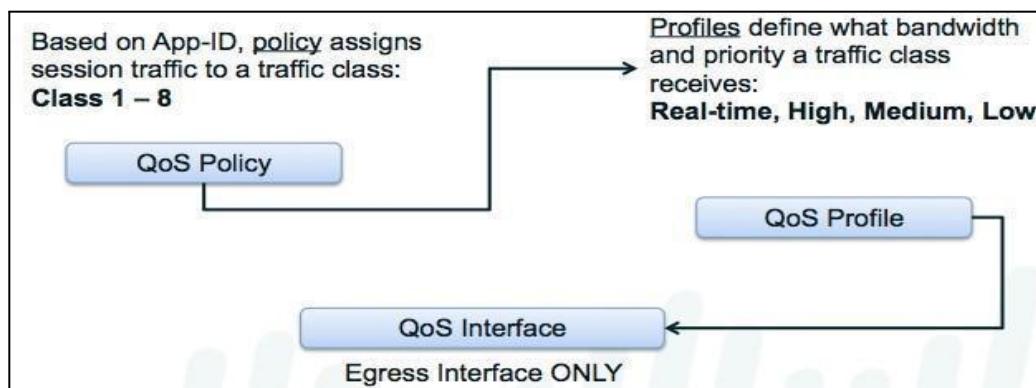
QoS is a set of technologies that works on a network to guarantee its ability to dependably run high-priority applications and traffic with shared network capacity. QoS technologies achieve this by providing differentiated handling and capacity allocation to specific flows in network traffic, which enables the network administrator to assign the order in which traffic is handled and the amount of bandwidth provided to traffic.

### 2.11.1 Enablement requirements

#### *QoS*

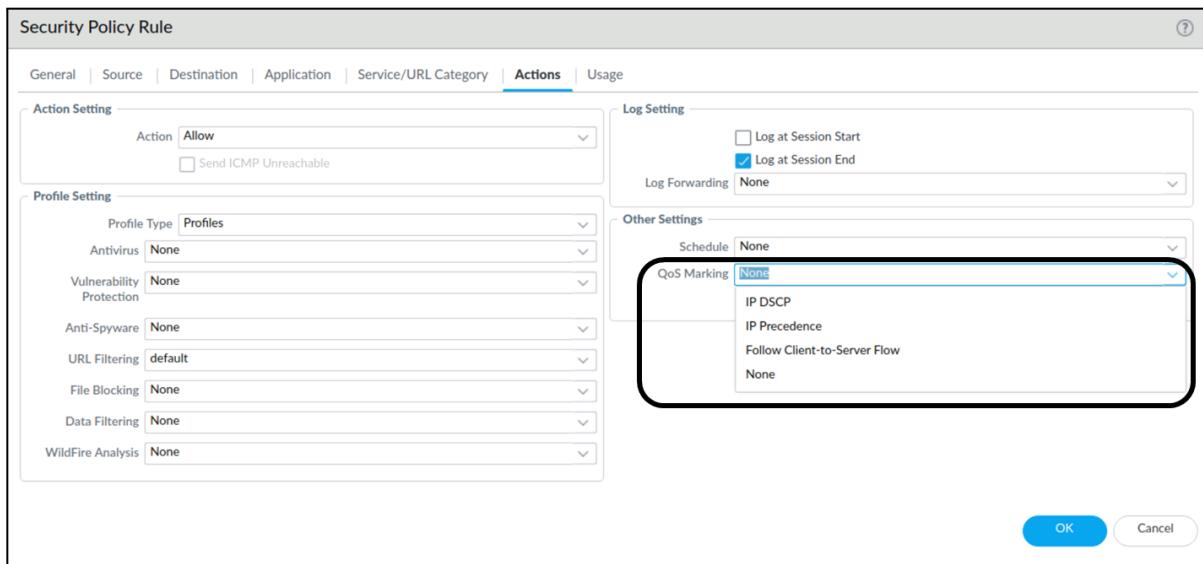
Palo Alto Networks QoS provides an “application-aware” QoS service that can be driven by the traffic’s App-ID. The firewall’s QoS implementation is a self-contained system local to the firewall that can consider existing QoS packet markings but does not act directly on them. Traffic is evaluated against QoS policy rules, including existing QoS packet markings, App-ID, and other matching conditions, to assign a traffic classification value of 1 through 8. These values are the basis for QoS decision making. QoS traffic control is limited to egress traffic for the configured interface(s) only. Ingress traffic cannot be managed.

The interrelationship between the QoS policies, traffic classes, QoS Profiles, and interfaces is displayed in the following figure:



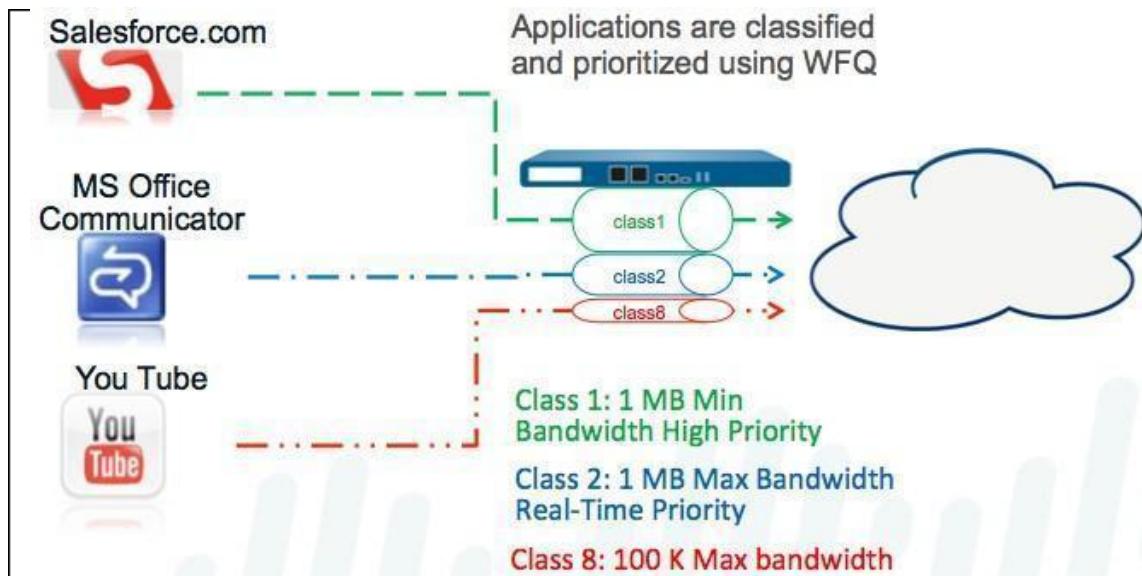
### 2.11.2 QoS policy rule

Use the QoS Marking field when setting up a Security policy rule to write QoS marking into packet headers. This will apply to any traffic that the Security policy rule processes. Note that this marking is not directly related to QoS processing in the firewall.



QoS implementation on a Palo Alto Networks firewall begins with three primary configuration components that support a full QoS solution: a QoS policy, a QoS Profile, and configuration of the QoS egress interface. Each option in the QoS configuration task facilitates a broader process that optimizes and prioritizes the traffic flow and allocates bandwidth according to configurable parameters.

QoS policies assign traffic classes (1 to 8) to traffic that matches the policy conditions. PAN-OS QoS functionality can use App-ID for specific bandwidth reservation.



### 2.11.3 Add Differentiated Services Code Point/ToS component

A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request (for example) high priority or best effort delivery for traffic. Session-based DSCP classification allows you to both honor DSCP values for incoming traffic and to mark a session with a DSCP value as session traffic exits the firewall. This enables all inbound and outbound traffic for a session to receive continuous QoS treatment as it flows through your network. For example, inbound return traffic from an external server can now be treated with the same QoS priority that the firewall initially enforced for the outbound flow based on the DSCP value the firewall detected at the beginning of the session. 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).

Different types of DSCP markings indicate different levels of service:

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.

**Expedited Forwarding (EF):** Can be used to request low loss, low latency, and guaranteed bandwidth for traffic. Packets with EF codepoint values 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:** 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:** Can be used to match to traffic by entering a codepoint name and binary value.

For example, select **AF** to ensure that traffic marked with an AF codepoint value has higher priority for reliable delivery over applications marked to receive lower priority. 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.

### 2.11.4 QoS profile

QoS Profiles describe the priority to be given to the specified traffic when the interface becomes constrained. As priority decreases, more packets are randomly dropped until the constraint is cleared. The number of

packets dropped is determined by their assigned priority. A real-time priority setting means that no packet dropping will be performed. High-, medium-, and low-priority settings indicate that greater levels of random packet dropping will be performed during movement down the scale. No packets will be dropped until the egress traffic on the managed interface becomes constrained, meaning that outbound traffic queues for the interface will fill faster than they can be emptied.

Profiles also specify the maximum bandwidth enforcement that is always applied. Bandwidth that is configured as the maximum limit can be used by all traffic until the interface becomes constrained. After an interface is constrained, sessions might receive no more than their guaranteed bandwidth.

QoS Profiles prioritize specified traffic. The following figure shows the four possible priority values:

NAME	GUARANTEED EGRESS	MAXIMUM EGRESS	PRIORITY
default			
class1			real-time
class2			high
class3			high
class4			medium
class5			medium
class6			low
class7			low
class8			low

## 2.11.5 Determine how to control bandwidth use on a per-application basis

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 the following 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, partners, and customers. An IT administrator intends to implement QoS to address these issues and ensure effective and reliable business communication for branch employees. Because the administrator 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.

**Step 1:** The administrator creates a QoS Profile that defines Class 2 so that Class 2 traffic receives real-time priority on an interface with a maximum bandwidth of 1,000Mbps. Class 2 is also guaranteed a bandwidth of 250Mbps at all times, including peak periods of network usage.

Real-time priority is typically recommended for applications affected by latency. It's particularly useful in guaranteeing performance and quality of voice and video applications.

On the firewall web interface, the administrator selects **Network > Network Profiles > QoS Profile**, clicks **Add**, enters the **Profile Name** as **ensure voip-video traffic**, and defines Class 2 traffic.

CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
class2	real-time	1000	250

**Step 2:** The administrator creates a QoS policy to identify voice and video traffic. Because the company does not have one standard voice and video application, the administrator wants to ensure that QoS is applied to a few applications that are widely and regularly used by employees to communicate with other offices, partners, and customers. On the **Policies > QoS > QoS Policy Rule > Applications** tab, the administrator clicks **Add** and opens the **Application Filter** window. The administrator 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.

**Application Filter**

NAME: voip-video-low-risk    Shared    Apply to New App-IDs only    Clear Filters   15 matching applications

CATEGORY	SUBCATEGORY	TECHNOLOGY	RISK	TAGS	CHARACTERISTIC
15 collaboration	15 voip-video	1 browser-based 6 client-server 8 peer-to-peer	15 [1]	4 Enterprise VoIP 0 G Suite 0 Palo Alto Networks 12 Web App 0 Bandwidth heavy	/ NO CERTIFICATIONS 1 Poor Financial Viability 3 Poor Terms Of Service 9 SaaS 1 SOC I 1 SOC II 2 Vulnerability 15 Widely used

NAME	CATEGORY	SUBCATEGORY	TECHNOLOGY	RISK	TAGS	STANDARD PORTS	EXCLUDE
facebook (1 out of 10 shown)	collaboration	voip-video	peer-to-peer	1	Web App	443,tcp	<input checked="" type="checkbox"/>
facebook-voice	collaboration	voip-video	peer-to-peer	1	Web App	443,tcp	<input checked="" type="checkbox"/>
foonz	collaboration	voip-video	browser-based	1		80,tcp	<input checked="" type="checkbox"/>
fring	collaboration	voip-video	client-server	1	Web App	dynamic,tcp,udp	<input checked="" type="checkbox"/>
google-duo	collaboration	voip-video	peer-to-peer	1	Web App	19305,443,tcp,udp	<input checked="" type="checkbox"/>

Page 1 of 1 | Displaying 1 - 20 of 20

Show Technology Column     

The administrator names the application filter **voip-video-low-risk** and includes it in the QoS policy:

**QoS Policy Rule**

General | Source | Destination | **Application** | Service/URL Category | DSCP/ToS | Other Settings

Any

APPLICATIONS

voip-video-low-risk

The administrator names the QoS policy **Voice-Video**, and selects **Other Settings** to assign all traffic matched to the policy Class 2. 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**:

NAME	TAGS	Source				Destination				APPLICATION	SERVICE	DSCP/TOS	CLASS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1 HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	any	2
2 Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	any	1

**Step 3:** Because the administrator 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 administrator begins by enabling the QoS Profile he created, **ensure voice-video traffic**, on the external-facing interface — in this case, **ethernet 1/2**.

The screenshot shows the 'QoS Interface' configuration dialog. At the top, there are tabs for 'Physical Interface', 'Clear Text Traffic', and 'Tunneled Traffic'. The 'Physical Interface' tab is selected. Under 'Physical Interface', the 'Interface Name' is set to 'ethernet1/2', 'Egress Max (Mbps)' is set to '1000', and the checkbox 'Turn on QoS feature on this interface' is checked. In the 'Default Profile' section, under 'Clear Text', the profile 'ensure voip-video traffic' is selected. At the bottom right are 'OK' and 'Cancel' buttons.

He then enables the same QoS Profile, **ensure voip-video traffic**, on a second interface: the internal-facing interface (in this case, **ethernet 1/1**).

**QoS Interface**

**Physical Interface** | Clear Text Traffic | Tunneled Traffic

Interface Name	ethernet1/1
Egress Max (Mbps)	1000
<input checked="" type="checkbox"/> Turn on QoS feature on this interface	
<b>Default Profile</b>	
Clear Text	ensure voip-video traffic
Tunnel Interface	None

**OK**    **Cancel**

**Step 4:** The administrator selects **NetworkQoS** to confirm 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"/>	<a href="#">Statistics</a>
🔗 Tunneled Traffic					
📝 Clear Text Traffic	250.000		ensure voip-video traffic		
ethernet1/2		1,000.000		<input checked="" type="checkbox"/>	<a href="#">Statistics</a>
🔗 Tunneled Traffic					
📝 Clear Text Traffic	250.000		ensure voip-video traffic		

The administrator 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 can be used reliably and effectively to perform both internal and external business communications.

### 2.11.6 Use QoS to monitor bandwidth utilization

QoS bandwidth management allows you to control traffic flows on a network so that traffic does not exceed network capacity and result in network congestion. It also allows you to allocate bandwidth for certain types of traffic and for applications and users. With QoS, you can enforce bandwidth for traffic on a narrow scale or a broad scale. A QoS Profile rule allows you to set bandwidth limits for individual QoS classes and the total combined bandwidth for all eight QoS classes. As part of the steps to [configure QoS](#), you can attach the QoS Profile rule to a physical interface to enforce bandwidth settings on the traffic exiting that interface; the individual QoS class settings are enforced for traffic matching that QoS class are assigned to traffic

matching QoS policy rules. The overall bandwidth limit for the profile can be applied to all cleartext traffic, specific cleartext traffic originating from source interfaces and source subnets, all tunneled traffic, and individual tunnel interfaces. You can add multiple profile rules to a single QoS interface to apply varying bandwidth settings to the traffic exiting that interface.

Egress guaranteed and egress max support QoS bandwidth settings.

### **Egress Guaranteed**

**Egress guaranteed specifies** the amount of bandwidth guaranteed for matching traffic. When the egress guaranteed bandwidth is exceeded, the firewall passes traffic on a best-effort basis. Bandwidth that is guaranteed but is unused continues to remain available for all traffic. Depending on your QoS configuration, you can guarantee bandwidth for a single QoS class, for all or some cleartext traffic, and for all or some tunneled traffic.

**Example:** Class 1 traffic has 5Gbps of egress guaranteed bandwidth, which means that 5Gbps is available but is not reserved for Class 1 traffic. If Class 1 traffic does not use or only partially uses the guaranteed bandwidth, the remaining bandwidth can be used by other classes of traffic. However, during high-traffic periods, 5Gbps of bandwidth is absolutely available for Class 1 traffic. During these periods, any Class 1 traffic that exceeds 5Gbps is passed on a best-effort basis.

### **Egress Max**

**Egress max specifies** the overall bandwidth allocation for matching traffic. The firewall drops traffic that exceeds the egress max limit that you set. Depending on your QoS configuration, you can set a maximum bandwidth limit for a QoS class, for all or some cleartext traffic, for all or some tunneled traffic, and for all traffic exiting the QoS interface.

## **2.11.6 References**

QoS policy rule:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service/enforce-qos-based-on-dscp-classification>

Quality of Service:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service>

QoS Bandwidth Management:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service/qos-concepts/qos-bandwidth-management>

Use Case: QoS for Voice and Video Applications:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service/qos-use-cases/use-case-qos-for-voice-and-video-applications>

## 2.11.7 Sample Questions

1. Which parameter is important for QoS policy match decisions?
  - a. App-ID
  - b. Content-ID
  - c. User-ID
  - d. ingress interface
2. What is the maximum number of QoS classes supported by the next-generation firewall?
  - a. 4
  - b. 8
  - c. 16
  - d. 32
3. In a site-to-site VPN configuration, what is an alternative method to the use of preshared keys to authenticate each device during connection setup?
  - a. certificates
  - b. expected IP address of the partner's interface
  - c. known hexadecimal string configured in both endpoints
  - d. matching proxy ID definitions configured in both endpoints
4. Which type of firewall interface can be associated with a tunnel interface?
  - a. tap
  - b. virtual wire
  - c. Layer 2
  - d. Layer 3
5. A firewall administrator is deploying 50 Palo Alto Networks firewalls to protect remote sites. Each firewall must have a site-to-site IPsec VPN tunnel to each of three campus locations. Which configuration function is the basis for automatic site-to-site IPsec tunnels set up from each remote location to the three campuses?
  - a. import of a settings table into the remote firewall's IPsec tunnel configuration
  - b. import of a settings table into the IPsec tunnel configuration of the three campuses
  - c. configuration of the GlobalProtect satellite settings of the campus and remote firewalls
  - d. entry of campus IPsec tunnel settings for each remote firewall's IPsec Profile

# Domain 3- Deploy and Configure Features and Subscriptions

## 3.1 Configure App-ID

### 3.1.1 Create Security rules with App-ID

#### *Security Policy Overview*

The firewall will not allow any traffic to flow from one zone to another unless there is a Security policy rule to allow it. When a packet enters a firewall interface, the firewall matches the attributes in the packet against the Security policy rules to determine whether to block or allow the session based on attributes such as the source and destination security zone, the source and destination IP address, the application, the user, and the service. The firewall evaluates incoming traffic against the Security policy rulebase from left to right and from top to bottom. Then, it takes the action specified in the first Security rule that matches (for example, whether to allow, deny, or drop the packet). Because processing occurs from top to bottom, you must order the rules in your Security policy rulebase so that more specific rules are at the top of the rulebase and more general rules are at the bottom. This ensures that the firewall enforces policy as expected.

#### *Configuring Security rules*

A Security policy allows you to enforce rules and actions. It can be as general or specific as needed. The policy rules are compared against the incoming traffic in sequence. Because the first rule that matches the traffic is applied, more specific rules must precede more general rules. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same.

Security policy rules are matched from the top down. Up to two processing steps are in each Security policy match. Step 1 confirms that a match has been made based on the matching conditions provided in the Security policy. If a match is found in Step 1, the traffic is logged (based on that policy rule's configuration) and the chosen action (deny, allow, drop, reset) is performed. Once processing is complete, there will be no further matching in the Security policy rulebase.

#### *Security Policy: Allow*

If the action is allow, Step 2 of the policy is evaluated. Step 2 is the application of configured Security Profiles. In Step 2, the content of sessions is scanned for various threat signatures. In this step, URLs can also be scanned for unauthorized destinations and files can be scanned for malware.

If Panorama device groups are used to push Security policy to one or more firewalls, the Security policy list is expanded to include rules before (pre) and after (post) the local firewall rules. Panorama rules are merged with local firewall policies in the position chosen during Panorama rule creation. Panorama-supplied rules are read-only to local firewall administrators. The Security policy rule list displayed in the following screenshot is for a local administrator logged directly into a managed firewall.

The diagram illustrates the evaluation flow of security policy rules. It shows four categories of rules on the left, each pointing to specific rows in a table of 10 rules:

- Pre rules from Panorama** points to rows 1 and 2.
- Local rules created directly in the firewall** points to row 3.
- Post rules from Panorama** points to rows 4 through 8.
- Default rules from Panorama** points to rows 9 and 10.

**Table of Security Policy Rules:**

NAME	Source	Destination	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	ZONE	ZONE					
1 Block_Bad_IPs_Inbound	Internet	Extranet	any	application-default	Deny	none	
		Users_Net					
2 Block_Bad_IPs_Outbound	Extranet	Internet	any	application-default	Deny	none	
		Internet					
3 Local-Allow Facebook	Internet	Internet	facebook	application-default	Allow	QoS, Log, SSL, Web, Firewall	
			mqtt				
			rtp				
			rtp-base				
			ssl				
			stun				
			web-browsing				
4 Users_to_Extranet	Users_Net	Extranet	any	any	Allow	Log	
5 Extranet_to_Internet	Extranet	Internet	any	application-default	Allow	Log	
6 Extranet_to_Users_Net	Extranet	Users_Net	any	application-default	Allow	none	
7 Danger_Traffic	Danger	any	any	application-default	Allow	Log	
8 Allow-Internet-Access	Users_Net	Internet	any	application-default	Allow	Log	
9 intrazone-default	any	(intrazone)	any	any	Allow	Log	
10 interzone-default	any	any	any	any	Deny	none	

Security policy should use App-ID for match criteria rather than only services (ports).

At the end of the list are two default policy rules: one for an intrazone allow and one for an interzone deny. Together, they implement the default security behavior of the firewall to block interzone traffic and allow intrazone traffic. By default, traffic logging is disabled in both rules.

Security policy rules in PAN-OS are configured by type: universal (default), interzone, and intrazone. (All policy rules – regardless of type – are evaluated top down, first match, then exit.) The universal type covers both interzone and intrazone.

**Security Policy Rule**

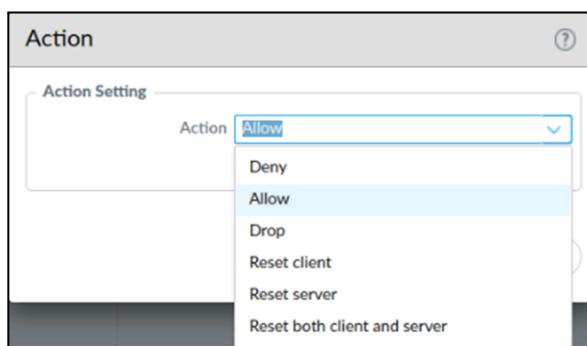
General	Source	Destination	Application	Service/URL Category	Actions
Name					
Rule Type	universal (default)				
Description	universal (default)				
Tags					
Group Rules By Tag	None				
Audit Comment					
<a href="#">Audit Comment Archive</a>					

The Security policy **Rule Type** selects the type of traffic the policy applies to.

Throughput performance does not change based on how quickly a match is made. Because evaluation is top down, first match, then exit, exceptions to policy rules must appear before the general policy. Beyond this policy, order is based on administrative preference. Use tags, a policy search bar, or a global find to quickly navigate to the policy or policy rules needed for troubleshooting and moves, adds, changes, deletes, and clones.

### **Security Policy: Deny**

The deny action is a legacy setting from prior versions of PAN-OS, when denying traffic was the only way to stop traffic. Before PAN-OS 7, the software referenced the App-ID database to find the preferred method of stopping traffic for the matching session's application, which ranged from blocking to reset. These choices now have been added directly to the list of action choices available. Firewall administrators now can choose the desired blocking action directly, or they can continue to rely on the Palo Alto Networks specification by choosing **Deny**.



## **App-ID vs. Port-Based Security**

Security policy rules that evaluate based on protocol type and port numbers are not accurate enough to effectively control application access through your firewall. Many applications use alternative or even multiple port numbers, making their detection even more difficult. For instance, allowing TCP port 80 provides access for all web-based applications — and their associated vulnerabilities.

Palo Alto Networks App-ID enables positive application identification, regardless of port usage. App-ID allows you to safely enable access to only those applications that you want users to reach. This practice reduces your attack surface by eliminating unauthorized applications and their potential vulnerabilities.

### **Note About Using App-ID**

Because applications often can use non-standard ports for communication, a traffic enforcement technology based only on port numbers does not provide security administrators enough control over the actual application traffic entering their organizations. Because App-ID identifies applications based primarily on packet contents and not on port numbers, it provides a much higher level of capability. When you use Palo Alto Networks firewalls, your Security policy rules should use App-ID as selection criteria, not port numbers.

### **3.1.2 Convert port and protocol rules to App-ID rules**

#### **Moving from Port-Based to App-ID Security**

Moving from a port-based Security policy to an application-based Security policy may seem like a daunting task. However, the security risks of staying with a port-based policy far outweigh the effort required to implement an application-based policy. And, although legacy port-based Security policies may have thousands of rules (many of which have an unknown purpose), a best practice policy has a streamlined set of rules that aligns with your business goals, simplifying administration and reducing the chance of error. Because the rules in an application-based policy align with your business goals and acceptable use policies, you can quickly scan the policy to understand the reason for every rule.

As with any technology, organizations usually take a gradual approach to implementation with carefully planned deployment phases to make the transition as smooth as possible, with minimal impact to end users. The general workflow for implementing a best practice internet gateway Security policy is as follows:

- **Assess your business and identify what you need to protect:** The first step in deploying a security architecture is to assess your business and identify your most valuable assets — and the greatest threats to those assets. For example, if you are a technology company, your intellectual property is your most valuable asset. In this case, one of your biggest threats would be source code theft.
- **Segment your network using interfaces and zones:** Traffic cannot flow between zones unless there is a Security policy rule to allow it. One of the easiest defenses against lateral attacker movement is to define granular zones and allow access only to the specific user groups that need to access an application or resource in each zone. By segmenting your network into granular zones, you can prevent an attacker from establishing a communication channel within your network (either via malware or by exploiting legitimate applications), thereby reducing the likelihood of a successful attack on your network.

- **Identify allow list applications:** Before you can create an internet gateway best practice Security policy, you must have an inventory of the applications that you want to allow on your network. You must also distinguish between those applications that you administer and officially sanction and those that you want users to be able to use safely. After you identify the applications (including general types of applications) that you want to allow, you can map them to specific best practice rules.
- **Create user groups for access to allow list applications:** After you identify the applications that you plan to allow, you must identify the user groups that require access to each one. Because compromising an end user's system is one of the cheapest and easiest ways for an attacker to gain access to your network, you can greatly reduce your attack surface by allowing access only to applications to the user groups that have a legitimate business need.
- **Decrypt traffic for full visibility and threat inspection:** You cannot inspect traffic for threats if you cannot see it in cleartext. Today, SSL/TLS traffic flows account for 40 percent or more of the total traffic on a typical network, which is precisely why encrypted traffic is a common way for attackers to deliver threats. For example, an attacker may use a web application such as Gmail, which uses SSL encryption, to email an exploit or malware to employees accessing that application on the corporate network. Or, an attacker may compromise a website that uses SSL encryption to silently download an exploit or malware to site visitors. If you are not decrypting traffic for visibility and threat inspection, you are leaving a large surface open for attack.
- **Create best practice Security Profiles for the internet gateway:** C2 traffic, Common vulnerabilities and exposures (CVEs), drive-by downloads of malicious content, phishing attacks, advanced persistent threats — all are delivered via legitimate applications. To protect against known and unknown threats, you must attach stringent Security Profiles to all Security policy allow rules.
- **Define the initial internet gateway Security policy:** Using the application and user group inventory that you conducted, you can define an initial policy that allows access to all the applications you want to allow by user or user group. The initial policy rulebase that you create also must include rules for blocking known malicious IP addresses, temporary rules to prevent other applications you might not have known about from breaking, and identification of policy gaps and security holes in your design.
- **Monitor and fine-tune the policy rulebase:** After the temporary rules are in place, you can begin monitoring traffic that matches to them so that you can fine-tune your policy. Because the temporary rules are designed to uncover unexpected traffic on the network (such as traffic running on non-default ports or traffic from unknown users), you must assess the traffic matching these rules and adjust your application allow rules accordingly.
- **Remove the temporary rules:** After a monitoring period of several months, you should see less and less traffic hitting the temporary rules. When you reach the point where traffic no longer hits the temporary rules, you can remove them.
- **Maintain the rulebase:** Because applications are dynamic, you must continually monitor your application allow list and adapt your rules to accommodate new applications and to determine how new or modified App-IDs impact your policy. Because the rules in a best practice rulebase align with

your business goals and leverage policy objects, adding support for a new sanctioned application or new or modified App-ID often is as simple as adding or removing an application from an application group or modifying an application filter.

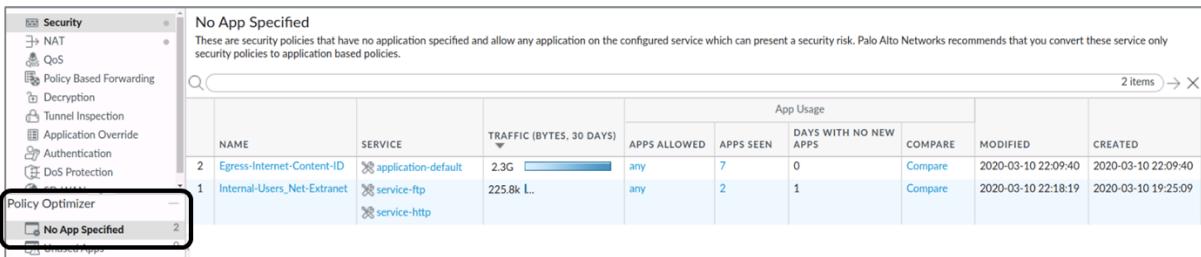
Palo Alto Networks has developed an innovative approach to securing networks that identifies all traffic by applications. This approach replaces conventional approaches that attempt to control traffic based on port numbers.

### **Port-Based Rules**

When you transition from a legacy firewall to a Palo Alto Networks NGFW, you inherit many port-based rules that allow any application on the allowed ports. This increases the attack surface because any application can use an open port. Policy Optimizer identifies all applications seen on any legacy port-based Security policy rule and provides an easy workflow for selecting the applications you want to allow on that rule. You can migrate port-based rules to application-based allow list rules to reduce the attack surface and safely enable applications on your network. Use Policy Optimizer to maintain the rulebase as you add new applications.

### **Step 1: Identify port-based rules**

Port-based rules have no configured (allow list) applications. **Policies > Security > Policy Optimizer > No App Specified** displays all port-based rules.



The screenshot shows the 'Policy Optimizer' section under 'Security'. A callout box highlights the 'No App Specified' link. The main table lists two port-based rules:

NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	App Usage			MODIFIED	CREATED
			APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS		
Egress-Internet-Content-ID	application-default	2.3G	any	7	0	Compare	2020-03-10 22:09:40
Internal-Users_Net-Extranet	service-ftp service-http	225.8k L..	any	2	1	Compare	2020-03-10 22:18:19

### **Step 2: Prioritize which port-based rules to convert first**

**Policies > Security > Policy Optimizer > No App Specified** enables you to sort rules without affecting their order in the rulebase. It also provides other information that helps you prioritize rules for conversion based on your business goals and risk tolerance. This information includes:

- **Traffic (Bytes, 30 days):** Displays rules with applications transferring the most data, which appear at the top of the list. Rules with applications transferring less data are shown at the bottom. This is the default application sorting order. (Click to reverse the sort order.)
- **Apps Seen:** Many legitimate applications matching a port-based rule may indicate that you should replace it with multiple application-based rules that tightly define the applications, users, sources, and destinations. For example, if a port-based rule controls traffic for multiple applications for different user groups on different sets of devices, create separate rules that pair applications with their legitimate users and devices to reduce the attack surface and increase visibility. (Click to sort. Also, click the **Apps Seen** number or **Compare** to display the applications that have matched the rule.)

- **Days with No New Apps:** When the applications seen on a port-based rule stabilize, you can be more confident that the rule is mature, that conversion will not accidentally exclude legitimate applications, and that no more new applications will match the rule. The **Created** and **Modified** dates help you evaluate a rule's stability; older rules that have not been modified recently also may be more stable. (Click to reverse the sort order.)
- **Hit Count:** Displays rules with the most traffic matches over a selected time frame. You can exclude rules for which you reset the hit counter and specify the exclusion time period in days. Exclusion of rules with recently reset hit counters prevents misconceptions about rules that show fewer hits than you expect because you did not know the counter was reset.

### *Step 3: Review Apps Seen on port-based rules with highest priority*

On **No Apps Specified**, click **Compare** or the number in **Apps Seen** to open **Applications & Usage**, which lists applications that matched a port-based rule over a specified time frame, with each application's **Risk**, the date it was **First Seen**, the date it was **Last Seen**, and the amount of traffic over the last 30 days.

The screenshot shows the 'Applications & Usage - Internal-Users\_Net-Extranet' window. At the top, there is a 'Timeframe' dropdown set to 'Anytime'. Below it, a table header reads 'Apps on Rule' and 'Apps Seen 2'. The table has columns: APPLICATIONS, SUBCATEG..., RISK, FIRST SEEN, LAST SEEN, and TRAFFIC (30 DAYS). Two rows are listed: 'web-browsing' (internet-utility, Risk 4) and 'ftp' (file-sharing, Risk 5). Both rows have a blue checkmark in the first column. At the bottom of the table, there are buttons for 'Browse', 'Add', 'Delete', 'Create Cloned Rule', 'Add to This Rule', 'Add to Existing Rule', and 'Match Usage'.

Apps on Rule		Apps Seen 2					
<input checked="" type="checkbox"/> Any	<input type="checkbox"/> APPLICATIONS ▲	APPLICATIONS	SUBCATEG...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS) ▾
<input type="checkbox"/>	web-browsing	internet-utility	4	2020-03-10	2020-03-11	210.8k	
<input checked="" type="checkbox"/>	ftp	file-sharing	5	2020-03-10	2020-03-10	15.1k	

You can check applications seen on port-based rules over the past **7**, **15**, or **30** days, or over the rule's lifetime (**Anytime**). For migrating rules, **Anytime** provides the most complete assessment of applications that matched the rule.

You can search and filter Apps Seen, but remember that an hour or more is required to update Apps Seen. You also can order Apps Seen by clicking the column headers. For example, you can click **Traffic (30 days)** to bring the applications with the most recent traffic to the top of the list, or click **Subcategory** to organize the applications by subcategory.

### *Step 4: Clone or add apps to the rule*

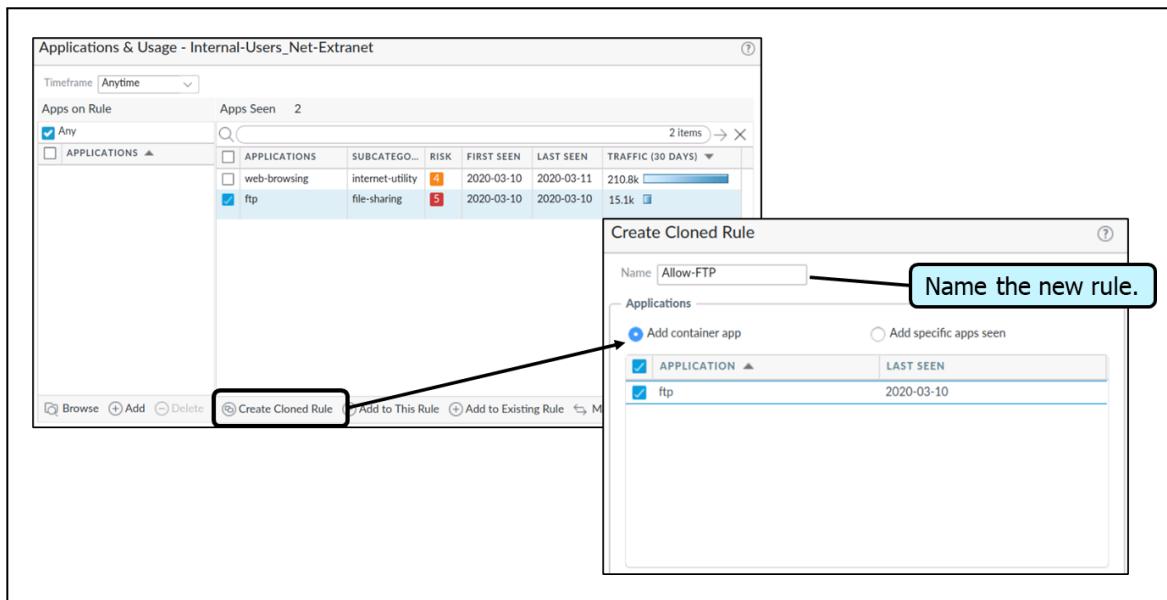
On **Applications & Usage**, convert a port-based rule to an application-based rule by doing the following:

- **Cloning the rule:** Preserves the original port-based rule and places the cloned application-based rule directly above it in the port-based rule
- **Adding applications to the rule:** Replaces the original port-based rule with the new application-based rule and deletes the original rule

Cloning is the safest way to migrate rules, especially when Applications & Usage shows more than a few well-known applications matching the rule. Cloning preserves the original port-based rule and places it below the cloned application-based rule, which eliminates the risk of losing application availability because traffic that does not match the cloned rule flows through to the port-based rule. When traffic from legitimate applications has not hit the port-based rule for a reasonable period of time, you can remove it to complete that rule's migration.

Follow these steps to clone a port-based rule:

- In **Apps Seen**, click the check box next to each application that you want in the cloned rule. Remember that an hour or more is required to update Apps Seen.
- Click **Create Cloned Rule**. In the Create **Cloned Rule** dialog, **Name** the cloned rule. Add other **Applications** in the same container and application dependencies, if required. The following figure shows how to clone a rule by selecting the slack-base application:



In the **Clone** window, the green row is the selected application to clone. The container application (**slack**) is in the gray row. The applications listed in italics are applications in the same container as the selected application but that have not been seen on the rule. Individual applications that have been seen on the rule are in normal font. All the applications are included in the cloned rule by default to help prevent the rule from breaking.

- If the container app is a *tolerated* application (i.e., not an application sanctioned for business purposes) and you want to constrain access to some of the individual functional applications in the container, uncheck the box next to each individual application that you do not want users to access. If the container app is a sanctioned business application, add the container app and its individual applications.
- Leave the application dependencies checked. These are applications that the selected application requires — in this example, **ssl** and **web-browsing**.
- Click **OK** to add the new application-based rule directly above the port-based rule in the rulebase.
- Commit the configuration.

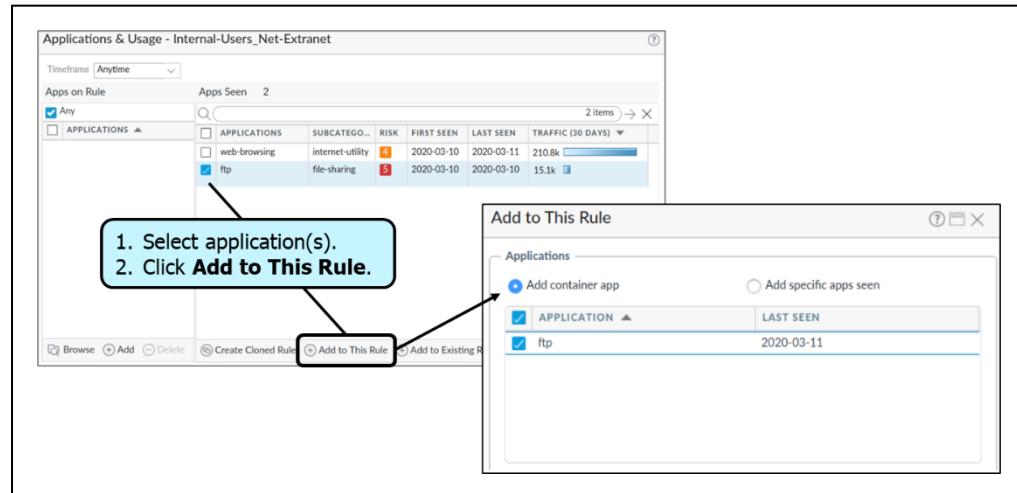
After you clone a rule and commit the configuration, the applications that you select for the cloned rule are removed from the original port-based rule's Apps Seen list. For example, if a port-based rule has 16 Apps Seen and you select two individual applications and one dependent application for the cloned rule, after cloning, the port-based rule shows 13 Apps Seen because the three selected applications have been removed from the port-based rule ( $16 - 3 = 13$ ). The cloned rule shows the three added applications in **Apps on Rule**.

Creation of a cloned rule with a container app works differently. For example, let's say a port-based rule has 16 Apps Seen and you select one individual application and a container app for the cloned rule. The container app has five individual applications and one dependent application. After cloning, the cloned rule shows seven Apps on Rule: the individual application, the five individual applications in the container app, and the dependent application for the container app. However, in the original port-based rule, Apps Seen shows 13 applications because only the individual application, the container app, and the container app's dependent application are removed from the port-based rule.

Unlike with cloning, adding applications to a port-based rule replaces the rule with the resulting application-based rule. Adding applications to a rule is simpler than cloning, but it is also riskier. You may inadvertently miss applications that should be on the rule, and the original port-based rule is not in the rulebase to identify accidental omissions. However, adding applications to port-based rules that apply to only a few well-known applications migrates the rule quickly to an application-based rule. For example, for a port-based rule that controls only traffic to TCP port 22, the only legitimate application is SSH, so it is safe to add applications to the rule.

There are three ways to add applications to replace a port-based rule with an application-based rule: using Add to This Rule, using Match Usage in Apps Seen, and using Add in Apps on Rule:

- **Add to This Rule: Adds applications** from Apps Seen (applications that matched the rule). Remember that an hour or more is required to update Apps Seen.
  - Select applications from **Apps Seen** on the rule.
  - Click **Add to This Rule**. In the **Add to This Rule** dialog, add other applications in the same container app and application dependencies, if required. For example, to add slack-base to a rule:



Like with the Clone dialog, the green row in the Add to Rule dialog is the selected application to add to the rule. The container app (slack) is in the gray row. The applications listed in italics are applications in the same container that have not been seen on the rule. Individual applications that have been seen on the rule are in normal font. All the applications are included in the new rule by default to help prevent the rule from breaking.

- If you are sure that the italicized applications in the container that have not been seen on the rule will never be seen on the rule, you can uncheck the box next to them so they are not included in the rule. If you uncheck a container app, its individual applications also are unchecked.
- Leave the application dependencies checked. These are applications that the selected application requires — in this example, **ssl** and **web-browsing**.
- Click **OK** to replace the port-based rule with the new application-based rule.
- When you **Add to Rule** and **Commit** the configuration, the applications that you did not add are removed from Apps Seen because the new application-based rule no longer allows them. For example, if a rule has 16 Apps Seen and you Add to Rule three applications, the resulting new rule shows only those three added applications in Apps Seen.
- Add to Rule with a container app works differently. For example, let's say a port-based rule has 16 Apps Seen and you select one individual application and a container app to add to the new rule. The container app has five individual applications and one dependent application. After you add the applications to the rule, the new rule shows seven Apps on Rule: the individual application, the five individual applications in the container app, and the dependent application for the container app. However, Apps Seen shows 13 applications because the individual application, the container app, and the container app's dependent application are removed from that list.
- Match Usage in Apps Seen: Adds all the Apps Seen on the rule to the rule at one time with one click. To use this method:

- In **Apps Seen**, click **Match Usage**. (Remember that an hour or more is required to update Apps Seen.) All the applications in Apps Seen are copied to **Apps on Rule**.
  - Click **OK** to create the application-based rule and replace the port-based rule.
- Add in Apps on Rule: Adds applications manually. You can use this method if you know the applications that you want on the rule. To use this method:
  - In **Apps on Rule**, click **Add** (or **Browse**) and select applications to add to the rule.
  - Click **OK** to add the applications to the rule and replace the port-based rule with the new application-based rule.
  - This method is equivalent to using the traditional Security policy rule Application tab, and it does not change Apps Seen or Apps on Rule. To preserve accurate application usage information, convert rules using Add to Rule, Create Cloned Rule, or Match Usage in Apps Seen.

#### ***Step 5: For each application-based rule, set the service to application-default***

If business needs require you to allow applications (e.g., internal custom applications) on non-standard ports between clients and servers, restrict the exception to only the required application, sources, and destinations. Consider rewriting custom applications so they use the application default port.

#### ***Step 6: Commit the configuration***

#### ***Step 7: Monitor the rules***

- **Cloned rules:** Monitor the original port-based rule to ensure that the application-based rule matches the desired traffic. If applications that you want to allow match the port-based rule, add them to the application-based rule or clone another application-based rule for them. When only applications that you do not want on your network match the port-based rule for a reasonable period of time, the cloned rule is robust (it catches all the application traffic you want to control). You can safely remove the port-based rule.
- **Rules with added applications:** Because you convert only port-based rules that have a few well-known applications directly to application-based rules, in most cases, the rule operates properly from the beginning. Monitor the converted rule to see if the expected traffic matches the rule. If there is less traffic than expected, the rule may not allow all the necessary applications. If there is more traffic than expected, the rule may allow unwanted traffic. Listen to user feedback. If users cannot access the applications that they need for business purposes, the rule (or another rule) may be too restrictive.

### **3.1.3 Identify the impact of application override to overall firewall functionality**

#### ***Application Override Configuration***

To change how the firewall classifies network traffic into applications, you can specify Application Override policy rules. These policy rules attach the specified App-ID to matching traffic and bypass the normal App-ID processing steps in the firewall. This assigned application functions identically to an App-ID supplied

application name and can be used in the same way. For example, if you want to control one of your custom applications, you can use an Application Override policy to identify traffic for that application according to zone, source, destination address, port, and protocol. After an Application Override rule has assigned a custom application name to network traffic, that traffic can be controlled by the firewall through use of the custom application name in a Security policy rule.

Note that the App-ID bypass characteristic of Application Override also skips essential Content-ID processing, which could result in undetected threats. This feature should be used for trusted traffic only.

### 3.1.4 Create custom apps and threats

To make sure that your internal custom apps do not appear as “unknown traffic,” you’ll need to create a custom app. Creating a custom app allows you to minimize the range of incoming unidentified traffic on your network.

To create a custom app, you must define the app attributes:

- Characteristics
- Category and subcategory
- Risk
- Timeout
- Port

You also must define patterns or values that the PAN-OS firewall can use to match to the traffic flows themselves (app signatures).

### 3.1.5 Review App-ID dependencies

You now have simplified workflows to find and manage any application dependencies. These workflows allow you to see application dependencies when you create a new Security policy rule and when performing commits. When a policy does not include all application dependencies, you can directly access the associated Security policy rule to add the required applications.

Using these workflows along with Policy Optimizer, you can now more easily identify, organize, and resolve application dependencies. You can take advantage of the new workflows by upgrading your Panorama management server to 9.1 and pushing rules to your firewalls. [Resolve Application Dependencies](#) provides detailed steps.

**Step 1:** Create a [security policy rule](#).

**Step 2:** Specify the application that the rule will allow or block.

**Step 3:** Click **OK** and **Commit** your changes:

1. Review any commit warnings in the **App Dependency** tab.

2. Select the **Rule name** to open the policy and add the dependencies.
3. Click **OK** and **Commit** your changes.

### 3.1.6 References

Custom Application and Threat Signatures:

<https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures>

Policies > Application Override:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/policies/policies-application-override>

Defining Applications:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-applications/defining-applications>

Policies > Security:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/policies/policies-security>

Set Up a Basic Security Policy:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/getting-started/set-up-a-basic-security-policy>

Internet Gateway Best Practice Security Policy:

<https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices>

Create Best Practice Security Profiles for the Internet Gateway:

<https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles>

Example Web-Based App-ID Listing:

<https://applipedia.paloaltonetworks.com/>

Create a Custom Application Signature:

<https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures/create-a-custom-application-signature>

Resolve Application Dependencies:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies>

### 3.1.7 Sample Questions

1. Which option is not a parameter that is used to identify applications in an Application Override policy?

- a. protocol
  - b. port number
  - c. first characters in the payload
  - d. destination IP address
2. How does the firewall resolve conflicting App-ID assignments to the same traffic between an Application Override policy rule and the firewall's built-in App-ID?
- a. The firewall's regular App-ID is assigned.
  - b. The Application Override's App-ID is assigned.
  - c. The App-ID is set to duplicate definitions.
  - d. The App-ID is set to not available.
3. Which firewall process is bypassed when an Application Override policy matches traffic and assigns an App-ID?
- a. QoS
  - b. IPsec
  - c. Content-ID
  - d. User-ID
4. Which firewall tool provides settings and tools to convert policies from port-based to App-ID?
- a. Network Monitor display under App Scope
  - b. Policy Optimizer under Policies
  - c. Application Hit Count under Policies
  - d. View Applications as Groups under Policies
5. An administrator creates a Security policy rule that allows office-on-demand traffic through the firewall. After the change is committed, the firewall issues the following warning:
- "vsys1: Rule 'Allow Office apps' application dependency warning:  
Application 'office-on-demand' requires 'ms-office365-base' be allowed  
Application 'office-on-demand' requires 'sharepoint-online' be allowed  
Application 'office-on-demand' requires 'ssl' be allowed  
Application 'office-on-demand' requires 'web-browsing' be allowed"*
- Which action should the administrator take?
- a. Create an application chain that includes the dependencies.
  - b. Add the listed applications to the same Security policy rule.
  - c. Set the service action of the rule to dependent application default.
  - d. Create a new Security policy rule for each listed application with an allow action higher in the rule list.
6. Which security risk is elevated when port-based Security policy rules are used?
- a. The firewall's resources will be negatively impacted by processing unwanted traffic.

- b. Unwanted applications can get through the firewall, bringing their vulnerabilities with them.
  - c. The network is more vulnerable to TCP DoS attacks.
  - d. The firewall is more vulnerable to UDP DoS attacks.
7. What is the Palo Alto Networks suggested process for converting port-based Security policy rules to use App-ID?
- a. Use the Expedition tool to analyze Traffic logs against Security policy to suggest policy changes.
  - b. Use the built-in firewall reports to identify applications found in the traffic and update policy based on desired traffic.
  - c. Use the Policy Optimizer feature of the firewall to identify applications and update policy rules.
  - d. Use the firewall's New Applications Seen feature to identify applications and update policy rules.
8. If App-ID is implemented in Security policy rules, should port numbers also be included?
- a. No, App-ID-based Security policy rules detect and allow or block any desired application using the included port number values in the App-ID database.
  - b. Yes, including the port numbers as a *service-matching* condition can eliminate some traffic before App-ID processing, thus conserving firewall resources.
  - c. Yes, including an *application-default* setting in the *service-matching* condition requires that applications use only known or typical port numbers.
  - d. No, App-ID based Security policy rules detect and allow or block any desired application using the edited port number values in the App-ID database.
9. An application using which protocol can receive an incomplete value in the Application field in the Traffic log?
- a. UDP
  - b. TCP
  - c. ICMP
  - d. GRE
10. Session traffic being evaluated by a firewall is encrypted with SSL. If the firewall does not decrypt the traffic, how can the firewall make an App-ID determination?
- a. Evaluate the HTTP headers.
  - b. Evaluate the SSL Hello exchange.
  - c. Evaluate certificate contents used for encryption.
  - d. Use information in the SSL Decryption Exclusion cache.
11. While a firewall is scanning an active session, how does it respond when it detects a change of application?
- a. closes the session, opens a new one, and evaluates all Security policy rules again
  - b. closes the session, opens a new one, and evaluates the original matching Security policy rule only
  - c. updates the app in the existing session and evaluates all Security policy rules again

- d. updates the app in the existing session and continues to use the original action from the first Security policy rule match

## 3.2 Configure GlobalProtect

To implement GlobalProtect, configure the following:

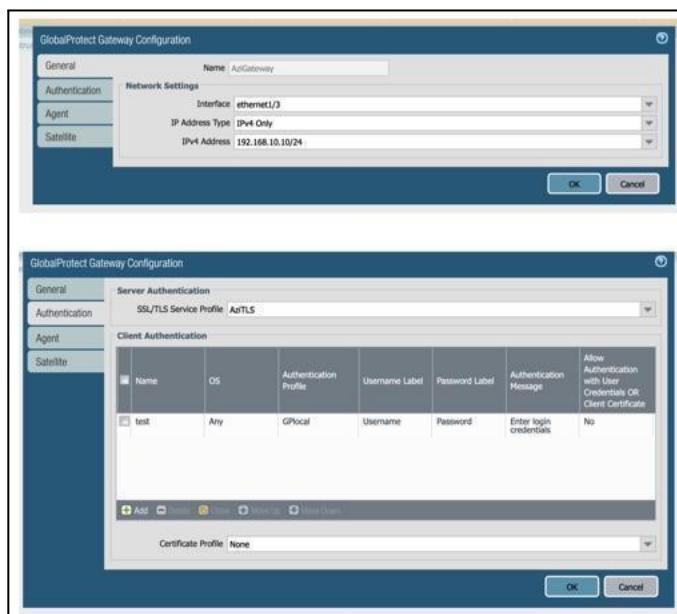
- Download the GlobalProtect client and activate it on the PAN-OS firewall.
- Configure the portal.
- Configure the gateway configuration
- Set up routing between the trust zones and GlobalProtect clients.
- Configure Security and NAT policies that permit traffic between the GlobalProtect clients and trust zones.
- Use the GlobalProtect app to connect mobile devices.

### 3.2.1 GlobalProtect licensing

By default, you can deploy GlobalProtect portals and gateways (without HIP checks) without a license. If you want to use advanced GlobalProtect features (HIP checks and related content updates, the GlobalProtect mobile app, IPv6 connections, or a GlobalProtect clientless VPN) you will need a GlobalProtect license (subscription) for each gateway.

### 3.2.2 Configure the gateway and portal

For initial testing, we recommend configuring basic authentication. To authenticate devices with a third-party VPN app, check **Enable X-Auth Support** in the gateway's client configuration. Include the **Group Name** and password for this setting.



## **Software Support for GlobalProtect Mobile App 5.0 and PAN-OS 9.0 and Later**

You can configure a label to identify the physical location of GlobalProtect gateways and portals using the CLI or the XML API. The GlobalProtect app displays the location label for the gateway to which users connect. For clientless VPN, the portal landing page displays the physical location of the portal to which clientless VPN users are logged in.

When end users experience unusual behavior such as poor network performance, they can provide location information to support or Help Desk professionals to assist with troubleshooting. They can also use this location information to determine their proximity to the portal or gateway. Based on their proximity, they can evaluate whether they need to switch to a closer portal or gateway.

Refer to the [GlobalProtect App 5.0 New Features Guide](#) for more information on gateway and portal location visibility for end users.

### **CLI**

Use the following CLI command to specify the physical location of the firewall on which you configured the portal and/or gateway:

```
username@hostname> set deviceconfig setting global-protect location  
<location>
```

### **XML API**

Use the following XML API to specify the physical location of the firewall on which you configured the portal and/or gateway:

```
curl -k -F file=@filename.txt -g  
'https://<firewall>/api/?key=<apikey>type=config&action=set&xpath=/config/  
devices/entry[@name='<device-name>']/deviceconfig/setting/global-protect&  
lement=<location><location-string></location>'
```

**Where:**

**Devices:** Name of the firewall on which you configured the portal and/or gateway

**Location:** Location of the firewall on which you configured the portal and/or gateway

### **3.2.3 GlobalProtect agent**

The GlobalProtect agent is a program that runs on your endpoint to protect you by using the same security policies that protect the sensitive resources on your corporate network. (An endpoint can be a desktop computer, laptop, notebook, or smartphone.) You can use the GlobalProtect agent to connect to your corporate network and access your company's internal resources from anywhere in the world.

To install the GlobalProtect agent, download the GlobalProtect VPN client. Choose from the Windows, MacOS, Linux, iOS, and Android client options. The iOS client is available for download from iTunes, and the Android client is available from Google Play.

- To install the agent, install the GlobalProtect Setup Wizard.

Authenticate on the campus VPN network using DUO two-factor authentication.

### 3.2.4 Differentiate between logon methods

Supported GlobalProtect authentication methods include the following:

- Local authentication
- External authentication
- Client certificate authentication
- Two-factor authentication
- MFA for non-browser-based applications
- SSO

### 3.2.5 Configure clientless VPN

Install a GlobalProtect subscription on the firewall that hosts the clientless VPN from the GlobalProtect portal.

### 3.2.6 HIP

One of the jobs of the GlobalProtect app is to collect information about the host it is running on. The app then submits this host information to the GlobalProtect gateway upon successful connection. The gateway matches this raw host information submitted by the app against any HIP objects and HIP profiles that you have defined. If it finds a match, it generates an entry in the HIP Match log. Additionally, if it finds a HIP profile match in a policy rule, it enforces the corresponding Security policy.

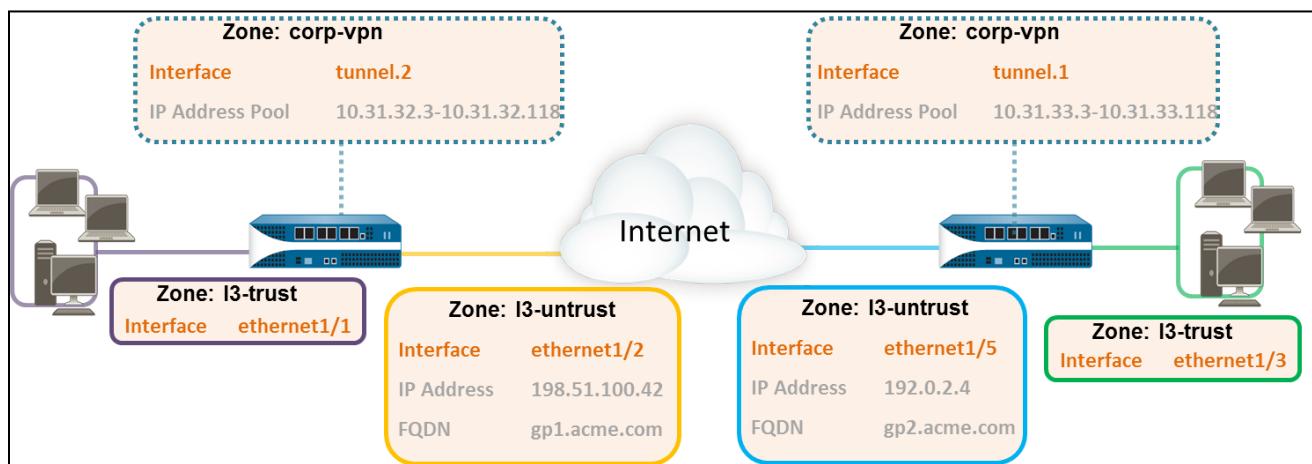
HIP checks are performed when the app connects to the gateway. Subsequent checks are performed hourly while the GlobalProtect agent is connected. The GlobalProtect agent can request an updated HIP report if the previous HIP check has changed. Only the latest HIP report is retained on the gateway per endpoint.

Using HIPs for policy enforcement enables granular security that ensures that the remote hosts accessing your critical resources are adequately maintained and adhere with your security standards before they are allowed access to your network resources. For example, before allowing access to your most sensitive data systems, you might want to ensure that the hosts accessing the data have encryption enabled on their hard drives. You can enforce this policy by creating a Security rule that only allows access to the application if the endpoint system has encryption enabled. In addition, for endpoints that are not in compliance with this rule, you could create a notification message that alerts users as to why they have been denied access and links

them to the file share where they can access the installation program for the missing encryption software. (Of course, to allow the user to access that file share, you would have to create a corresponding Security rule allowing access to the particular share for hosts with that specific HIP profile match.)

### 3.2.7 Configure multiple gateway agent profiles

In the GlobalProtect multiple gateway topology below, a second external gateway is added to the configuration. In this topology, you must configure an additional firewall to host the second GlobalProtect gateway. When you add the client configurations to be deployed by the portal, you can also specify different gateways for different client configurations, or allow access to all gateways.



If a client configuration contains more than one gateway, the app attempts to connect to all gateways listed in its client configuration. The app uses priority and response time to determine the gateway to which it will connect. The app only connects to a lower-priority gateway if the response time for the higher-priority gateway is greater than the average response time across all gateways. For more information, see [Gateway Priority in a Multiple Gateway Configuration](#).

### 3.2.8 Split tunneling

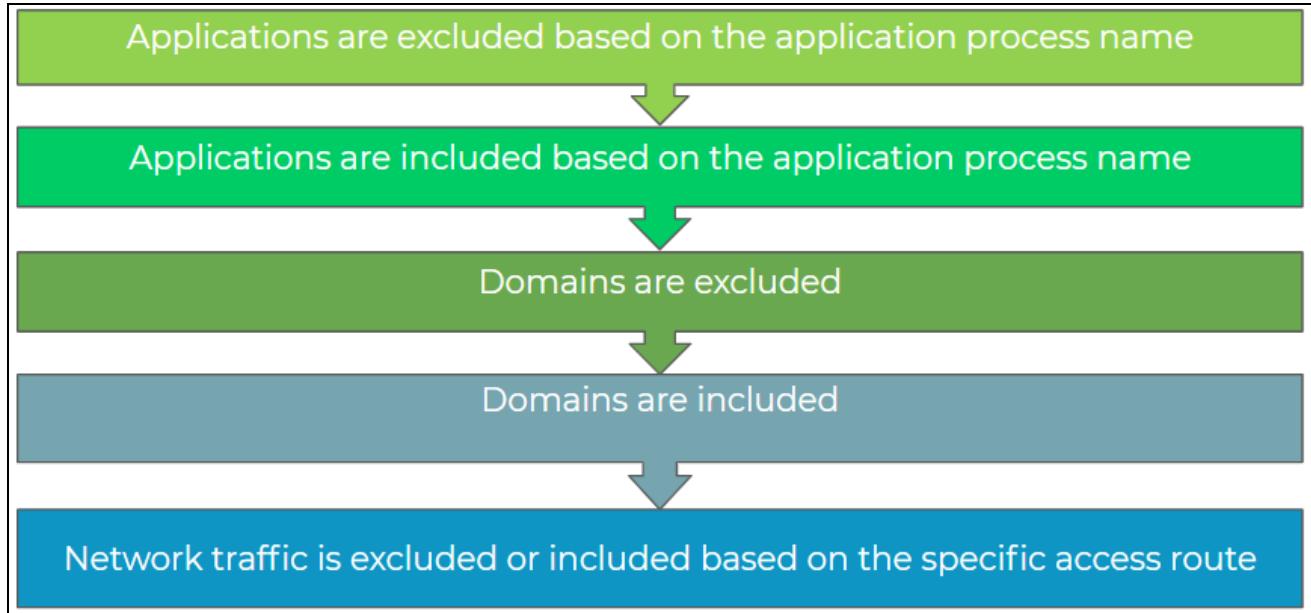
You can configure split tunnel traffic based on an access route, destination domain, application, and HTTP/HTTPS video streaming application.

The split tunnel capability allows you to conserve bandwidth and route traffic to:

- Tunnel enterprise SaaS and public cloud applications for comprehensive SaaS application visibility and control. This also helps you avoid risks associated with shadow IT in environments where it is not feasible to tunnel all traffic.
- Send latency-sensitive traffic, such as VoIP, outside the VPN tunnel while sending all other traffic through the VPN for inspection and policy enforcement.

- Exclude HTTP/HTTPS video streaming traffic from the VPN tunnel. Video streaming applications, such as YouTube and Netflix, consume large amounts of bandwidth. By excluding lower-risk video streaming traffic from the VPN tunnel, you can decrease bandwidth consumption on the gateway.

The split tunnel rules are applied for Windows and macOS endpoints in the following order:



### 3.2.9 References

GlobalProtect Overview:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-overview>

About Host Information:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/host-information/about-host-information>

How to Configure GlobalProtect:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFbCAK>

Configure NAT:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/nat/configure-nat>

Getting Started: Network Address Translation (NAT):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIzCAC>

Global protect multiple gateway configuration:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-quick-configs/globalprotect-multiple-gateway-configuration>

Host Information:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/host-information>

Split Tunnel Traffic on GlobalProtect Gateways:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-gateways/split-tunnel-traffic-on-globalprotect-gateways>

### 3.2.10 Sample Questions

1. Which GlobalProtect configuration component contains the setting that specifies when the agent software starts on the client system?
  - a. agent settings in GlobalProtect portal settings
  - b. general settings in GlobalProtect portal settings
  - c. agent settings in the GlobalProtect gateway
  - d. general settings in the GlobalProtect gateway
2. Which configuration or service is required for an iOS device using the GlobalProtect license to connect to a GlobalProtect gateway?
  - a. X-Auth configuration in the gateway settings
  - b. a GlobalProtect gateway license
  - c. a firewall Authentication policy with an iOS setting
  - d. a GlobalProtect client downloaded from the GlobalProtect portal
3. A GlobalProtect gateway is solely responsible for which function?
  - a. terminating SSL tunnels
  - b. authenticating GlobalProtect users
  - c. creating on-demand certificates to encrypt SSL
  - d. managing and updating GlobalProtect client configurations
  - e. managing GlobalProtect gateway configurations

## 3.3 Configure decryption

You can configure the firewall to decrypt traffic for visibility, control, and granular security. Decryption policy rules can apply to SSL, including SSL encapsulated protocols (such as IMAP[S], POP3[S], SMTP[S], FTP[S]), and to SSH traffic. SSH decryption can be used to decrypt outbound and inbound SSH traffic to ensure that secure protocols are not being used to tunnel disallowed applications and content.

### 3.3.1 Inbound decryption

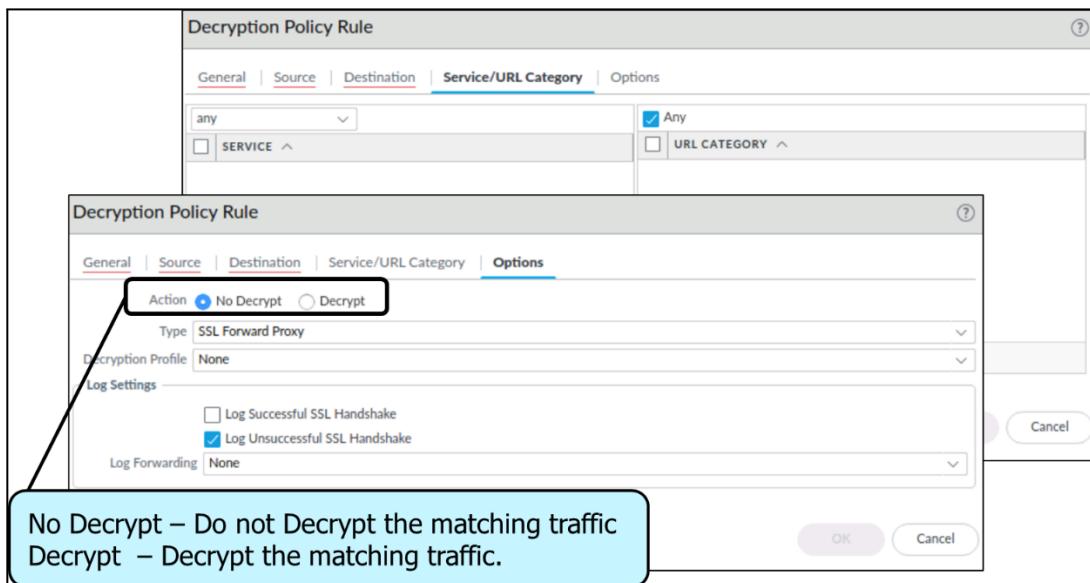
#### *Configuring Decryption*

A Palo Alto Networks firewall also can act as a decryption broker for other external security services. This feature will decrypt traffic and forward it out of the selected interface to a specific security device or service

(or chain of devices) that examines the cleartext traffic. The last service in the chain returns the packet to the firewall, which then encrypts it and forwards it to the original destination.

### Decryption Policies

Ingress traffic decryption is controlled by decryption policies. Palo Alto Networks firewalls automatically detect encrypted traffic and react by evaluating the decryption policy rules. If a matching policy rule is found, the firewall will attempt to decrypt the traffic according to the policy rule's specified decryption action. Normal packet processing resumes afterward.



### 3.3.2 SSL Forward Proxy

To configure SSL Forward Proxy decryption, you must set up the certificates required to establish the firewall as a trusted third-party (proxy) to the session between the client and the server.

### 3.3.3 SSL decryption exclusions

There are two types of decryption exclusions: predefined exclusions and custom exclusions.

- Predefined decryption exclusions allow applications and services that might break when the firewall decrypts them to remain encrypted. Palo Alto Networks defines the predefined decryption exclusions and delivers updates and additions to the predefined exclusions list at regular intervals as part of the Applications and Threats content update. Predefined exclusions are enabled by default, but you can choose to disable the exclusion as needed.
- You also can create custom decryption exclusions to exclude server traffic from decryption. All traffic originating from or destined to the targeted server remains encrypted.

### 3.3.4 SSH Proxy

To configure SSH Proxy, you do not need certificates and the key used to decrypt SSH sessions. With SSH decryption enabled, the firewall decrypts SSH traffic and blocks or restricts the SSH traffic based on your decryption policy and Decryption Profile settings. The traffic is re-encrypted as it exits the firewall. Decryption can only be performed on virtual wire, Layer 2, or Layer 3 interfaces.

### 3.3.5 References

Decryption Concepts:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts>

Decryption Best Practices:

<https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices>

IPv6 Support by Feature:

<https://docs.paloaltonetworks.com/compatibility-matrix/ipv6-support-by-feature/ipv6-support-by-feature-table>

Decryption Broker Concepts:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts>

Configure SSL Forward Proxy:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>

### 3.3.6 Sample Questions

1. Which two configuration conditions must be met for a firewall to NAT between IPv4 and IPv6? (Choose two.)

- a. Select NAT64 in the Session tab under Device > Setup > Session.
- b. Choose the NAT Type of NAT64 in the General tab of a NAT policy rule.
- c. Add an IPv6 address to the Translated Packet tab.
- d. Add an IPv6 prefix in the NAT64 configuration in the NAT policy rule.

2. Which two configuration conditions must be met for a Palo Alto Networks firewall to send and receive IPv6 traffic? (Choose two.)

- a. The Enable IPv6 check box in the virtual router configuration is checked.
- b. An Ethernet interface is configured for virtual wire.
- c. An Ethernet interface is configured for Layer 3.
- d. The Enable IPv6 Firewalling check box under Session Settings is turned on.

## 3.4 Configure User-ID

### 3.4.1 User-ID agent and agentless

#### *User-ID Agent*

To map usernames to IP addresses, User-ID agents monitor various sources, such as directory servers. The agents send the user mappings to firewalls, Log Collectors, or Panorama. Each of these appliances can then serve as redistribution points that forward the mappings to other firewalls, Log Collectors, or Panorama. For a firewall (device user identification User-ID agents) or Panorama (Panorama user identification) to collect user mappings, you must configure its connections to the User-ID agents or redistribution points.

#### *User-ID Agentless*

**You can use agentless User-ID** if you have a small to medium deployment with 10 or fewer domain controllers or Exchange servers and you wish to share PAN-OS-sourced mappings from AD, Captive Portal, or GlobalProtect with other Palo Alto devices (max 255 devices).

### 3.4.2 User-ID group mapping

The following are best practices for group mapping in an AD environment:

- If you have a single domain, you need only one group mapping configuration with an LDAP server profile that connects the firewall to the domain controller with the best connectivity. You can add up to four domain controllers to the LDAP server profile for redundancy. Note that you cannot increase redundancy beyond four domain controllers for a single domain by adding multiple group mapping configurations for that domain.
- If you have multiple domains or multiple forests, you must create a group mapping configuration with an LDAP server profile that connects the firewall to a domain server in each domain or forest. Take steps to ensure unique usernames in separate forests.
  - If you have universal groups, you can create an LDAP server profile to connect to the root domain of the global catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information are available for all domains and subdomains.
  - Before using group mapping, configure a primary username for user-based Security policies, since this attribute will identify users in the policy configuration, logs, and reports.

### 3.4.3 Shared User-ID mapping across virtual systems

You can enable a firewall or virtual system to serve as a data distribution agent that redistributes user mapping information and timestamps associated with authentication challenges. Simply configure the Data Redistribution settings to create an agent that will communicate with any firewalls or other devices to share local information.

### **3.4.4 Data redistribution**

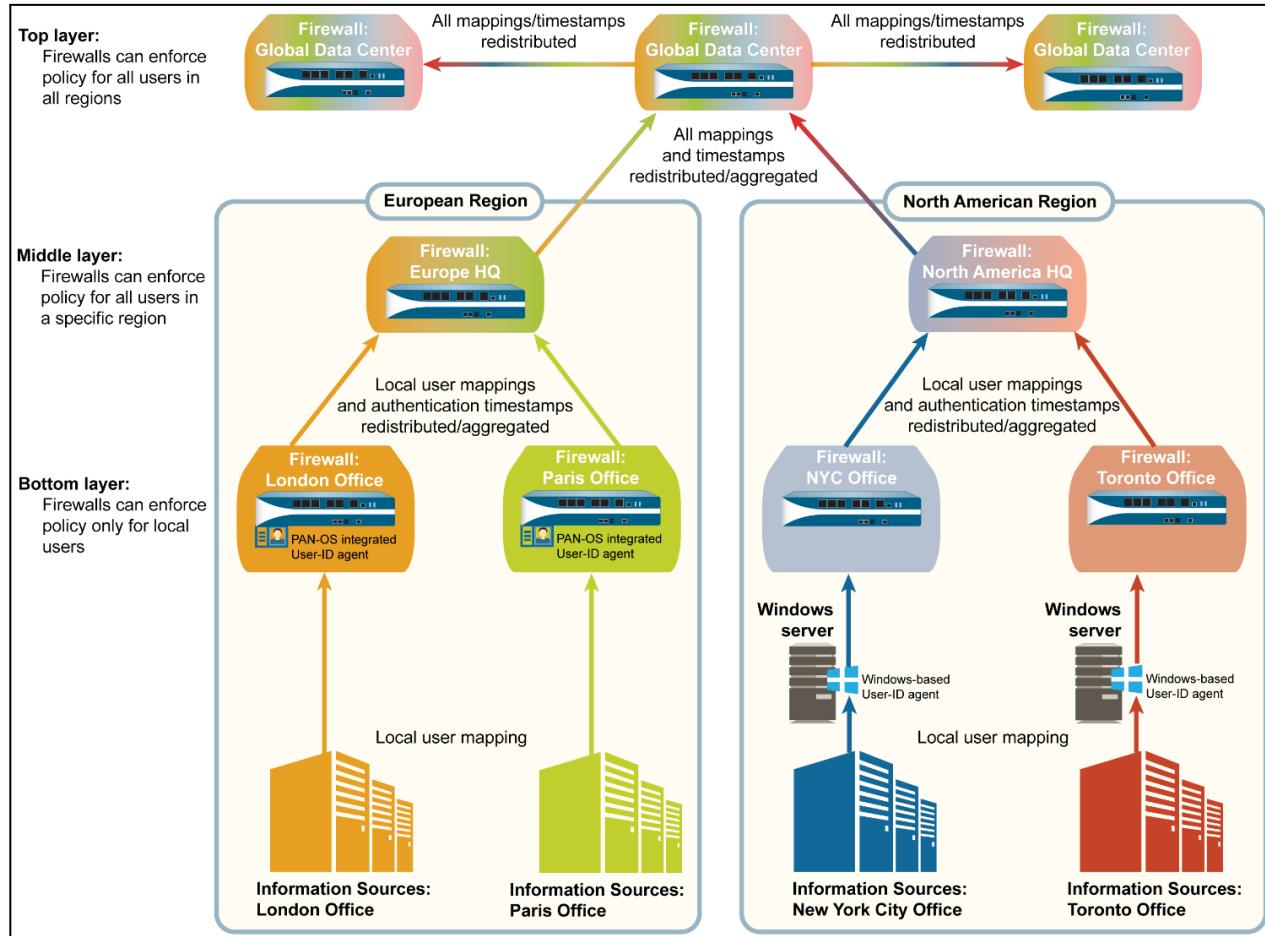
Every firewall that enforces user-based policy requires user mapping information. In a large-scale network, instead of configuring all your firewalls to directly query the mapping information sources, you can streamline resource usage by configuring some firewalls to collect mapping information through redistribution.

Redistribution also enables the firewalls to enforce user-based policies when users rely on local sources for authentication (such as regional directory services) but need access to remote services and applications (such as global data center applications). The Data Redistribution feature allows a firewall to be a source of IP user mappings, among other types of data, for any device that is configured to communicate with the agent service of that source firewall or via Panorama.

If you configure an Authentication policy, your firewalls also must redistribute the authentication timestamps that are generated when users authenticate to access applications and services. Firewalls use the timestamps to evaluate the timeouts for Authentication policy rules. The timeouts allow a user who successfully authenticates to later request services and applications without authenticating again within the timeout periods. Redistribution of timestamps enables you to enforce consistent timeouts across all the firewalls in your network.

Firewalls share user mappings and authentication timestamps as part of the same redistribution flow; you do not have to configure redistribution for each information type separately.

## Use Case Example



### 3.4.5 User-ID methods

User-ID enables you to identify all users on your network to ensure that you can identify users in all locations across access methods and operating systems, including Microsoft Windows, Apple iOS, macOS, Android, and Linux/UNIX. Knowing who your users are instead of just their IP addresses enables:

- **Visibility:** Improved visibility into application usage based on users gives you a more relevant picture of network activity. The power of User-ID becomes evident when you notice a strange or unfamiliar application on your network. Using either ACC or the log viewer, your security team can discern what the application is, who the user is, the bandwidth and session consumption, the source and destination of the application traffic, and any associated threats.
- **Policy control:** Tying user information to Security policy rules improves safe enablement of applications traversing the network and ensures that only those users who have a business need for an application have access. For example, some applications (such as SaaS applications that enable access to Human Resources services) must be available to any known user on your network. However, for more sensitive applications, you can reduce your attack surface by

ensuring that only users who need these applications can access them. For example, while IT support personnel may legitimately need access to remote desktop applications, the majority of your users do not.

- **Logging, reporting, and forensics:** If a security incident occurs, forensics analysis and reporting based on user information rather than just IP addresses provides a more complete picture of the incident. For example, you can use the predefined user/group activity to see a summary of the web activity of individual users or user groups. The SaaS Application Usage report shows which users are transferring the most data over unsanctioned SaaS applications.

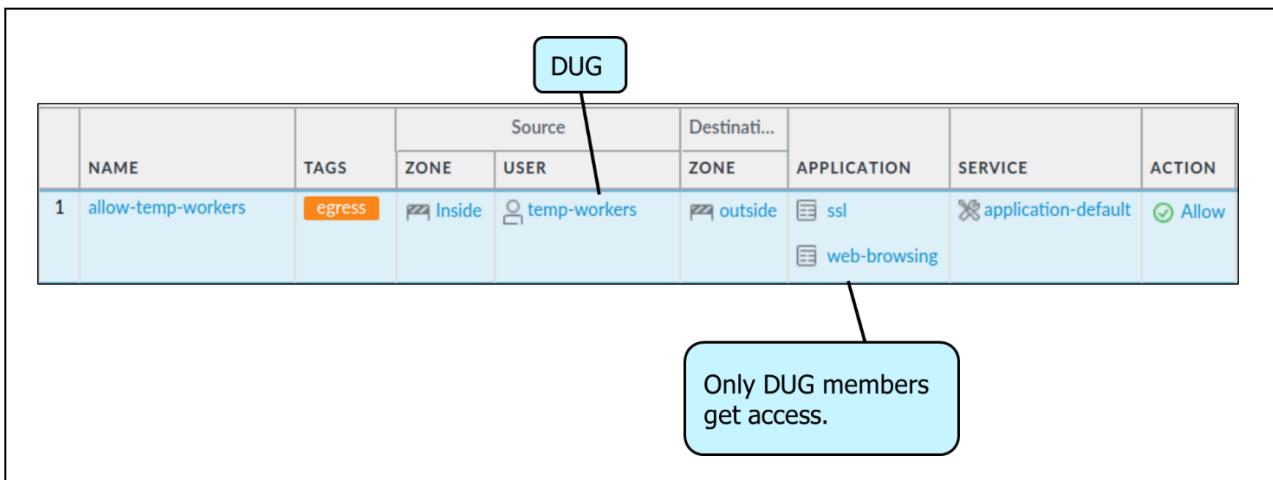
To enforce user- and group-based policies, the firewall must be able to map the IP addresses in the packets it receives to usernames. User-ID provides many mechanisms to collect this [user mapping](#) information. For example, the User-ID agent monitors server logs for login events and listens for syslog messages from authenticating services. To identify mappings for IP addresses that the agent didn't map, you can configure an authentication policy to redirect HTTP requests to an Authentication Portal login. You can tailor the user mapping mechanisms to suit your environment and even use different mechanisms at different sites to ensure that you are safely enabling access to applications for all users, in all locations, all the time.

### 3.4.6 Benefits of using dynamic user groups in policy rules

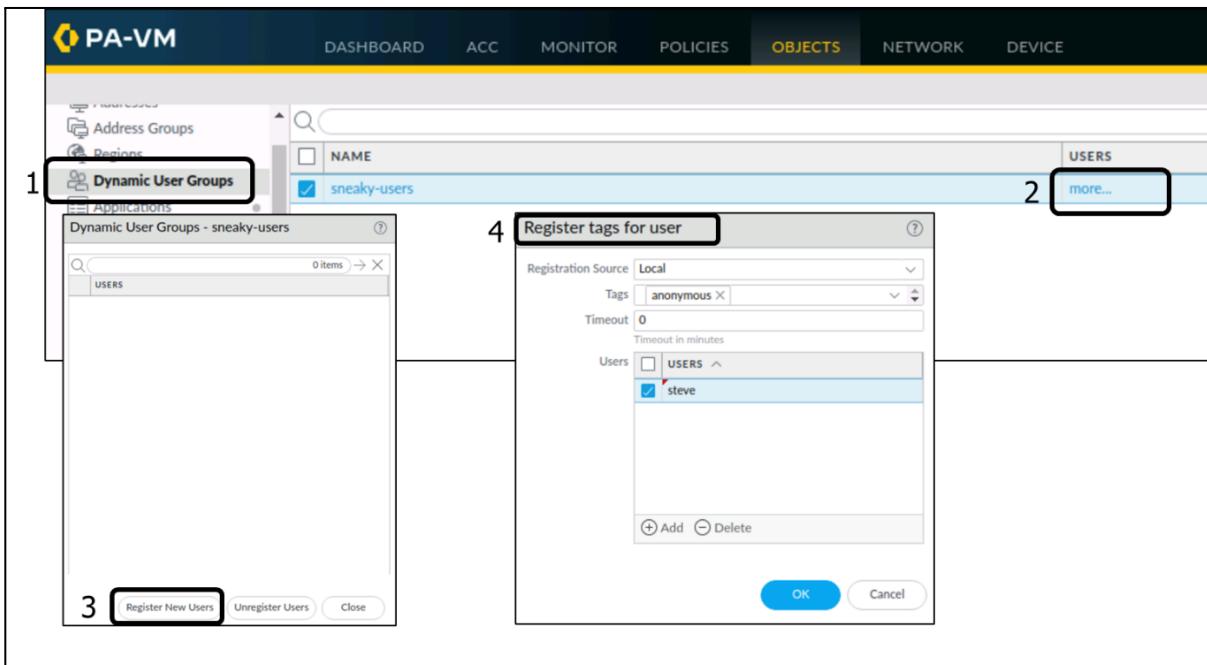
#### *Dynamic User Groups*

Dynamic user groups (DUGs) control access to resources that are managed by firewall policies, including the Security policy, authentication policy, and decryption policy. DUGs enable you to create policy rules that provide auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. When you create a policy rule, you can add a DUG to the Source User field as a match criterion. In past PAN-OS releases, you would have been able to add only a username or a static group name to the Source User field.

You must commit your firewall configuration after you have created a DUG and added it to a policy rule. However, you do not have to perform a commit when users are added to or removed from a DUG. User membership in a DUG is dynamic and controlled through tagging and untagging of usernames. Because updates to DUG membership are automatic, the use of DUGs instead of a static group (such as an LDAP group) enables you to respond to changes in user behavior or potential threats without manual policy changes.



Several methods are available to tag or untag usernames. As shown in the following screenshot, you can manually tag and untag usernames using the web interface:



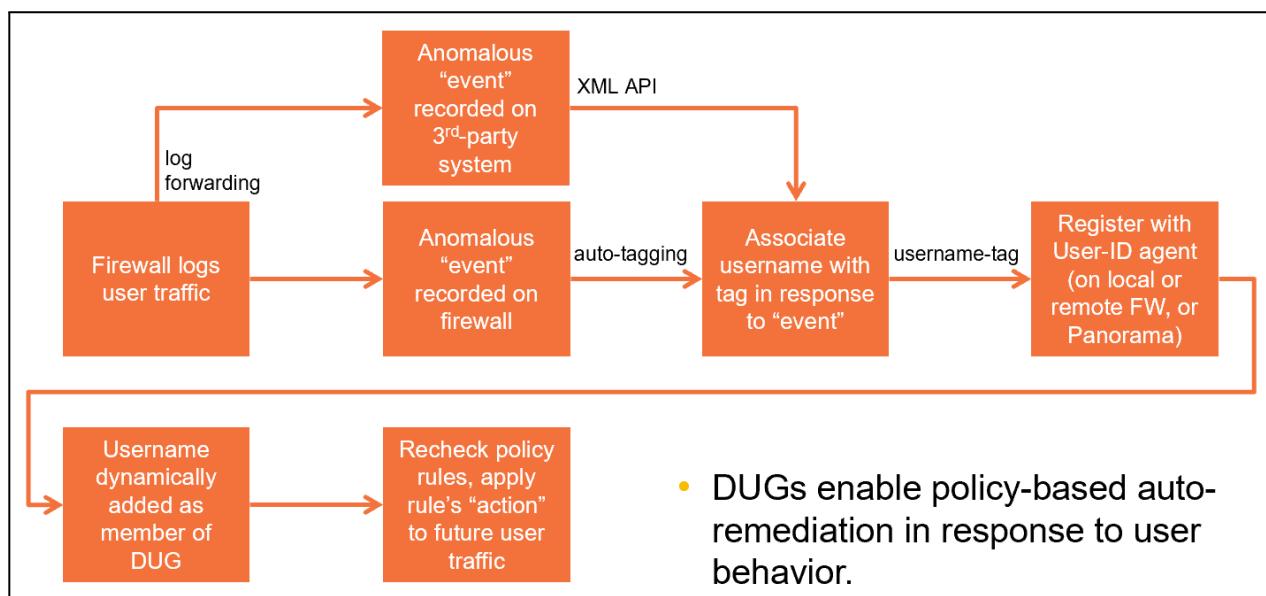
Usernames can also be tagged and untagged using the auto-tagging feature in a Log Forwarding Profile. You also can program another utility to invoke PAN-OS XML API commands to tag or untag usernames. In the web interface, you can use logical AND or OR operators with the tags to better filter or match against. You can configure a timeout value that determines when a username will be untagged automatically.

### DUG Operation

DUGs enable you to create a Security policy that provides auto-remediation in response to user behavior and activity. Auto-remediation reduces administrative burden by automating the firewall's response to user activity. Auto-remediation using DUGs also reduces the firewall's response time to malicious activity, which provides better security for your environment.

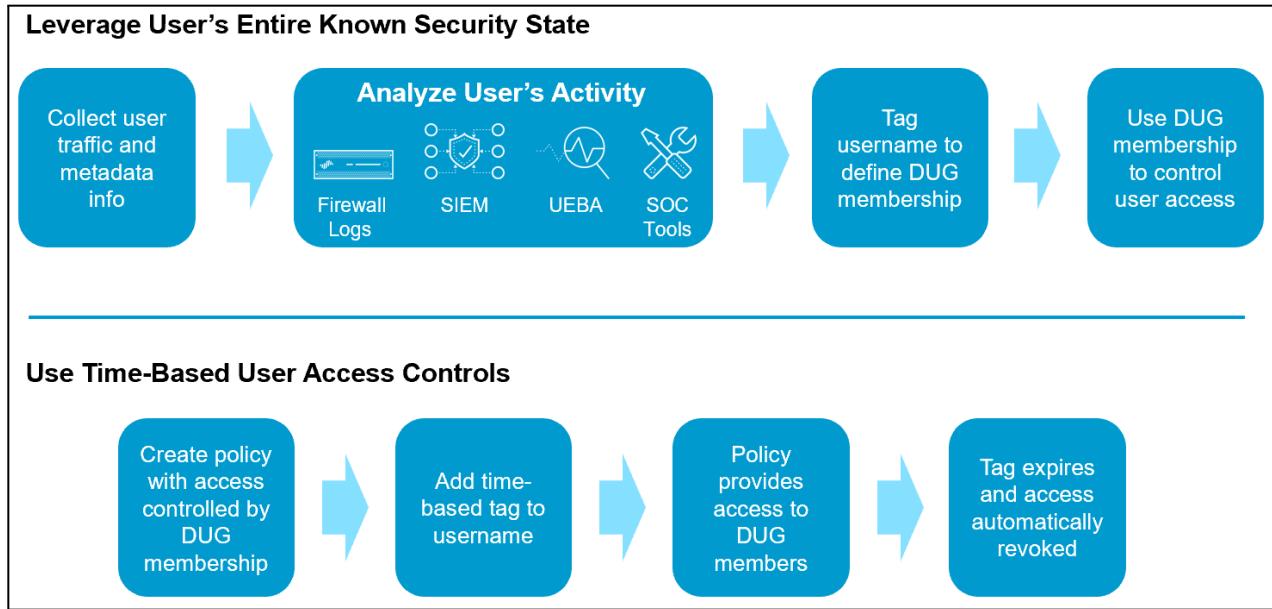
In the following figure, a user's traffic is recorded in the firewall logs. You can analyze these logs directly on the firewall, or you can configure log forwarding to forward the logs to a third-party system for analysis. If logs are being analyzed locally on the firewall, the log-forwarding configuration can invoke a new built-in action that will associate a tag with a username based on one or more events in a log. A third-party system can also associate a tag with a username using the PAN-OS XML API. Username-tag registrations are recorded in and maintained by a User-ID agent.

The firewall uses these username-tag pairs to determine which users are currently members of a DUG. When you configure a DUG, you associate it with one or more tags. Any user who is also associated with a tag configured in a DUG becomes a member of the DUG. DUG membership then is used to determine future policy rule matches. For example, a Security policy could block a user, an authentication policy could force the user to use MFA, or a decryption policy could force the user's traffic to be decrypted.



### *Example Use Cases*

Two DUG use case examples are shown here:



The first example shows how a user's entire known security state, which is derived from various sources, can determine how the firewall will control or affect the user's access to network resources. In this case, the user's network traffic is logged so that it can be analyzed. User metadata also might be collected from other resources, such as an LDAP server.

All this data can be analyzed in the firewall's logs, on a Security information and event management (SIEM), in a user and entity behavior analytics system, or by using a variety of tools available to a security operations center (SOC). Any of these tools can be configured to tag or untag a username, depending on the results of the analysis. Tagging and untagging of a username determines whether it is a member of a DUG. Then DUG membership and policy configuration determine how the firewall should treat the user's network traffic.

The second example illustrates how to use a DUG to implement time-based access controls for workers who might require only short-term access to network resources. In this case, you create a DUG and add it to policies that control user access to network resources. You then can add a time-based tag to a username. A tagged username is a member of the DUG, and network access is permitted by the DUG. When the time-based tag expires, the user's membership in the DUG is terminated, along with the network access that was provided by the DUG.

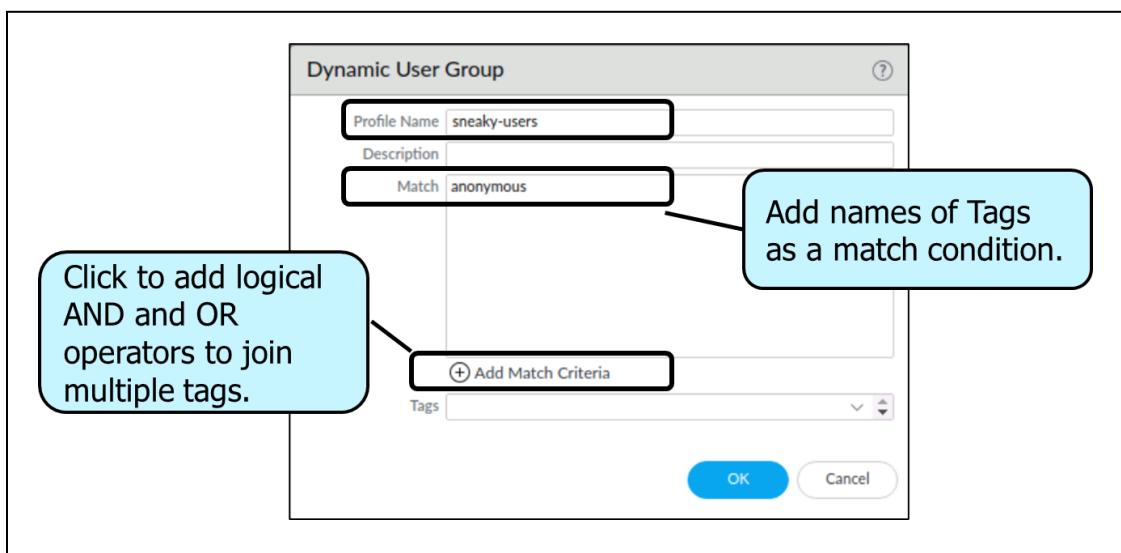
### 3.4.7 Requirements to support DUGs

#### *Configuring DUGs*

Before you can configure and use DUGs, first configure User-ID in your environment. The User-ID agent is used to maintain the list of which tags are associated with which usernames. To see the steps to configure User-ID, see the *PAN-OS Administrator's Guide* at <https://docs.paloaltonetworks.com>.

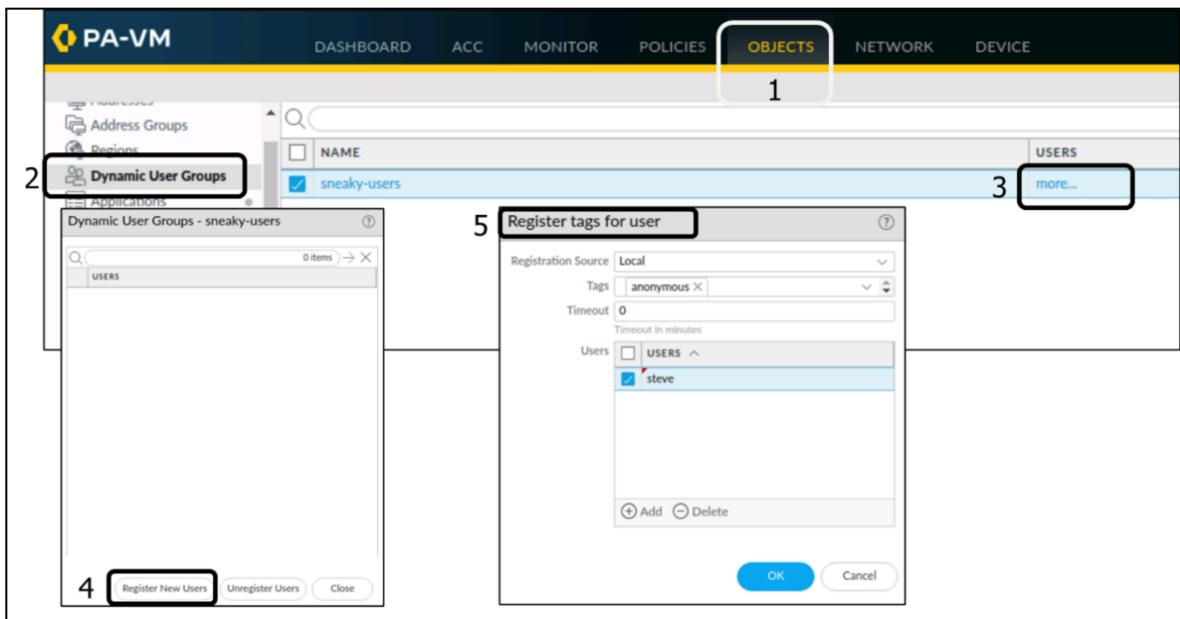
Then configure the custom tags to use as match conditions for DUG membership. In the web interface, browse to **Objects > Tags** and create one or more custom tags that can be dynamically assigned to users. After you have created custom tags, create the DUGs.

To create and configure a DUG, in the web interface browse to **Objects > Dynamic User Group**. Then click **Add** to create a new group. Provide a **Name** for the new group, optionally provide a **Description**, and then in the **Match** field, type one or more tags as match conditions. In the following example, the **Name** is **sneaky-users**, there is no **Description**, and the only **Match** condition is the tag named **anonymous**. If you click **Add Match Criteria**, then you can use the logical AND and OR operators to join multiple tags as match conditions. The **Tags** field value is the tag that is statically assigned to the DUG object itself. It is not assigned to a user and is not used as a match condition to identify users to add as DUG members.

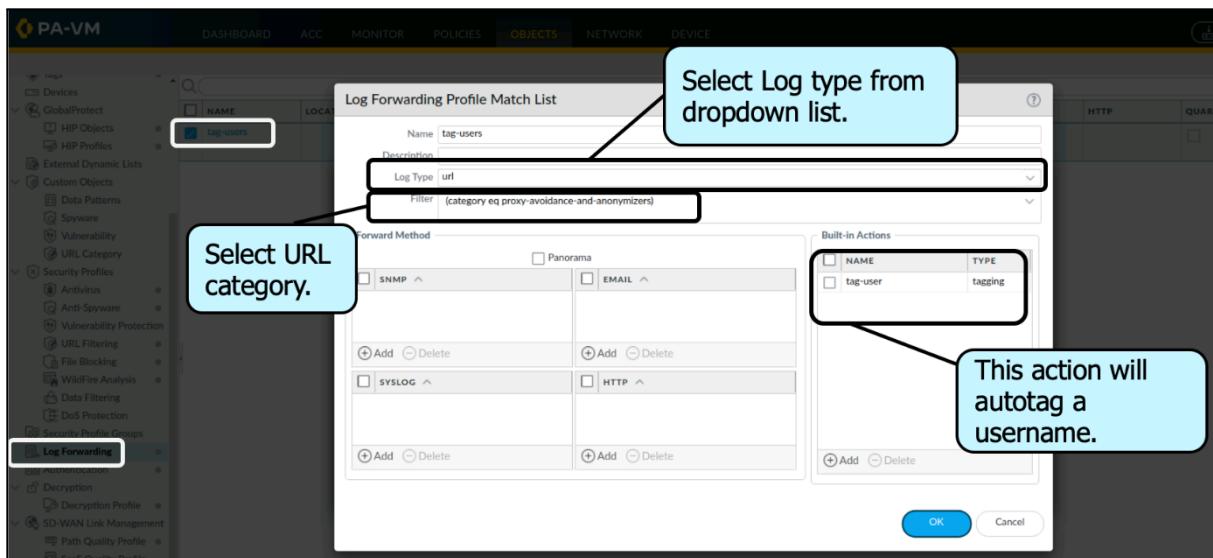


After you create the DUG, you must configure the firewall to use the DUG. Four options are available. To dynamically register a tag with a username, you can use Panorama, the XML API, a remote User-ID agent, or the web interface. A firewall can forward username and tag registration information to Panorama, and Panorama can distribute this information to other firewalls. Other applications can invoke firewall XML API commands to register username and tag associations. A remote User-ID agent can forward username and tag registrations to Panorama or other firewall User-ID agents. You also can use the web interface to register (or unregister) tags with usernames.

For example, the following screenshot illustrates use of the web interface to register or unregister tags from a username. Browse to **Objects > Dynamic User Groups** and click **more** next to a group name. In the window that opens, click **Register New Users** to register a tag with a username. In the next window that opens, select the **Registration Source**. You can choose the local User-ID agent, a remote User-ID agent, or Panorama. In the following example, the **Local User-ID** agent was selected. Then select the **Tags** to register with the user. The example uses the **anonymous** tag. If you want the tag to time out, which means the tag will be disassociated with the user, then choose a **Timeout** value in minutes. Then click **Add** and add one or more users to which to register the tag. To disassociate a tag from a username, start by clicking the **Unregister Users** button.



As a second example, you also can use a Log Forwarding Profile attached to a Security policy rule to auto-tag a username in response to a user's network behavior. In the following example, a Log Forwarding Profile named **tag-users** has been created. The profile is attached to a Security policy rule. If the rule matches an HTTP session and the URL Filtering log logs an entry where the URL category equals anonymous-proxy, then the Log Forwarding Profile invokes the built-in action that associates the tag *anonymous* with the username. The username is tagged and becomes a member of a DUG. Assuming that the DUG is used in the Security policy as a match condition, the firewall will modify what the user has access to.



For more information about using Panorama or the XML API to register and unregister tags, see the *PAN-OS Administrator's Guide* at <https://docs.paloaltonetworks.com>.

### **3.4.8 How GlobalProtect internal and external gateways can be used**

In a GlobalProtect mixed internal and external gateway configuration, you can set up two separate gateways for VPN access and for access to your sensitive internal resources. To do this, the GlobalProtect app performs internal host detection to determine if it is on the internal or external network.

### **3.4.9 References**

Mixed Internal and External Gateway Configuration:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-quick-configs/mixed-internal-and-external-gateway-configuration>

User-ID Agent:

<https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent>

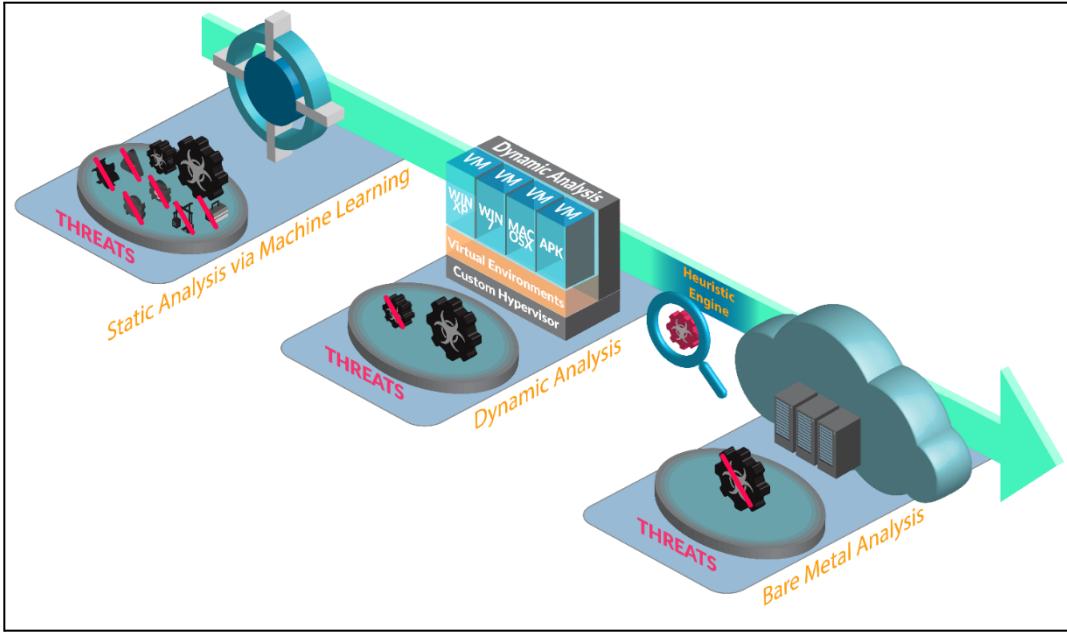
## **3.5 Configure Wildfire**

The WildFire Analysis sandbox identifies previously unknown malware and generates signatures that Palo Alto Networks firewalls can use to then detect and block malware. When a Palo Alto Networks firewall is instructed to forward files and URLs via a WildFire Analysis Profile, the firewall can automatically forward the sample for WildFire analysis. WildFire determines the sample to be benign, grayware, phishing, or malicious based on the properties, behaviors, and activities that the sample displays when analyzed and executed in the WildFire sandbox. WildFire then generates signatures to recognize the newly discovered malware and makes the latest signatures globally available every 5 minutes. Firewalls without a WildFire subscription license get the signature updates the following day, and firewalls with WildFire license gain access to signatures within 5 minutes of generation. All Palo Alto Networks firewalls worldwide then can compare incoming samples against these signatures to automatically block the malware first detected by a single firewall.

### **3.5.1 Configure a WildFire submission profile and add it to the Security rule**

WildFire is implemented in a Palo Alto Networks-managed public cloud or a WF-500 appliance installed on a user's network.

The following figure shows the principal workflow of WildFire:

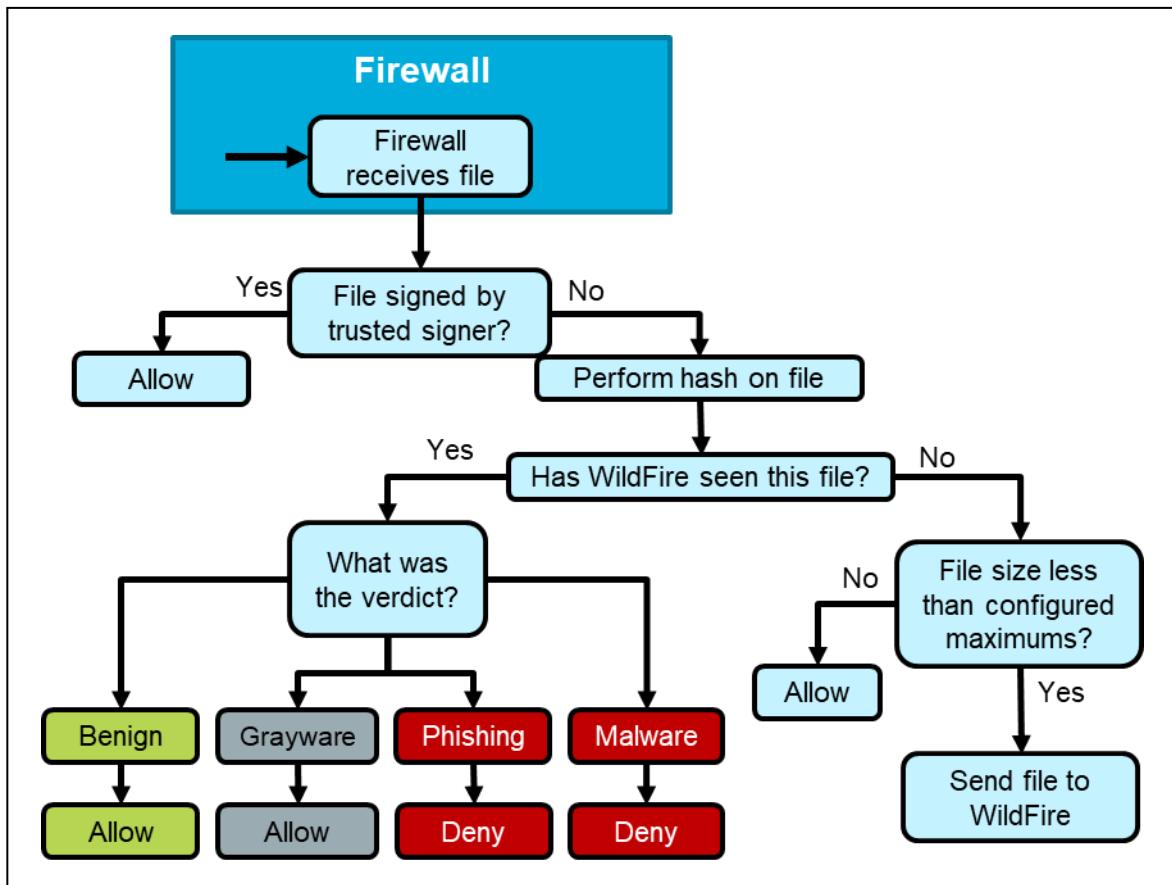


- WildFire looks within files or URLs for malicious activities and renders a verdict with an analysis report.
- WildFire analyzes files and URLs using the following methods:
  - **Static analysis:** Detects known threats by analyzing the characteristics of samples prior to execution
  - **ML:** Identifies variants of known threats by comparing malware feature sets against dynamically updated classification systems
  - **Dynamic analysis:** Creates a custom-built, evasion-resistant virtual environment in which previously unknown submissions are detonated to determine real-world effects and behavior
- **Bare-metal analysis (WildFire public cloud analysis only):** Creates a fully hardware-based analysis environment specifically designed for advanced VM-aware threats. Samples that display the characteristics of an advanced VM-aware threat are steered toward the bare-metal appliance by the heuristic engine.
- WildFire operates analysis environments that replicate the following operating systems:
  - Microsoft Windows XP 32-bit
  - Microsoft Windows 7 32-bit (supported as an option for the WildFire appliance only)
  - Microsoft Windows 7 64-bit
  - Microsoft Windows 10 64-bit
  - Mac OSX (WildFire cloud analysis only)

- Android (WildFire cloud analysis only)
- Linux (WildFire cloud analysis only)

The WildFire public cloud also analyzes samples using multiple versions of software to accurately identify malware that targets specific versions of client applications. The WildFire private cloud does not support multi-version analysis and does not analyze application-specific samples across multiple versions.

WildFire analysis of files is controlled by the configuration of a WildFire Analysis Profile attached to a Security policy allow rule. If the sample matches a rule, the firewall applies the WildFire forwarding evaluation shown in the following figure.



Files that are sent to WildFire for analysis are *not* quarantined in the firewall during the analysis process. They are forwarded normally to their destination. If WildFire detects malware, a notification can be sent, which should then be treated as an incident response appropriate to the organization's policies.

WildFire is available to every Palo Alto Networks firewall for use at no charge. A WildFire license is available that provides additional WildFire features.

### 3.5.2 Configure a WildFire action profile and add it to the Security rule

Use the **Antivirus Profiles** page to configure options to have the firewall scan for viruses on the defined traffic. Set the applications that should be inspected for viruses and the action to take when a virus is detected. The default profile inspects all of the listed protocol decoders for viruses, generates alerts for Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP), and Post Office Protocol Version 3 (POP3), and takes the default action for other applications (alert or deny), depending on the type of virus detected. The profile will then be attached to a Security policy rule to determine the traffic traversing specific zones that will be inspected.

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.

To add a new Antivirus profile, select Add and enter the following settings:

FIELD	DESCRIPTION
Name	Enter a profile name (up to 31 characters). This name appears in the list of antivirus profiles when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, periods, and underscores.
Description	Enter a description for the profile (up to 255 characters).
Shared <small>(Panorama only)</small>	Select this option if you want the profile to be available to: <ul style="list-style-type: none"><li>• Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the profile will be available only to the <b>Virtual System</b> selected in the <b>Objects</b> tab.</li><li>• Every device group on Panorama. If you clear this selection, the profile will be available only to the <b>Device Group</b> selected in the <b>Objects</b> tab.</li></ul>
Disable override <small>(Panorama only)</small>	Select this option to prevent administrators from overriding the settings of this Antivirus profile in device groups that inherit the profile. This selection is cleared by default, which means administrators can override the settings for any device group that inherits the profile.

#### Action Tab

Specify the action for the different types of traffic, such as FTP and HTTP.

Enable Packet Capture

Select this option if you want to capture identified packets.

Decoders and Actions

For each type of traffic that you want to inspect for viruses, select an action from the drop-down. You can define different actions for standard antivirus signatures (**Signature Action** column), signatures generated by the WildFire system (**WildFire Signature Action** column), and malicious threats detected in real-time by the WildFire Inline ML models (**WildFire Inline ML Action** column).

Some environments may have requirements for a longer soak time for antivirus signatures, so this option enables the ability to set different actions for the two antivirus signature types provided by Palo Alto Networks. For example, the standard antivirus signatures go through a longer soak period before being released (24 hours), versus WildFire signatures, which can be generated and released within 15 minutes after a threat is detected. Because of this, you may want to choose the alert action on WildFire signatures instead of blocking.



For the best security, clone the default Antivirus profile and set the Action and WildFire Action for all the decoders to **reset-both** and attach the profile to all Security policy rules that allow traffic.

Application Exceptions and Actions

The **Applications Exceptions** table allows you to define applications that will not be inspected. For example, to block all HTTP traffic except for a specific application, you can define an antivirus profile for which the application is an exception. **Block** is the action for the HTTP decoder, and **Allow** is the exception for the application. For each application exception, select the action to be taken when the threat is detected. For a list of actions, see [Actions in Security Profiles](#).

To find an application, start typing the application name in the text box. A matching list of applications is displayed, and you can make a selection.



If you believe a legitimate application is incorrectly identified as carrying a virus (false positive), open a support case with TAC so Palo Alto Networks can analyze and fix the incorrectly identified virus. When the issue is resolved, remove the exception from the profile.

#### Signature Exceptions Tab

Use the **Signature Exception** tab to define a list of threats that will be ignored by the antivirus profile.



Only create an exception if you are sure an identified virus is not a threat (false positive). If you believe you have discovered a false positive, open a support case with TAC so Palo Alto Networks can analyze and fix the incorrectly identified virus signature. When the issue is resolved, remove the exception from the profile immediately.

Threat ID

To add specific threats that you want to ignore, enter one Threat ID at a time and click **Add**. Threat IDs are presented as part of the threat log information. Refer to [Monitor > Logs](#).

#### WildFire Inline ML Tab

Use the **WildFire Inline ML** tab to enable and configure real-time WildFire analysis of files using a firewall-based machine learning model.



Palo Alto Networks recommends forwarding samples to the WildFire cloud when Wildfire inline ML is enabled. This allows samples that trigger a false-positive to be automatically corrected upon secondary analysis. Additionally, it provides data for improving ML models for future updates.

Available Models

For each available WildFire inline ML **Model**, you can select one of the following action settings:

- enable (**inherit per-protocol actions**)—Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab.
- alert-only (**override more strict actions to alert**)—Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab. Any action with a severity level higher than alert (drop, reset-client, reset-server, reset-both) will be overridden to alert, allowing traffic to pass while generating and saving an alert in the threat logs.
- disable (**for all protocols**)—Traffic is allowed to pass without any policy action.

File Exceptions

The **File Exceptions** table allows you to define specific files that you do not want analyzed, such as false-positives.

To create a new file exception entry, **Add** a new entry and provide the partial hash, filename, and description of the file that you want to exclude from enforcement.

To find an existing file exception, start typing the partial hash value, file name, or description in the text box. A list of file exceptions matching any of those values are displayed.



You can find partial hashes in the threat logs ([Monitor > Logs > Threat](#)).

### 3.5.3 Review the WildFire submissions and verdicts

The firewall forwards samples (files and emails links) to the WildFire cloud for analysis based on WildFire analysis profile settings. The firewall generates WildFire Submissions log entries for each sample it forwards after WildFire completes static and dynamic analysis of the sample. WildFire Submissions log entries include the firewall action for the sample (allow or block), the WildFire verdict for the submitted sample, and the severity level of the sample.

The following table summarizes the WildFire verdicts.

VERDICT	DESCRIPTION
Benign	Indicates that the entry received a WildFire analysis verdict of benign. Files categorized as benign are safe and do not exhibit malicious behavior.
Grayware	Indicates that the entry received a WildFire analysis verdict of grayware. Files categorized as grayware do not pose a direct security threat, but they might display otherwise obtrusive behavior. Grayware can include adware, spyware, and browser helper objects.
Phishing	Indicates that the entry received a WildFire analysis verdict of phishing. A phishing verdict indicates that the site to which the link directs users displayed credential phishing activity.
Malicious	Indicates that the entry received a WildFire analysis verdict of malicious. Samples categorized as malicious can pose a security threat. Malware can include viruses, C2, worms, Trojan horses, remote access tools (RATs), rootkits, and botnets. For samples that are identified as malware, the WildFire cloud generates and distributes a signature to prevent against future exposure.

### 3.5.4 Review WildFire signature actions

The Palo Alto Networks NGFW supports real-time retrieval of WildFire signatures. This enables you to access signatures as soon as they are generated, which greatly minimizes the window in which malware can infiltrate your network. Signature downloads that occur during a sample check are saved in the firewall cache and are available for fast (local) lookups. In addition, to maximize coverage, the firewall automatically downloads a supplementary signature package on a regular basis when you enable real-time signatures. These signatures remain available in the firewall cache until they become stale and are refreshed or are overwritten by new signature updates. Palo Alto Networks determines which protections are the most relevant and timely and includes those in the signature packages.

### 3.5.5 Supported file types and file sizes

#### File Types

The following table lists the file types that are supported for analysis in the WildFire cloud environments.

FILE TYPES SUPPORTED FOR ANALYSIS	WILDFIRE PUBLIC CLOUD (ALL REGIONS)	WILDFIRE U.S GOVERNMENT CLOUD	WILDFIRE PRIVATE CLOUD (WILDFIRE APPLIANCE)	WILDFIRE PORTAL   API (DIRECT UPLOAD; ALL REGIONS)
Links contained in emails	✓	✓	✓	✓
Adobe Flash files	✓	✓	X	✓
Java Archive (JAR) files	✓	✓	✓	✓
Microsoft office files (includes SLK and IQY files)	✓	✓	✓	✓
Portable executable files (includes MSI files)	✓	✓	✓	✓
Portable document format (PDF) files	✓	✓	✓	✓
Mac OS X files	✓	✓	X	✓
Linus (EFL files and Shell scripts) files	✓	✓	X	✓
Archive (RAR, 7-Zip, Zip*) files	✓	✓	✓	✓

Script (BAT, JS, VBS, PS1, and HTA) files	✓	X	✓	✓
Script (Perl and Python) scripts	X	X	X	✓
Archive (ZIP [direct upload] and ISO) files	X	X	X	✓

\* ZIP files are not directly forwarded to the Wildfire cloud for analysis. Instead, they are first decoded by the firewall, and files that match the WildFire Analysis profile criteria are separately forwarded for analysis.

## File Analysis

A Palo Alto Networks firewall configured with a WildFire analysis profile forwards samples for WildFire analysis based on file type (including email links). Additionally, the firewall decodes files that have been encoded or compressed up to four times (such as files in ZIP format); if the decoded file matches WildFire Analysis profile criteria, the firewall forwards the decoded file for WildFire analysis.

The WildFire analysis capabilities can also be enabled on the firewall to provide inline antivirus protection. The WildFire inline ML option present in the Antivirus profiles enables the firewall dataplane to apply machine learning analysis on PE and ELF files as well as PowerShell scripts in real-time. Each inline ML model dynamically detects malicious files of a specific type by evaluating file details, including decoder fields and patterns, to formulate a high probability classification of a file. This protection extends to currently unknown as well as future variants of threats that match characteristics that Palo Alto Networks has identified as malicious. To keep up with the latest changes in the threat landscape, inline ML models are added or updated via content releases. See WildFire Inline ML for more information.

The WildFire cloud is also capable of analyzing certain file types which are used as secondary payloads as part of multi-stage PE, APK, and ELF malware packages. Analysis of secondary payloads can provide additional coverage to disrupt sophisticated attacks by advanced threats. These advanced threats operate by executing code which activate additional malicious payloads, including those designed to assist in the circumvention of security measures as well as facilitate proliferation of the primary payload. WildFire analyzes the multi-stage threats by processing them in static, dynamic, or bare metal analysis environments. Files referenced by multi-stage malware are treated independently during analysis; as a result, verdicts and protections are delivered as soon as they finish for each file. The overall verdict for the multi-stage file is determined based on a threat assessment of malicious content found in all analyzed stages of the attack. Any malicious content discovered during analysis of the multi-stage file immediately marks the file as malicious.

Organizations with safe-handling procedures for malicious content can manually submit password-protected samples using the RAR format through the API or WildFire portal. When the WildFire cloud receives a sample that has been encrypted using the password *infected* or *virus*, the WildFire cloud decrypts and analyzes the

archive file. You can view the WildFire verdict and analysis results for the file in the format that it was received, in this case, an archive.

While the firewall can forward all the file types listed below, WildFire analysis support can vary depending on the WildFire cloud to which you are submitted samples. Review [WildFire File Type Support](#) to learn more.

FILE TYPES SUPPORTED FOR WILDFIRE FORWARDING	DESCRIPTION
apk	Android Application Package (APK) files.
flash	Adobe Flash applets and Flash content embedded in web pages.
jar	Java applets (JAR/class files types).
ms-office	Files used by Microsoft Office, including documents (DOC, DOCX, RTF), workbooks (XLS, XLSX), PowerPoint (PPT, PPTX) presentations, and Office Open XML (OOXML) 2007+ documents. Internet Query (IQY) and Symbolic Link (SLK) files are supported with content version 8462.
pe	Portable Executable (PE) files. PEs include executable files, object code, DLLs, FON(fonts), and LNK files. MSI files are supported with content version 8462. A subscription is not required to forward PE files for WildFire analysis, but is required for all other supported file types.
pdf	Portable Document Format (PDF) files.
MacOSX	Mach-O, DMG, and PKG files are supported with content version 599. You can also manually or programmatically submit all Mac OS X supported file types for analysis (including application bundles, for which the firewall does not support automatic forwarding).
email-link	HTTP/HTTPS links contained in SMTP and POP3 email messages. See <a href="#">Email Link Analysis</a> .
archive	Rosenthal Archive (RAR) and 7-Zip (7z) archive files. Multi-volume archives are split into several smaller files that cannot be submitted for analysis. Only RAR files encrypted with the password <i>infected</i> or <i>virus</i> are decrypted and analyzed by the Wildfire cloud.

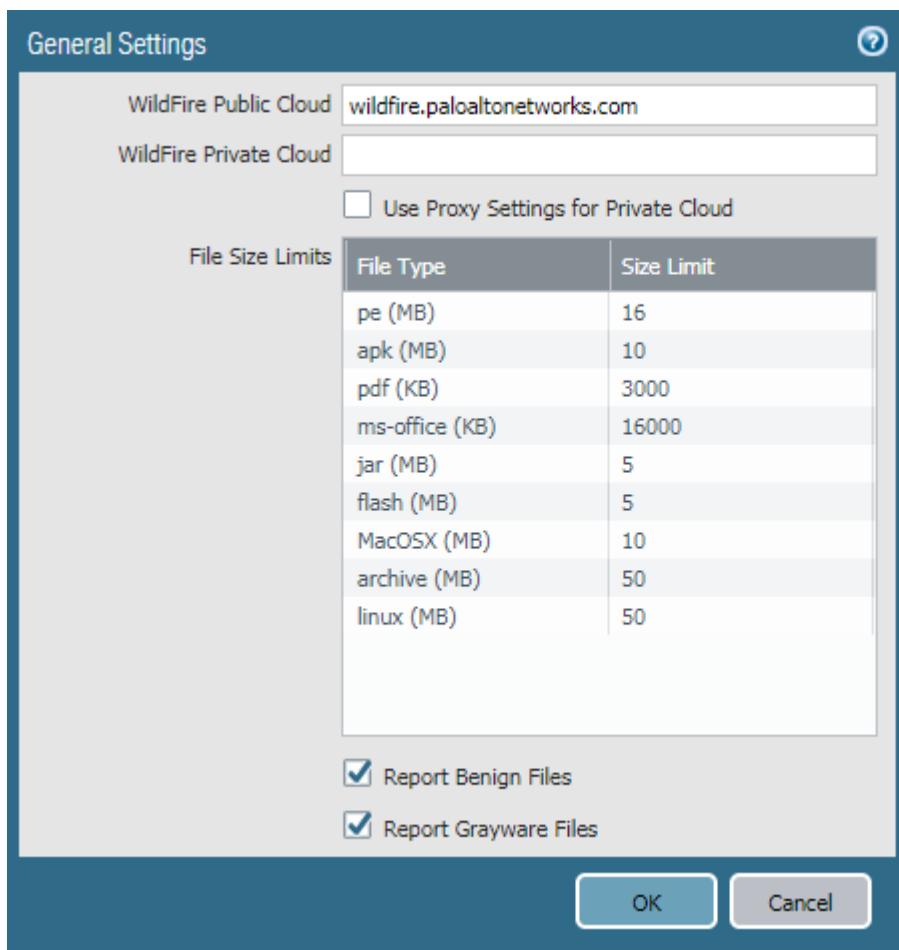
linux	Executable and Linkable Format (ELF) files.
script	<p>Various script files:</p> <ul style="list-style-type: none"> <li>• Jscript (JS), VBScript (VBS), and PowerShell Scripts (PS1) are supported with content version 8101.</li> <li>• Batch (BAT) files are supported with content version 8168.</li> <li>• HTML Application (HTA) files are supported with content version 8229.</li> </ul>

### File Sizes

The maximum and default WildFire file forwarding sizes and rates are increased in PAN-OS® 9.0 to provide optimal visibility and detection. Based on Palo Alto Network's data analytics, the new default capacities protect against the majority of threats, and is a best practice to use the new default values.

FILE TYPE	PAN-OS 9.0 DEFAULT FILE FORWARDING SIZES	PAN-OS 9.0 SIZE LIMITS
pe	16MB	1-50MB
apk	10MB	1-50MB
pdf	3,073KB	100-51,200KB
ms-office	16,384KB	200-51,200KB
jar	5MB	1-20MB
flash	5MB	1-10MB
MacOSX	10MB	1-50MB
archive	50MB	1-50MB
linux	50MB	1-50MB

**Step 1:** Log in to the firewall and verify the WildFire file forwarding size limits.



Size limits shown  
here do not  
necessarily reflect  
current defaults

**Step 2:** Commit your configuration updates.

**Step 3:** Verify that the firewall is forwarding files to the WildFire public cloud.

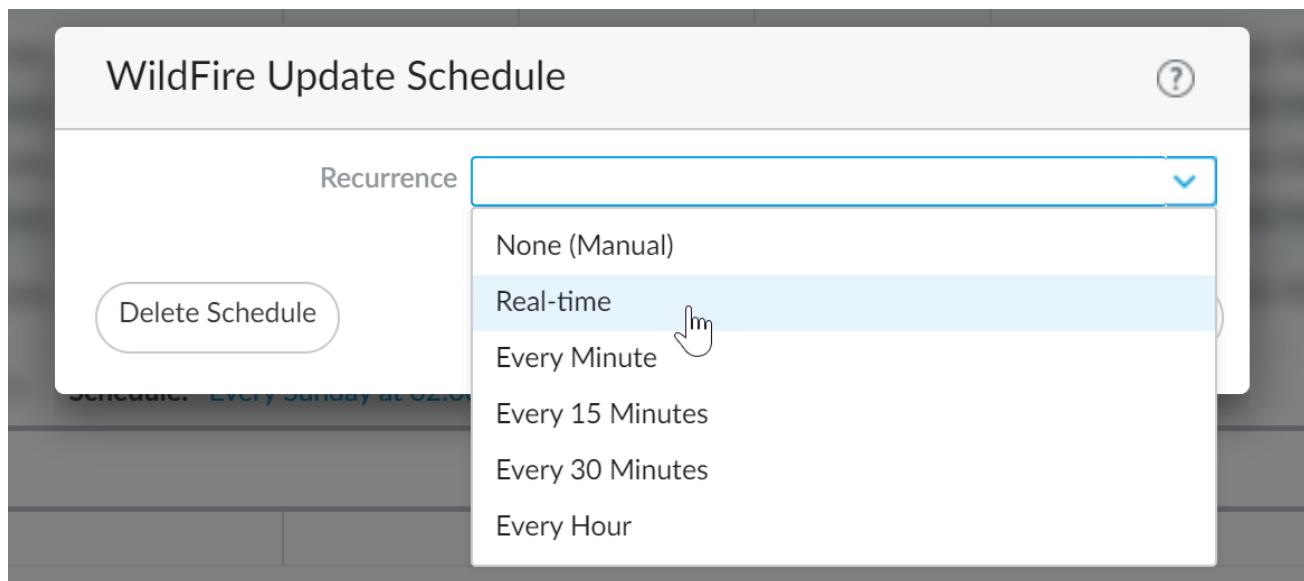
### 3.5.6 Configure WildFire update schedule

**Step 1:** To unlock access to real-time WildFire signatures, you must have a WildFire subscription service license. Make sure to activate the license on the firewall if you have not done so already.

- Select **Device > Licenses**.
- Manually upload the license key or retrieve it from the Palo Alto Networks license server.
- Verify that the WildFire subscription license is active.

**Step 2:** Set the schedule for the firewall to retrieve WildFire signatures in real-time and install periodic signature packages every five minutes.

Even when the firewall is configured to use real-time signatures, supplemental signature packages are still installed on a regular basis. This provides an up-to-date signature source when you experience connectivity issues, as well as a speed benefit, where signatures are available locally.



- Select **Device > Dynamic Updates**.
- Select the **Schedule** for WildFire updates.
- Set the **Recurrence** (how often the firewall checks the Palo Alto Networks update server for new signatures) for **Real-time** updates.
- Click **OK** to save the WildFire update schedule and then **Commit** your changes.

### 3.5.7 Configure forwarding decrypted traffic to WildFire

You can enable the firewall to forward decrypted SSL traffic for WildFire analysis. Traffic that the firewall decrypts is evaluated against Security policy rules; if it matches the WildFire analysis profile attached to the Security rule, the decrypted traffic is forwarded for WildFire analysis before the firewall re-encrypts it. Only a super user can enable this option.

- On a firewall that does not have multiple virtual systems enabled:
  1. If you have not already, enable the firewall to perform decryption and forward files for WildFire analysis.
  2. Select **Device > Setup > Content-ID**.
  3. Edit the Content-ID settings and click **Allow Forwarding of Decrypted Content**.
  4. Click **OK** to save the changes.

- On a firewall with virtual systems enabled:
  1. If you have not already, enable decryption and forward files for WildFire analysis.
  2. Select **Device > Virtual Systems**, click the virtual system you want to modify, and click **Allow Forwarding of Decrypted Content**.

### 3.5.8 References

Dynamic updates- wildfire:

<https://live.paloaltonetworks.com/t5/best-practice-assessment-device/dynamic-updates-wildfire/ta-p/338110>

Objects > Security Profiles > Antivirus:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-security-profiles-antivirus>

WildFire File Type Support:

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-file-type-support>

File Analysis:

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis>

WildFire Real-Time Signature Updates:

<https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-100/wildfire-real-time-signature-updates>

Increased WildFire File Forwarding Capacity:

<https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-90/increased-wildfire-file-forwarding-capacity.html>

### 3.5.8 Sample Questions

1. For WildFire file type support, what file types are supported for analysis? Select all that apply.

- links contained in emails
- Adobe Flash files
- PDF files
- Java Archive (JAR) files

2. A server on the DMZ with a private NIC address has network access provided by a NAT policy rule whose bi-directional check box is selected in the Translated Packet settings for static IP source address translation. Which Security policy rule must be created to allow bidirectional traffic to and from the DMZ server?

- a rule for each direction of travel using the pre-NAT server IP address

- b. a rule with the post-NAT source IP address
  - c. a rule for each direction of travel using the post-NAT server IP address
  - d. a rule with the pre-NAT source IP address
3. An internal web browser sends a packet to a server. The browser's connection has the source IP address 192.168.5.3, port 31415. The destination is 209.222.23.245, port 80. The firewall translates the source to 75.22.21.54, port 27182. Which three of these source IP addresses would cause a NAT policy rule to apply to this traffic? (Choose three.)
- a. 192.168.5.0/24
  - b. 75.22.21.0/24
  - c. 192.168.4.0/23
  - d. 192.168.0.0/16
  - e. 75.22.0.0/17
  - f. 75.22.128.0/17
4. A NAT policy rule is created to change the destination address of any packets with a source of any address and a destination address of 10.10.10.10 (in the DMZ zone) to 192.168.3.45 (in the trust zone). Which Security policy rule components are required for a packet that has this rule applied to match and allow this traffic?
- a. source address any, source zone any, destination address 192.168.3.45, destination zone Trust, action = allow
  - b. source address any, source zone any, destination address 10.10.10.10, destination zone Trust, action = allow
  - c. source address any, source zone any, destination address 192.168.3.45, destination zone DMZ, action = allow
  - d. source address any, source zone any, destination address 10.10.10.10, destination zone DMZ, action = allow
5. Which file type is not supported by WildFire?
- a. iOS
  - b. Android
  - c. Windows PE
  - d. Microsoft Excel
6. The firewall will skip the file upload to WildFire in which three cases? (Choose three.)
- a. The file has been signed by a trusted signer.
  - b. The file is being uploaded rather than downloaded.
  - c. The file is an attachment in an email.
  - d. The file hash matches a previous submission.
  - e. The file is larger than 50MB.
  - f. The file is transferred through HTTPS.

7. Which feature is *not* supported on the WF-500 appliance?

- a. bare-metal analysis
- b. Microsoft Windows XP 32-bit analysis
- c. Microsoft Windows 7 64-bit analysis
- d. static analysis

# Domain 4- Deploy and Configure Firewalls Using Panorama

## 4.1 Configure templates and template stacks

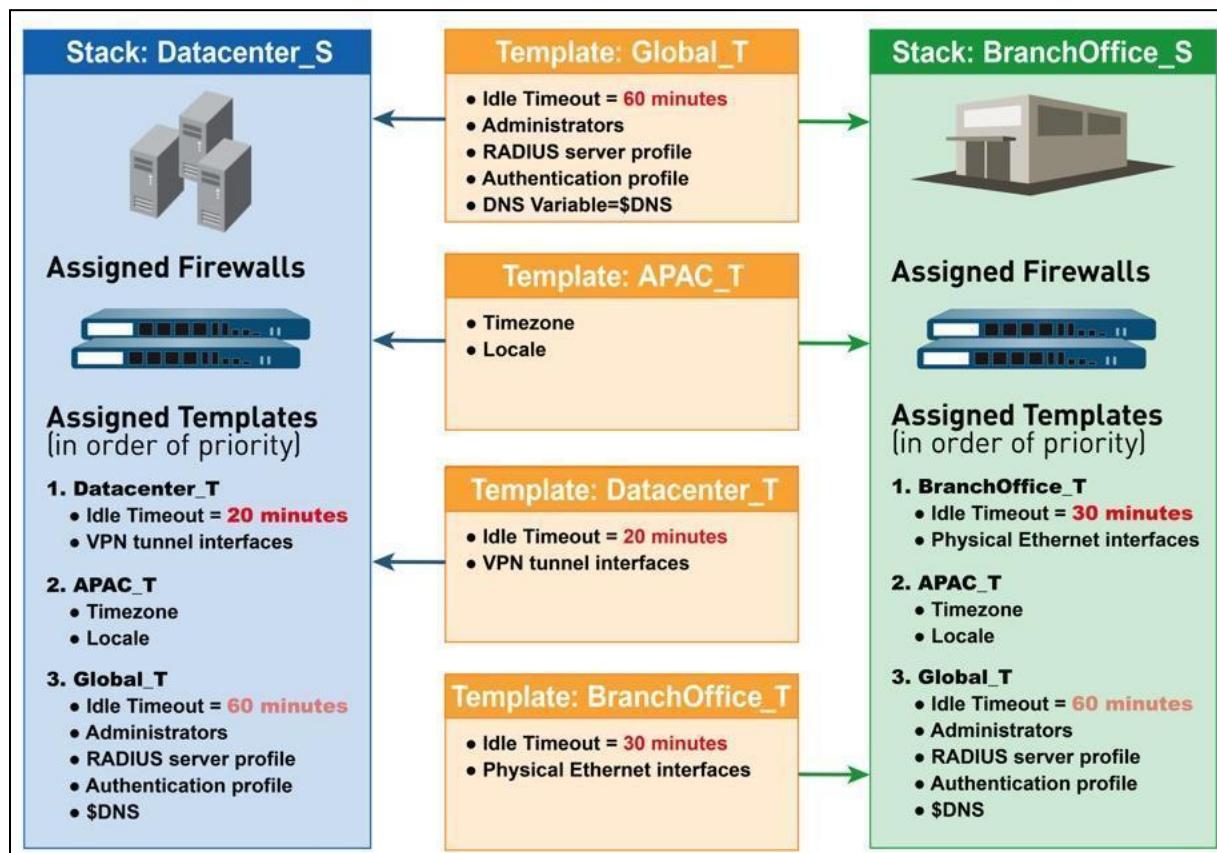
For centralized firewall configuration and update management, define a template stack.

### 4.1.1 Components configured in a template

To create a template stack, navigate to **Panorama > Templates > Add Stack**, then name the stack. Template stacks can combine up to eight templates. . Add templates in the order of priority. Next, in the **Device** section, select firewalls to assign them to the stack. You can assign any firewall to only one template stack. Optionally, select **Group HA Peers to** for firewalls in HA configuration.

### 4.1.2 How the order of templates in a stack affects the configuration push to a firewall

Templates in a stack have a configurable priority order to ensure that Panorama pushes only one value for any duplicate setting. The following illustration shows a data center stack in which the data center template has a higher priority than the global template.



### 4.1.3 Overriding a template value in a stack

While templates and template stacks enable you to apply a base configuration to multiple firewalls, you might want to configure firewall-specific settings that don't apply to all the firewalls in a template or template stack. Conversely, you may want to override the template settings to create a template stack configuration that you can apply as a base configuration to all your managed firewalls. Overrides allow for exceptions or modifications to meet your configuration needs. For example, if you use a template to create a base configuration but a few firewalls in a test lab environment need different settings for the DNS server IP address or the Network Time Protocol server, you can override the template and template stack settings.

You can override a template or template stack value in one of the following ways:

- Using variables: Define a value locally on the firewall to override a value pushed from a template or template stack, or define firewall-specific variables to override values pushed from a template or template stack.
- **Using a template stack:** Define values or variables on the template stack to override values pushed from a template.

### 4.1.4 Configure variables in templates

You can use template stack variables to replace IP addresses, group IDs, and interfaces in your configurations. Variables allow you to reduce the total number of templates and template stacks. This lets you use fewer templates and template stacks while using specific values that otherwise would have needed their own template or template stack.

### 4.1.5 Relationship between Panorama and devices for dynamic update versions, policy implementation, and HA peers

The firewall retrieves updates and uses them to enforce policy, without requiring configuration changes. You can view the latest updates, read the release notes for a description of each update, and then select the update you want to download and install.

### 4.1.6 References

Configure a Template or Template Stack Variable:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables>

Templates and Template Stacks:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

Manage Templates and Template Stacks:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks>

Template Capabilities and Exceptions:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/template-capabilities-and-exceptions>

Device > Dynamic Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-dynamic-updates>

Override a Template or Template Stack Value:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/override-a-template-setting>

#### 4.1.7 Sample Questions

1. The Security policy for all a customer's remote offices is the same, but different offices have different firewall models. If the remote offices are managed by Panorama, how might the offices share device groups and templates?
  - a. same device groups, same template stacks
  - b. same device groups, different template stacks
  - c. different device groups, same template stacks
  - d. different device groups, different template stacks
2. A Panorama template stack contains two templates, and one configuration setting has a different value in each template. When Panorama pushes the template stack to the managed firewalls, which setting value will the firewalls receive?
  - a. value from the top template of the stack
  - b. value from the bottom template in the stack
  - c. value from the template designated as the parent
  - d. value an administrator selects from the two available values
3. Which two firewall settings are stored in Panorama templates? (Choose two.)
  - a. custom Application-ID signatures
  - b. Server Profile for an external LDAP server
  - c. services definitions
  - d. DoS Protection profiles
  - e. data plane interface configurations

## 4.2 Configure device groups

Before you can use Panorama effectively, you must group the firewalls in your network into logical units called device groups. A device group enables grouping based on network segmentation, geographic location,

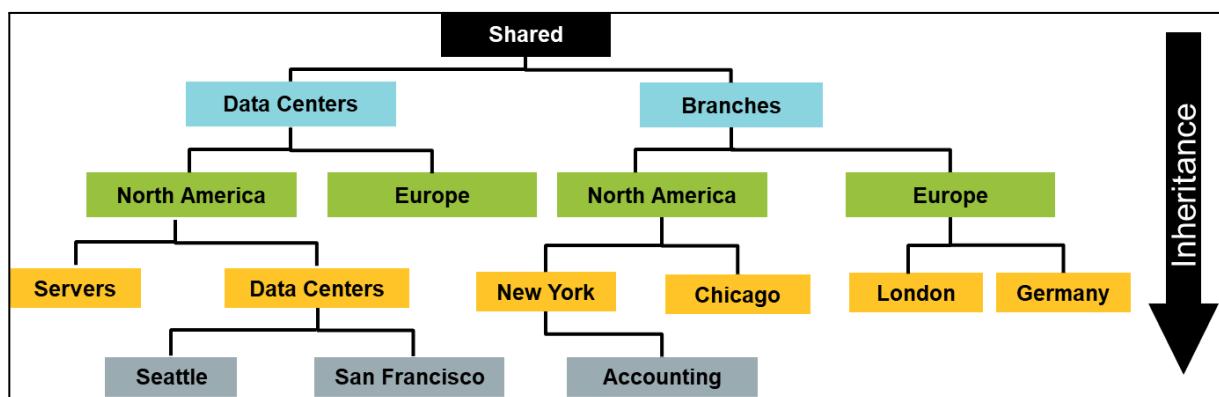
organizational function, or any other common aspect of firewalls that require similar policy configurations. You can use device groups to configure policy rules and the objects they reference. You can organize device groups hierarchically, with shared rules and objects at the top and device group-specific rules and objects at subsequent levels. Organization enables you to create a hierarchy of rules that enforces how firewalls handle traffic. For example, you can define a set of shared rules as a corporate acceptable use policy. Then, to allow only regional offices to access peer-to-peer traffic such as BitTorrent, you can define a device group rule that Panorama pushes only to the regional offices (or define a shared Security rule and target it to the regional offices).

#### 4.2.1 Device group hierarchies

##### *Device Groups*

You can create a device group hierarchy to nest device groups in a hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) of higher-level groups. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups (ancestors). At the top level, a device group can have child, grandchild, and great-grandchild device groups (descendants). All device groups inherit settings from the shared location, a container at the top of the hierarchy for configurations that are common to all device groups.

Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. For example, you could configure shared settings that are global to all firewalls, configure device groups with function-specific settings at the first level, and configure device groups with location-specific settings at lower levels. Without a hierarchy, you would have to configure both function-specific and location-specific settings for every device group in a single level under the shared location.



#### 4.2.2 Identify what device groups contain

Device groups enable a layered approach for managing policies across a network of managed firewalls. A firewall evaluates policy rules by layer (shared, device group, and local) and by type (pre-rules, post-rules, and default rules) in the order that is shown from top to bottom in the following figure.

Name	Tags	Type	Source				Destination		Rule Usage		
			Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit
Allow Web	none	universal	Trust-L3	any	any	any	Untrust-L3	any	2285	2017-11-14 20:17:53	2017-11-11 21:52:58
Outbound FTP	none	universal	Trust-L3	any	any	any	Untrust-L3	any	0	-	-
Local Policy	none	universal	Trust-L3	any	any	any	DMZ	any	-	-	-
Allow Facebook	none	universal	Trust-L3	any	any	any	Untrust-L3	any	0	-	-
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	6772	2017-11-14 20:17:23	2017-10-31 20:58:56
interzone-default	none	interzone	any	any	any	any	any	any	298702	2017-11-14 19:54:12	2017-10-31 21:02:50

Pre-Policy Rules

Local Policy Rules

Post-Policy Rules

Default Rules

#### 4.2.3 Differentiate between different use cases for pre-rules, local rules, default rules, and post-rules

When the firewall receives traffic, it performs the action defined in the first evaluated rule that matches the traffic and disregards all subsequent rules. Whether you view rules on a firewall or in Panorama, the web interface displays them in evaluation order. All the shared, device group, and default rules that the firewall inherits from Panorama are shaded orange. Local firewall rules display between the pre-rules and post-rules.

Objects are configuration elements that policy rules reference — for example, IP addresses, URL categories, Security Profiles, users, services, and applications. Rules of any type (pre-rules, post-rules, default rules, and rules locally defined on a firewall) and any rulebase (security, NAT, QoS, PBF, decryption, Application Override, Captive Portal, and DoS protection) can reference objects. You can reuse an object in any number of rules that have the same scope as that object in the device group hierarchy.

For example, if you add an object to the shared location, all rules in the hierarchy can reference that shared object because all device groups inherit objects from the shared location. If you add an object to a particular device group, only the rules in that device group and its descendant device groups can reference that device group object. If object values in a device group must differ from those inherited from an ancestor device group, you can override inherited object values. You also can revert to inherited object values at any time. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

When new policy rules are entered into a Panorama device group, the device group and the pre or post designation must be decided. The pre and post designations are chosen through selection of the appropriate policy menu item, as shown in the following figure.



#### 4.2.4 Identify the impact of configuring a primary device

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).

In a high availability (HA) configuration, you must use the same master key on both firewalls because the master key is not synchronized across HA peers. Otherwise, HA synchronization will not work properly.

If you are using Panorama to manage your firewalls, you can configure the same master key on Panorama and all managed firewalls or configure a unique master key for each managed firewall. For managed firewalls in an HA configuration, you must configure the same master key for each HA peer. See [Manage the Master Key from Panorama](#) if the firewall is managed by a Panorama™ management server.

Be sure to store the master key in a safe location. You cannot recover the master key and the only way to restore the default master key is to [Reset the Firewall to Factory Default Settings](#).

**Step 1:** Backup the configuration.

**Step 2:** (HA only) Disable Config Sync.

This step is required before deploying a new master key to any firewall HA pair

Before you deploy a new master key to any firewall HA pair, you must disable Config Sync. For Panorama-managed firewalls, if you do not disable Config Sync before deploying a new master key, Panorama loses connectivity to the primary firewall.

1. Select **Device > High Availability > General** and edit the **Setup**.
2. Disable (clear) **Enable Config Sync** and then click **OK**.
3. **Commit** your configuration changes.

**Step 3:** Select **Device > Master Key and Diagnostics** and edit the Master Key section.

**Step 4:** Enter the **Current Master Key** if one exists.

**Step 5:** Define a new **New Master Key** and then **Confirm New Master Key**. The key must contain exactly 16 characters.

**Step 6:** To specify the master key **Lifetime**, enter the number of **Days** and/or **Hours** after which the key will expire.

You must configure a new master key before the current key expires. If the master key expires, the firewall or Panorama automatically reboots in Maintenance mode. You must then Reset the Firewall to Factory Default Settings.

**Step 7:** Enter a **Time for Reminder** that specifies the number of **Days** and **Hours** before the master key expires when the firewall generates an expiration alarm. The firewall automatically opens the System Alarms dialog to display the alarm.

**Step 8:** Enable **Auto Renew Master Key** to configure the firewall to automatically renew the master key. To configure **Auto Renew With Same Master Key**, specify the number of **Days** and/or **Hours** to renew the same master key. The key extension allows the firewall to remain operational and continue securing your network; it is not a replacement for configuring a new key if the existing master key lifetime expires soon.

Automatically renewing the master key has benefits and risks. The benefit is that extending the master key **Lifetime** protects against failure to change the master key before its lifetime expires. The risk is that encryptions will repeat and cause a security risk if the number of encryptions the device performs with the master key exceeds the number of unique encryptions the master key can generate (232 unique encryptions).

**Step 9:** (Optional) For added security, select whether to use an **HSM** to encrypt the master key. For details, see [Encrypt a Master Key Using an HSM](#)

**Step 10:** Click **OK** and **Commit**.

**Step 11:** (HA only) Re-enable Config Sync.

1. Select **Device > High Availability > General** and edit the **Setup**.
2. Enable (check) **Enable Config Sync** and then click **OK**.
3. **Commit** your configuration changes.

#### 4.2.5 Assign firewalls to device groups

Device groups comprise firewalls and virtual systems you want to manage as a group, such as the firewalls that manage a group of branch offices or individual departments in a company. Panorama treats these groups as single units when applying policies. Firewalls can belong to only one device group, but, because virtual systems are distinct entities in Panorama, you can assign virtual systems within a firewall to different device groups.

You can nest device groups in a tree hierarchy of up to four levels under the shared location to implement a layered approach for managing policies across your network of firewalls. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups at successively higher levels — collectively called ancestors — from which the bottom-level device group inherits policies and objects. At the top level, a device group can have child, grandchild, and great-grandchild device groups — collectively called descendants. When you select **Panorama > Device Groups**, the **Name** column displays this device group hierarchy.

After adding, editing, or deleting a device group, perform a Panorama commit and device group commit (see [Panorama Commit Operations](#)). Panorama then pushes the configuration changes to the firewalls that are assigned to the device group. Panorama supports up to 1,024 device groups.

#### 4.2.6 Reference:

Configure the Master Key:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-the-master-key>

### 4.3 Manage firewall configurations within Panorama

#### 4.3.1 Licensing

The Panorama Software Firewall License plugin allows you to automatically license a VM-Series firewall when it connects to Panorama. If your VM-Series firewalls are located in the perimeter of your deployment and do

not have connectivity to the Palo Alto Networks licensing server, the Software Firewall License plugin simplifies the license activation process by using Panorama to license the VM-Series firewall.

Additionally, the Software Firewall License plugin simplifies the license activation and deactivation of VM-Series firewalls in environments that use auto-scaling and automation to deploy and delete firewalls to address changes in the cloud.

To install the Panorama Software Firewall License plugin, you must be using Panorama 10.0.0 or later and VM-Series plugin 2.0.4 or later. Your VM-Series firewalls must be running PAN-OS 9.1.0 or later.

### 4.3.2 Panorama commit recovery feature

When you initiate a commit, Panorama checks the validity of the changes before activating them. The validation output displays conditions that block the commit (errors) or that are important to know (warnings). For example, validation could indicate an invalid route destination that you need to fix for the commit to succeed. The validation process enables you to find and fix errors before you commit because no changes to the running configuration are made. This is useful if you have a fixed commit window and want to be sure the commit will succeed without errors.

### 4.3.3 Configuration settings for Panorama automatic commit recovery

Panorama automatic commit recovery enables you to configure the firewall to attempt a specified number of connectivity tests after you push a configuration change from Panorama or commit a configuration change locally on the firewall. Automatic commit recovery is enabled by default, thus enabling managed firewalls to locally test the configuration pushed from Panorama to verify that the new changes do not break the connection between Panorama and the managed firewall. If the committed configuration breaks the connection between Panorama and a managed firewall, then the firewall automatically fails the commit, and the configuration is reverted to the previous running configuration.

The firewall also checks connectivity to Panorama every hour to ensure consistent communication if unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration may have affected connectivity. If an hourly connectivity check fails, the firewall generates a system log to alert administrators of potential configuration or network connectivity issue. An event is generated in the system log when you disable the setting, when a connectivity test fails, or when a firewall configuration reverts to the last running configuration.

In HA firewall configurations, each HA peer performs connectivity tests independently of each other. HA configuration syncs may occur only after each HA successfully tests connectivity to Panorama and verifies its connection.

#### *Configuration Settings for Panorama Automatic Commit Recovery*

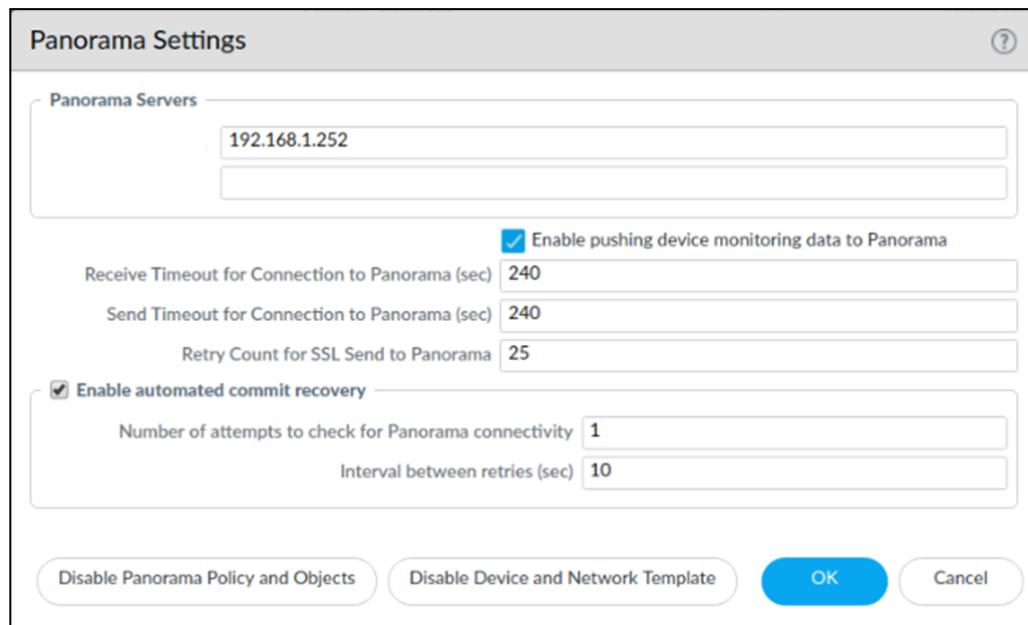
PAN-OS allows managed firewalls to check for connectivity to the Panorama management server and to automatically revert to the last running configuration when the firewall is unable to communicate with Panorama.

Automatic commit recovery enables you to configure the firewall to attempt a specified number of connectivity tests, as well as the interval at which each test occurs. Connectivity tests occur before the firewall automatically reverts its configuration to the previous running configuration after you push a configuration from Panorama or commit a configuration change locally on the firewall.

#### 4.3.4 Commit types and schedules

To commit types and schedules:

1. Log in to the Panorama web interface.
2. Select **Device > Setup > Management**.
3. In the **Template context** drop-down list, select the template or template stack that manages the devices for which you want to configure the automated commit recovery parameters. Configure the automated commit recovery settings:
  - a. Edit () the **Panorama Settings**.
  - b. Verify that **Enable automated commit recovery** is selected.
  - c. Enter a value in the **Number of attempts to check for Panorama connectivity** field.
  - d. Enter a value in the **Interval between retries** field.
  - e. Click **OK** to save your configuration changes.
4. Select **Commit**, and **Commit and Push** your configuration changes.



Verify that the automated commit recovery feature is enabled on your managed firewalls.

5. Launch the firewall web interface.
6. Select **Device > Setup > Management**. In **Panorama Settings**, verify that **Enable automated commit recovery** is selected.

### 4.3.5 Configuration backups

#### *Running Configuration and Candidate Configuration*

Firewall settings are stored in XML configuration files that can be archived, restored, and managed. A firewall contains both a running configuration that contains all settings currently active and a candidate configuration. The candidate configuration is a copy of the running configuration that also includes settings changes that are not yet committed. Changes you make using the management web interface, the CLI, or the XML API are staged in the candidate configuration until you perform a commit operation. During a commit operation, the candidate configuration replaces the running configuration.

#### *Panorama and Firewall Configuration Backups and Restorations*

When Panorama has a management relationship with a firewall, Panorama can obtain copies of both that firewall's Panorama-managed and locally managed configurations. After a commit on a local firewall that runs PAN-OS 5.0 or later, a backup is sent of the running configuration to Panorama. Any commits performed on the local firewall will trigger the backup, including any commits that an administrator performs locally on the firewall or that PAN-OS initiates and automatically commits (such as an FQDN refresh).

By default, Panorama stores up to 100 backups for each firewall, though this is configurable. To store Panorama and firewall configuration backups on an external host, you can schedule exports from Panorama or complete an export on demand. These saved configuration files can be restored to the firewall at any time by a Panorama administrator using the **Panorama > Managed Devices > Summary** tools.

#### *Return Merchandise Authorization Replacement of a Panorama-Managed Firewall*

To minimize the effort required to restore the configuration on a managed firewall, you can use a Return Merchandise Authorization to replace the serial number of the old firewall with that of the new firewall on Panorama. To then restore the configuration on the replacement firewall, either import a firewall state that you previously generated and exported from the firewall or use Panorama to generate a *partial device state* for managed firewalls running PAN-OS 5.0 and later versions. By replacing the serial number and importing the firewall state, you can resume using Panorama to manage the firewall.

### 4.3.6 Software and dynamic updates

#### *Dynamic Updates*

Palo Alto Networks frequently publishes dynamic updates to your firewall. This allows for security updates without the need to upgrade firmware.

## **Software Updates**

Schedule each content update. Set the schedule of each update.

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 firewalls up-to-date with the latest content and software updates published by Palo Alto Networks. The Dynamic Content Updates available to you depend on which Subscriptions you have.

Follow these steps to install content updates. You can also set a schedule for content updates, to define the frequency at which the firewall retrieves and installs updates.

Applications and Threats content updates work a little differently than other update types—to get the most out of the latest application knowledge and threat prevention, follow the guidelines to Deploy Applications and Threats Content Updates instead of the steps here.

**Step 1:** Ensure that the firewall has access to the update server.

- By default, the firewall accesses the **Update Server** at `updates.paloaltonetworks.com` so that the firewall receives content updates from the server to which it is closest. If your firewall has limited access to the Internet, it might be necessary to configure your allow list to enable access to servers involved in update downloads. For more information about content update servers, refer to Content Delivery Network Infrastructure for Dynamic Updates. If you want additional reference information or are experiencing connectivity and update download issues, please refer to <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU>.
- (Optional) Click **Verify Update Server Identity** for an extra level of validation to enable the firewall to check that the server's SSL certificate is signed by a trusted authority. This is enabled by default.
- (Optional) If the firewall needs to use a proxy server to reach Palo Alto Networks update services, in the **Proxy Server** window, enter:
  - **Server**—IP address or host name of the proxy server.
  - **Port**—Port for the proxy server. Range: 1-65535.
  - **User**—Username to access the server.
  - **Password**—Password for the user to access the proxy server. Re-enter the password at **Confirm Password**.
- (Optional) Configure up to three reconnection attempts if a connection failure occurs. Use `debug set-content-download-retry attempts` to set the number of connection attempts. The default is 0.

**Step 2:** Check for the latest content updates.

Select **DeviceDynamic Updates** and click **Check Now** (located in the lower left-hand corner of the window) to check for the latest updates. The link in the **Action** column indicates whether an update is available:

- **Download**—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 **Action** column changes from **Download to Install**.

▼ WildFire	Last checked: 2020/09/21 09:45:42 PDT	Schedule: None										<a href="#">Download</a>
515237-522316	panupv3-all-wildfire-515237-522316.candidate	PAN OS 10.0 And Later	Full	8 MB	5a46cd783114c7627162...	2020/09/21 09:45:03 PDT						

- **Revert**—Indicates that a previously installed version of the content or software version is available. You can choose to revert to the previously installed version.

#### Step 3: Install the content updates.

Click the **Install** link in the **Action** column. When the installation completes, a check mark displays in the **Currently Installed** column.

▼ WildFire	Last checked: 2020/09/21 09:48:44 PDT	Schedule: None										<a href="#">Install</a>
515238-522317	panupv3-all-wildfire-515238-522317.candidate	PAN OS 10.0 And Later	Full	8 MB	aed1502259d57604f288...	2020/09/21 09:50:06 PDT	✓					

#### Step 4: Schedule each content update.

1. Set the schedule of each update type by clicking the **None** link.

▼ WildFire	Last checked: 2020/09/21 09:48:44 PDT	Schedule: <a href="#">None</a>
515238-522317	panupv3-all-wildfire-515238-522317.candidate	PA

2. Specify how often you want the updates to occur by selecting a value from the **Recurrence** drop-down. The available values vary by content type (WildFire updates are available in **Real-time**, **Every Minute**, **Every 15 Minutes**, **Every 30 minutes**, or **Every Hour** whereas Applications and Threats updates can be scheduled for **Weekly**, **Daily**, **Hourly**, or **Every 30 Minutes** and Antivirus updates can be scheduled for **Hourly**, **Daily**, or **Weekly**). You can also select **None (Manual)** for Applications and Threats or for Antivirus updates. This means there is no recurring schedule for this item and you must manually install updates. To fully remove the schedule node, select **Delete Schedule**.
3. Specify the **Time** and (or, minutes past the hour in the case of WildFire), if applicable depending on the **Recurrence** value you selected, **Day** of the week that you want the updates to occur.
4. Specify whether you want the system to **Download Only** or, as a best practice, **Download And Install** the update.
5. Enter how long after a release to wait before performing a content update in the **Threshold (Hours)** field. 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.
6. (Optional) Enter the **New App-ID Thresholds** in hours to set the amount of time the firewall waits before installing content updates that contain new App-IDs.

## Applications and Threats Update Schedule



Recurrence Weekly

Day wednesday

Time 01:02

Action download-and-install

Disable new apps in content update

Threshold (hours) 24

A content update must be at least this many hours old for the action to be taken.

### Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

New App-ID Threshold (hours) 24

Delete Schedule

OK

Cancel

7. Click **Ok** to save the schedule settings.
8. Click **Commit** to save the settings to the run configuration.

### Step 5: Update PAN-OS.

1. Review the [Release Notes](#).
2. [Update the PAN-OS software](#)

### 4.3.7 Import firewall configurations into Panorama

If you have already deployed Palo Alto Networks firewalls and configured them locally but now want to use Panorama to centrally manage them, you must perform pre-migration planning. This involves importing firewall configurations into Panorama and verifying that the firewalls function as expected after the transition. If some settings are unique to individual firewalls, you can continue accessing the firewalls to

manage the unique settings. You can manage any firewall setting by pushing its value from Panorama or by configuring it locally on the firewall, but you cannot manage the setting through both Panorama and the firewall. If you want to exclude certain firewall settings from Panorama management, you can either:

- Migrate the entire firewall configuration and then, on Panorama, delete the settings that you will manage locally on firewalls. You can override a template or template stack value that Panorama pushes to a firewall instead of deleting the setting on Panorama.
- Load a partial firewall configuration, including only the settings that you will use Panorama to manage.

Firewalls do not lose logs during the transition to Panorama management.

#### 4.3.8 Configure Log Collectors

Select **Panorama > Managed Collectors** to manage Log Collectors. When you add a new Log Collector as a managed collector, the settings you configure vary based on the location of the Log Collector and whether you deployed Panorama in a HA configuration. Setting include:

- **Dedicated Log Collector:** The **Interfaces** tab will not initially display when you add a Log Collector. You must enter the serial number (**Collector S/N**) of the Log Collector, click **OK**, and then edit the Log Collector to display the interface settings.
- **Default Log Collector local to the solitary (non-HA) or active (HA) Panorama management server:** After you enter the serial number (**Collector S/N**) of the Panorama management server, the **Collector** dialog displays only the disks, communication settings, and a subset of the general settings. The Log Collector derives its values for all other settings from the configuration of the Panorama management server.
- **(HA only) Default Log Collector local to the passive Panorama management server:** Panorama treats this Log Collector as remote, so you must configure it as you would configure a dedicated Log Collector.

#### 4.3.9 Check firewall health and status from Panorama

Panorama allows you to monitor the hardware resources and performance for managed firewalls. Panorama centralizes time-trended performance information (CPU, memory, CPS, and throughput), logging performance, environmental information (fans, RAID status, and power supplies) and correlates events — such as commits, content installs, and software upgrades — to health data. When a firewall deviates from its calculated baseline, Panorama reports it as a deviating device to help identify, diagnose, and resolve any hardware issues quickly.

### 4.3.10 Configure role-based access control on Panorama

Role-based access control enables you to define the privileges and responsibilities of administrators. Every administrator must have a user account that specifies a role and authentication method. Administrative roles define access to specific configuration settings, logs, and reports within Panorama and firewall contexts. For device group and template administrators, you can map roles to access domains, which define access to specific device groups, templates, and firewalls through context switching. By combining each access domain with a role, you can enforce the separation of information among the functional or regional areas of your organization. For example, you can limit an administrator to monitoring activities for data center firewalls but allow that administrator to set policies for test lab firewalls. By default, every Panorama appliance (virtual appliance or M-Series appliance) has a predefined administrative account (admin) that provides full read-write access (superuser access) to all functional areas and to all device groups, templates, and firewalls. For each administrator, you can define an Authentication Profile that determines how Panorama verifies user access credentials.

### 4.3.11 References

For more information, refer to the link below:

[Use Panorama-Based Software Firewall License Management \(paloaltonetworks.com\)](https://paloaltonetworks.com/docs/panorama/10-2/panorama-admin/panorama-overview/panorama-use/)

Panorama Commit, Validation, and Preview Operations:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/panorama-commit-validation-and-preview-operations>

Enable Automated Commit Recovery:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/enable-automated-commit-recovery>

Schedule Dynamic Content Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/schedule-dynamic-content-updates>

Install Content Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/install-content-and-software-updates>

Manage Configuration Backups:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-configuration-backups>

Manage Panorama and Firewall Configuration Backups:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/manage-panorama-and-firewall-configuration-backups>

Replace an RMA Firewall:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/troubleshooting/replace-an-rma-firewall>

Backing Up and Restoring Configurations:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRcCAK>

Panorama > Managed Devices > Health:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health>

Transition a Firewall to Panorama Management:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management.html>

Log Collector Configuration:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-managed-collectors/log-collector-configuration>

### 4.3.12 Sample Questions

1. What is the format of the firewall configuration files?

- a. YAML
- b. JSON
- c. XML
- d. CSV

2. Which method can be used to restore the previous configuration when a new configuration committed on a firewall has undesired consequences?

- a. Use the load configuration version to restore the previous configuration settings, and follow with a commit.
- b. Use the rollback commit link in the commit completion message.
- c. Use the import device state to restore the pre-commit configuration.
- d. Use the load named configuration snapshot to restore the previous configuration, and follow with a commit.

3. Which CLI command do you use to move a configuration file from an external server to a firewall's local storage?

- a. rdist
- b. ssh
- c. scp
- d. rcp

4. Where in Panorama do you enter Security policy rules to ensure that your new rules will take precedence over locally entered rules?

- a. Security policy rules with a targeted firewall
- b. default rules section of Security policy rules
- c. pre-rules section of Security policy rules
- d. post-rules section of Security policy rules

5. In Panorama, how should you make changes to a Security policy rule for a specific firewall?

- a. Log in to Panorama, clone the rule, modify the clone, and add a target firewall to the new rule.
- b. Select the rule, click the override button, and enter the changes.
- c. Create a new locally defined Security policy rule that is placed higher in the rule list than the rule to be overridden.
- d. Log in to Panorama and modify the original rule.

6. Which three firewall settings are stored in Panorama device groups? (Choose three.)

- a. User Identification configuration
- b. custom Application-ID signatures
- c. services definitions
- d. DoS Protection profiles
- e. data plane interface configurations
- f. Zone Protection profiles
- g. Server Profile for an external LDAP server

# Domain 5- Manage and Operate

## 5.1 Manage and configure log forwarding

The Palo Alto Networks firewall contains several important features to identify log events and to forward the events to external monitoring solutions. The firewall also can extract IP addresses from events and add tags to them to include them in Dynamic Address Groups managed by the firewall. These groups can be used in Security policy rules to provide a higher level of security treatment.

### 5.1.1 Identify log types and criticalities

#### *Log Forwarding, Filtering, and Tagging*

Log Forwarding Profiles can be used to filter and forward logs from the following firewall logs:

- Authentication
- Data Filtering
- Decryption
- Traffic
- Threat
- Tunnel
- URL Filtering
- WildFire Submissions

#### *Methods Used to Forward Logs*

Two main methods are used to forward log events, depending on the log message type: redirecting log events based on event types, and redirecting log events to different systems.

Log events destined for the System, Config, User-ID, HIP Match, and IP-Tag logs can be redirected using specific event types. These types can be configured in **Device > Log Settings**, as illustrated in the following figure:

## Method 1

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. On the left, the navigation menu includes 'Log Settings' under 'Log Settings'. The main area displays a table for 'System' log types:

NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP
system-informational		(severity eq informational)	<input checked="" type="checkbox"/>	
system-low		(severity eq low)	<input checked="" type="checkbox"/>	
system-medium		(severity eq medium)	<input checked="" type="checkbox"/>	
system-high		(severity eq high)	<input checked="" type="checkbox"/>	

A callout box contains the text: "Choose event destination(s) for specific event types."

Log events can also be redirected to other systems, such as Panorama, SIEM products, and the syslog server, using a Log Forwarding Profile. A Log Forwarding Profile can route traffic, threat, WildFire, and other log events, as illustrated in the following figure:

## Method 2

The screenshot shows the 'Log Forwarding Profile Match List' dialog box. On the left, there is a sidebar for 'Log Forwarding Profile' settings. A callout box on the left says: "Select log type from dropdown." The main area has sections for 'Name' and 'Description', and a 'Forward Method' section. The 'Forward Method' section contains tables for 'SNMP' and 'SYSLOG' destinations, each with 'Add' and 'Delete' buttons. A callout box at the bottom right says: "Select the external destination(s)."

Log Forwarding Profiles are attached to individual firewall Security policy rules to enable forwarding events associated with specific policies. These profiles include one or more Log Forwarding Profile match lists. This granularity allows administrators specific control of forwarding and the potential to customize forwarding for policies of differing importance.

All forwarded events are sent to their destination as they are generated on the firewall. Palo Alto Networks also offers Cortex Data Lake, a cloud-based solution that can serve as a central repository for forwarded logs from multiple Palo Alto Networks devices. This central pool of log data is fully accessible to the owner, and it acts as an optional base for further third-party security applications through the Palo Alto Networks Cortex API.

### ***Log Forwarding Profiles***

To maximize the efficiency of your incident response and monitoring operations, you can create custom log forwarding filters based on any log attributes (such as threat type or source user). Instead of forwarding all logs or logs with specific severity levels, you can use the filters to forward only the information you need. For example, a security operations analyst who investigates malware attacks might be interested only in Threat logs with the type attribute set to wildfire-virus.

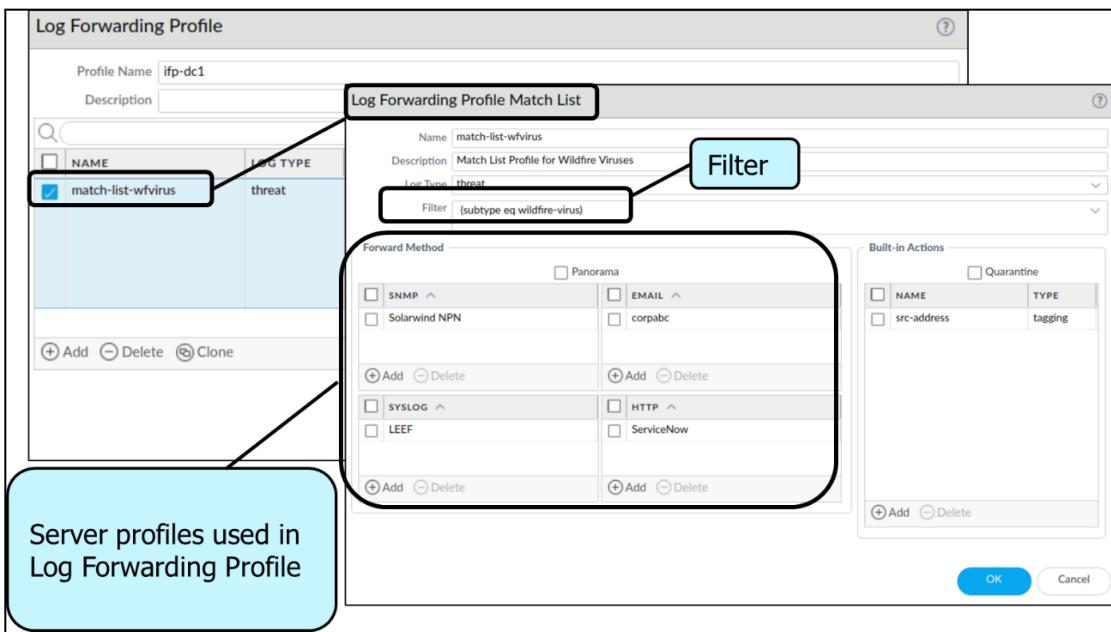
Follow these steps to create a custom log forwarding filter:

1. Configure a Server Profile for each external service that will receive logs from the firewall. The profiles define how the firewall connects to the services.

For example, to configure an HTTP Server Profile, select **Device > Server Profiles > HTTP**, and **Add** the profile.

2. Select **Objects > Log Forwarding**, and **Add a Log Forwarding Profile** to define the destinations for Traffic, Threat, WildFire Submissions, URL Filtering, Data Filtering, Tunnel, and Authentication logs.

In each Log Forwarding Profile, **Add** one or more match list profiles to specify log query filters, forwarding destinations, and automatic actions such as tagging.



In each match list profile, select **Filter > Filter Builder**, and **Add** filters based on log attributes.

3. Assign the Log Forwarding Profile to policy rules and network zones.

The firewall generates and forwards logs based on traffic that matches the rules and zones. Security, authentication, and DoS protection rules support log forwarding. For example, to assign the profile to a Security rule, select **Policies > Security**, edit the rule, select **Actions**, and select the **Log Forwarding Profile** you created.

4. Select **Device > Log Settings**, and configure the destinations for System, Configuration, User-ID, HIP Match, IP-Tag, and Correlation logs. For each log type that the firewall will forward, **Add** one or more match list profiles as you did in the Log Forwarding Profile.
5. Commit your changes.

### 5.1.2 Manage external services

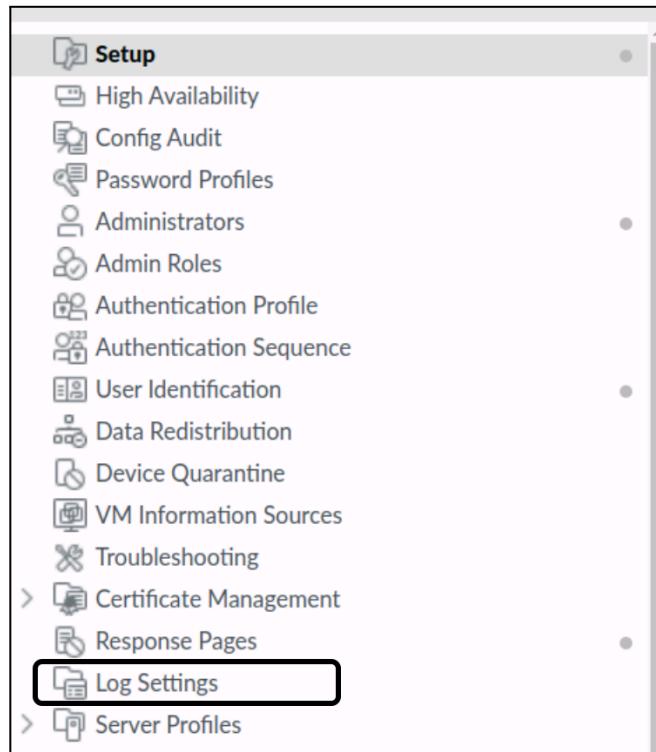
#### *Destination Log Types and Formatting*

External forwarding supports the following types of destinations:

- SNMP traps
- Syslog
- HTTP server
- Email
- Panorama

## **Filtering and Forwarding Log Events**

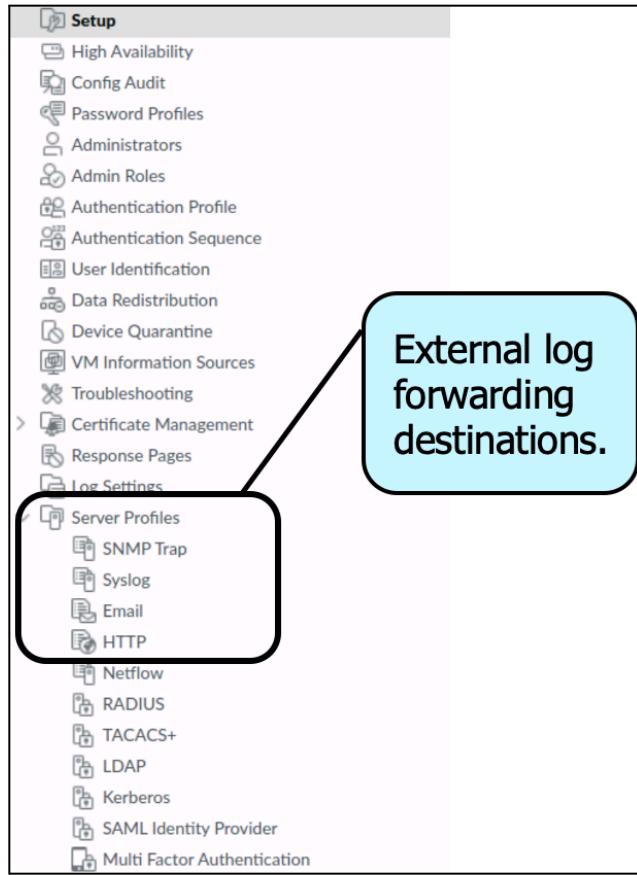
The Palo Alto Networks firewall has two primary methods to forward log events, depending on the log message type. Events associated with examined traffic use Log Forwarding Profiles. Events generally related to non-traffic-specific firewall activity can be filtered and forwarded using **Log Settings**, found in **Device > Log Settings**.



Log forwarding of any event type can send copies of log events to external destinations supporting the following data formats:

- SNMP
- Email
- Syslog
- HTTP

Each log forwarding destination is configured in the firewall with a Server Profile of the appropriate type. Navigate to **Device > Server Profiles**, and create a profile for each specific destination.



After the destination's Server Profile is created, it can be used in a Log Forwarding Profile.

All types (other than Panorama) support customization of the message format. A typical destination configuration is as follows:

The screenshot shows the PA-VM Device interface with the 'DEVICE' tab selected. On the left, a sidebar lists various profiles and databases. In the center, a table titled 'Syslog Server Profile' is displayed with one entry: 'Name: ThreatAmalgamation', 'SYSLOG SERVER: 192.168.2.20', 'TRANSPORT: UDP', 'PORT: 514', 'FORMAT: BSD', and 'FACILITY: LOG\_USER'. A callout box points to the 'Custom Log Format' tab in the 'Servers' section of the dialog, with the text: 'Click here to customize the message format.'

Email message formats can be customized. Here is an example:

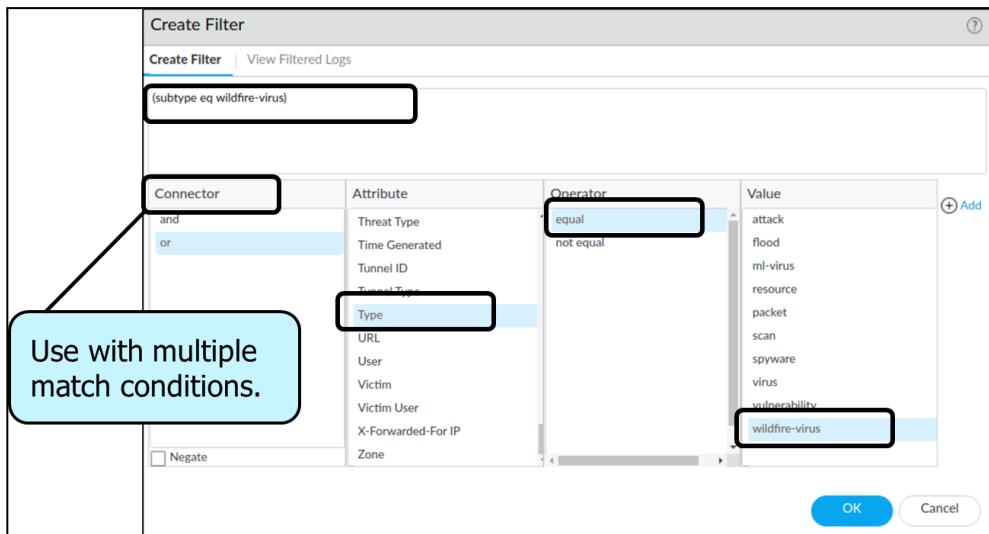
The screenshot shows the Email Server Profile interface with the 'Edit Log Format' dialog open. The 'Custom Log Format' tab is selected. A callout box points to the 'Threat Log Format' text area, which contains the template: 'A firewall threat was detected. A threat of type \$type was detected by firewall policy \$rule From \$src To \$dst Severity \$severity at time \$time\_generated'. Another callout box points to the 'Enter the custom message format here.' placeholder in the 'Threat Log Format' area.

Any log event redirection causes a copy of the log event to be forwarded as specified. It is logged on the firewall as usual.

### 5.1.3 Create and manage tags

#### Automated Actions and Tagging with Log Forwarding

Log Forwarding Profiles also provide a mechanism to collect the source or destination IP address of the event and tag it. The tag then can be used to assign the address to a Dynamic Address Group that is used in a Security policy rule.



Steps to configure tags:

**Step 1:** Add the action to perform.

Add or remove a tag to the source or destination IP address in a log entry automatically, and register the IP address and tag mapping to a User-ID agent on the firewall or Panorama. You can also map the tag to a remote User-ID agent so that you can respond to an event and dynamically enforce Security policy. The ability to tag an IP address and dynamically enforce policy using Dynamic Address Groups gives you better visibility, context, and control for consistently enforcing Security policy irrespective of where the IP address moves across your network.

**Step 2:** Configure the following settings:

1. Add an action, and enter a **Name** to describe it.
2. Select the target IP address that you want to tag: **Source Address or Destination Address**.

You can take an action for all log types that include a source or destination IP address in the log entry. In Correlation and HIP Match logs, you can tag the source IP address only. You cannot configure an action for System logs and Configuration logs because the log type does not include an IP address in the log entry.

3. Select the action: **Add Tag** or **Remove Tag**.
4. Select whether to register the IP address and tag mapping to the **Local User-ID agent** on this firewall, to **Panorama User-ID**, or to a **Remote User-ID agent**.

- To register the IP address and tag mapping to a Remote User-ID agent, select the HTTP Server Profile (**Device > Server Profiles > HTTP**) that will enable forwarding.
- Configure the **IP-Tag Timeout** to set, in minutes, the amount of time that IP address-to-tag mapping is maintained. Setting the timeout to 0 means that the IP-Tag mapping does not time out (range is 0 to 43200 [30 days]; default is 0).
- Enter or select the **Tags** you want to apply or remove from the target source or destination IP address. Within the Log Forwarding Profile, you can define a **Built-in Action**.

#### 5.1.4 Identify system and traffic issues using the web interface and CLI tools

The PAN-OS web UI provides firewall intelligence about traffic and user patterns using monitoring reports. The dashboard, ACC, firewall reports, and system logs on the firewall allow you to monitor activity on your network. You can use predefined templates to generate reports. Additionally, you can configure the firewall to forward monitored information as email notifications, syslog messages, SNMP traps, and NetFlow accounting and traffic records to external services.

You can also troubleshoot Palo Alto Networks firewalls using CLI commands. Here's a short list of CLI commands:

- show system info:** Displays the uptime, serial number, and more
- show session info:** Displays packet rate, number of sessions, and more
- show running resource-monitor:** Displays resource stats
- show session info:** Displays packet rate, number of sessions, and more
- show system statistics session:** Displays live stats about the current session
- ping host 8.8.8.8:** Displays the ping request from the management interface
- traceroute host 8.8.8.8:** Displays stats on the outgoing interface

#### 5.1.5 Configure Log Forwarding Profile and device log settings

In an environment where you use multiple firewalls to control and analyze network traffic, any single firewall can display logs and reports only for the traffic it monitors. Because logging in to multiple firewalls can make monitoring a cumbersome task, you can more efficiently achieve global visibility into network activity by forwarding the logs from all firewalls to Panorama or external services. If you Use External Services for Monitoring, the firewall automatically converts the logs to the necessary format: syslog messages, SNMP traps, email notifications, or as an HTTP payload to send the log details to an HTTP(S) server. In cases where some teams in your organization can achieve greater efficiency by monitoring only the logs that are relevant to their operations, you can create forwarding filters based on any log attributes (such as threat type or source user). For example, a security operations analyst who investigates malware attacks might be interested only in Threat logs with the type attribute set to wildfire-virus.

**Step 1:** Configure a server profile for each external service that will receive log information.

Configure one or more of the following server profiles:

- (Required for SMTP over TLS) If you have not already done so, create a [certificate profile](#) for the email server.
- To enable the SNMP manager (trap server) to interpret firewall traps, you must load the Palo Alto Networks [Supported MIBs](#) into the SNMP manager and, if necessary, compile them. For details, refer to your SNMP management software documentation.
- If the syslog server requires client authentication, you must also [5](#)
- Configure an HTTP server profile (see [Forward Logs to an HTTP/S Destination](#)).

**Step 2:** Create a Log Forwarding profile.

The profile defines the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel and Authentication logs.

- Select **Objects > Log Forwarding** and **Add** a profile.
- Enter a **Name** to identify the profile.

If you want the firewall to automatically assign the profile to new security rules and zones, enter default. If you don't want a default profile, or you want to override an existing default profile, enter a **Name** that will help you identify the profile when assigning it to security rules and zones.

- **Add** one or more `match list` profiles.

The profiles specify log query filters, forwarding destinations, and automatic actions such as tagging.

For each match list profile:

- Enter a **Name** to identify the profile.
- Select the **Log Type**.
- In the **Filter** drop-down, select **Filter Builder**. Specify the following and then **Add** each query:
  - **Connector** logic (and/or)
  - **Log Attribute**
  - **Operator** to define inclusion or exclusion logic
  - **Attribute Value** for the query to match
- Select **Panorama** if you want to forward logs to Log Collectors or the Panorama management server.
- For each type of external service that you use for monitoring (SNMP, Email, Syslog, and HTTP), **Add** one or more server profiles.
- (Optional, GlobalProtect Only) If you are using a log forwarding profile with a security policy to automatically quarantine a device using GlobalProtect, select **Quarantine** in the **Built-in Actions** area.
- Click **OK** to save the Log Forwarding profile.

Step 3: Assign the Log Forwarding profile to policy rules and network zones.

Security, Authentication, and DoS Protection rules support log forwarding. In this example, you assign the profile to a Security rule.

Perform the following steps for each rule that you want to trigger log forwarding:

- Select **Policies > Security** and edit the rule.
- Select **Actions** and select the **Log Forwarding** profile you created.
- Set the **Profile Type** to **Profiles or Group**, and then select the security profiles or Group Profile required to trigger log generation and forwarding for:

Threat logs—Traffic must match any security profile assigned to the rule.

WildFire Submission logs—Traffic must match a WildFire Analysis profile assigned to the rule.

- For Traffic logs, select **Log At Session Start** and/or **Log At Session End**.
- Click **OK** to save the rule.

Step 4: Configure the destinations for System, Configuration, Correlation, GlobalProtect, HIP Match, and User-ID logs.

- Select **Device > Log Settings**.
- For each log type that the firewall will forward, see Step Add one or more match list profiles.

Step 5: (PA-7000 Series firewalls only) Configure a log card interface to perform log forwarding.

- Select **Network > Interfaces > Ethernet** and click **Add Interface**.
- Select the **Slot** and **Interface Name**.
- Set the **Interface Type** to **Log Card**.
- Enter the **IP Address**, **Default Gateway**, and (for IPv4 only) **Netmask**.
- Select **Advanced** and specify the **Link Speed**, **Link Duplex**, and **Link State**.
- Click **OK** to save your changes.

Step 6: (PA-5450 firewall only) Configure a log interface to perform log forwarding.

(PAN-OS 10.2.0 and 10.2.1) The management interface handles log forwarding by default unless you configure a specific service route for log forwarding.

(PAN-OS 10.2.2 and later releases) The management interface handles log forwarding by default unless you configure the log interface or a specific service route for log forwarding. If a log interface is configured and committed, all internal logging, CDL, SNMP, HTTP, and Syslog will be forwarded by the log interface.

- Select **DeviceSetupManagement**.
- Select the settings gear on the top menu bar of **Log Interface**.
- Fill in the **IP Address**, **Netmask**, and **Default Gateway** fields.
- If your network uses IPv6, fill in the **IPv6 Address** and **IPv6 Default Gateway** fields instead.
- Specify the **Link Speed**, **Link Duplex**, and **Link State**.

- Click **OK** to save your changes.

#### **Step 7: Commit** and verify your changes.

- Commit your changes.
- Verify the log destinations you configured are receiving firewall logs:

Panorama—If the firewall forwards logs to a Panorama virtual appliance in Panorama mode or to an M-Series appliance, you must [configure a Collector Group](#) before Panorama will receive the logs. You can then [verify log forwarding](#).

Email server—Verify that the specified recipients are receiving logs as email notifications.

Syslog server—Refer to your syslog server documentation to verify it's receiving logs as syslog messages.

SNMP manager—[Use an SNMP Manager to Explore MIBs and Objects](#) to verify it's receiving logs as SNMP traps.

HTTP server—[Forward Logs to an HTTP/S Destination](#).

#### **5.1.6 Log monitoring**

A log is an automatically generated, time-stamped file that provides an audit trail for system events on the firewall or network traffic events that the firewall monitors. Log entries contain artifacts, which are properties, activities, or behaviors associated with the logged event, such as the application type or the IP address of an attacker. Each log type records information for a separate event type. For example, the firewall generates a Threat log to record traffic that matches a spyware, vulnerability, or virus signature or a DoS attack that matches the thresholds configured for a port scan or host sweep activity on the firewall.

#### **5.1.7 Customize logging and reporting settings**

##### **Logging and Reporting Settings**

Use this section to modify:

- Expiration periods and storage quotas for reports and for the following log types. The settings are synchronized across high availability pairs.
  - Logs of all types that the firewall generates and stores locally (**Device > Setup > Management**). The settings apply to all the virtual systems on the firewall.
  - Logs that an M-Series appliance or a Panorama virtual appliance in Panorama mode generates and stores locally: System, Config, Application Statistics, and User-ID™ logs (**Panorama > Setup > Management**).
  - Logs of all types that the Panorama virtual appliance in Legacy mode generates locally or collects from firewalls (**Panorama > Setup > Management**).

- Attributes for calculating and exporting user activity reports.
- Predefined reports created on the firewall or Panorama.

**Log Storage tab**

(Panorama management server and all firewall models except PA-5200 Series and PA-7000 Series firewalls)

Panorama displays this tab if you edit the Logging and Reporting Settings (Panorama > Setup > Management). If you use a Panorama template to configure the settings for firewalls (Device > Setup > Management), see Single Disk Storage and Multi Disk Storage tabs.

For each log type, specify:

- Quota**—The Quota, as a percentage, allocated on the hard disk for log storage. When you change a Quota value, the associated disk allocation changes automatically. If the total of all the values exceeds 100%, a message appears in red and an error message will appear if you try to save the settings. If this happens, adjust the percentages so that the total is within the 100% limit.
- Max Days**—The length (in days) of the log expiration period (range is 1 to 2,000). The firewall or Panorama appliance automatically deletes logs that exceed the specified period. By default, there is no expiration period, which means logs never expire.

The firewall or Panorama appliance evaluates logs during creation of the logs and then deletes logs that exceed the expiration period or quota size.

Weekly summary logs can age beyond the threshold before the next deletion if they reach the expiration threshold between times when the firewall deletes logs. When a log quota reaches the maximum size, new log entries start overwriting the oldest log entries. If you reduce a log quota size, the firewall or Panorama removes the oldest logs when you commit the changes. In an HA active/passive configuration, the passive peer does not receive logs and, therefore, does not delete them unless failover occurs and the passive peer becomes active.

**Session Log Storage and Management Log Storage tabs**  
**(PA-5200 Series and PA-7000 Series firewalls only)**

PA-5200 Series and PA-7000 Series firewalls store management logs and session logs on separate disks. Select the tab for each set of logs and configure the settings described in [Log Storage tab](#):

- **Session Log Storage**—Select **Session Log Quota** and set the quotas and expiration periods for Traffic, Threat, URL Filtering, HIP Match, User-ID, GTP/Tunnel, SCTP, and Authentication logs, as well as Extended Threat PCAPs.
- **Management Log Storage**—Set quotas and expiration periods for System, Config, and App Stats logs, as well as for HIP Reports, Data Filtering Captures, App PCAPs, and Debug Filter PCAPs.

**Single Disk Storage and Multi Disk Storage tabs**  
**(Panorama template only)**

If you use a Panorama template to configure log quotas and expiration periods, configure the settings in one or both of the following tabs based on the firewalls assigned to the template:

- **PA-5200 Series and PA-7000 Series firewalls**—Select **Multi Disk Storage** and configure the settings in the [Session Log Storage](#) and [Management Log Storage](#) tabs.



PA-5200 Series firewalls by default have a 0% quota allocated for **SCTP** log storage, **SCTP Summary**, **Hourly SCTP Summary**, **Daily SCTP Summary**, and **Weekly SCTP Summary**, so you must allocate some percentage for these firewalls to log SCTP information.

- **All other firewall models**—Select **Single Disk Storage**, select **Session Log Quota**, and configure the settings on the [Log Storage](#) tab.

- **Core Files**—If your firewall experiences a system process failure, it will generate a core file that contains details about the process and why it failed. If a core file is too large for the default core file storage location (/var/cores partition), you can enable the **large-core** file option to allocate an alternate and larger storage location (/opt/panlogs/cores). A Palo Alto Networks support engineer can increase the allocated storage if needed.

To enable or disable the **large-core** file option, enter the following CLI command from configuration mode and then commit the configuration:

```
# set deviceconfig setting management large-core [yes|no]
```



The core file is deleted when you disable this option.

You must use SCP from operational mode to export the core file:

```
> scp export core-file large-corefile
```



Only a Palo Alto Networks support engineer can interpret the contents of the core files.

- **Restore Defaults**—Select this option to revert to the default values.

**Session Log Storage and Management Log Storage tabs**  
**(PA-5200 Series and PA-7000 Series firewalls only)**

PA-5200 Series and PA-7000 Series firewalls store management logs and session logs on separate disks. Select the tab for each set of logs and configure the settings described in [Log Storage tab](#):

- **Session Log Storage**—Select **Session Log Quota** and set the quotas and expiration periods for Traffic, Threat, URL Filtering, HIP Match, User-ID, GTP/Tunnel, SCTP, and Authentication logs, as well as Extended Threat PCAPs.
- **Management Log Storage**—Set quotas and expiration periods for System, Config, and App Stats logs, as well as for HIP Reports, Data Filtering Captures, App PCAPs, and Debug Filter PCAPs.

**Single Disk Storage and Multi Disk Storage tabs**  
**(Panorama template only)**

If you use a Panorama template to configure log quotas and expiration periods, configure the settings in one or both of the following tabs based on the firewalls assigned to the template:

- **PA-5200 Series and PA-7000 Series firewalls**—Select **Multi Disk Storage** and configure the settings in the [Session Log Storage](#) and [Management Log Storage](#) tabs.



PA-5200 Series firewalls by default have a 0% quota allocated for **SCTP** log storage, **SCTP Summary**, **Hourly SCTP Summary**, **Daily SCTP Summary**, and **Weekly SCTP Summary**, so you must allocate some percentage for these firewalls to log SCTP information.

- **All other firewall models**—Select **Single Disk Storage**, select **Session Log Quota**, and configure the settings on the [Log Storage](#) tab.

#### Log Export and Reporting tab

Configure the following log export and reporting settings as needed:

- **Number of Versions for Config Audit**—Enter the number of configuration versions to save before discarding the oldest ones (default is 100). You can use these saved versions to audit and compare changes in configuration.
- **Number of Versions for Config Backups**—(**Panorama only**) Enter the number of configuration backups to save before discarding the oldest ones (default is 100).
- **Max Rows in CSV Export**—Enter the maximum number of rows that will appear in the CSV reports generated when you **Export to CSV** from the traffic logs view (range is 1 to 1,048,576; default is 65,535).
- **Max Rows in User Activity Report**—Enter the maximum number of rows that is supported for the detailed user activity reports (range is 1 to 1,048,576; default is 5,000).

#### Log Export and Reporting tab (cont)

- **Average Browse Time (sec)**—Configure this variable to adjust how the browse time is calculated in seconds for the [Monitor > PDF Reports > User Activity Report](#) (range is 0 to 300 seconds; default is 60).  
The calculation will ignore sites categorized as web advertisements and content delivery networks. The browse time calculation is based on container pages logged in the URL filtering logs. Container pages are used as the basis for this calculation because many sites load content from external sites that should not be considered. For more information on the container page, see [Container Pages](#). The average browse time setting is the average time that the administrator thinks it should take a user to browse a web page. Any request made after the average browse time has elapsed will be considered a new browsing activity. The calculation will ignore any new web pages that are loaded between the time of the first request (start time) and the average browse time. This behavior was designed to exclude any external sites that are loaded within the web page of interest. Example: If the average browse time setting is 2 minutes and a user opens a web page and views that page for 5 minutes, the browse time for that page will still be 2 minutes. This is done because there is no way to determine how long a user views a given page.
- **Page Load Threshold (sec)**—Allows you to adjust the assumed time (in seconds) that it takes for page elements to load on the page (range is 0 to 60; default is 20). Any request that occurs between the first page load and the page load threshold is assumed to be elements of the page. Any requests that occur outside of the page load threshold is assumed to be the user clicking a link within the page. The page load threshold is also used in the calculations for the [Monitor > PDF Reports > User Activity Report](#).
- **Syslog HOSTNAME Format**—Select whether to use the FQDN, hostname, or IP address (IPv4 or IPv6) in the syslog message header. This header identifies the firewall or Panorama management server where the message originated.
- **Report Runtime**—Select the time of day (default is 2 a.m.) when the firewall or Panorama appliance starts generating daily scheduled reports.
- **Report Expiration Period**—Set the expiration period (in days) for reports (range is 1 to 2,000). By default, there is no expiration period, which means reports never expire. The firewall or Panorama appliance deletes expired reports nightly at 2 A.M. according to its system time.

- **Stop Traffic when LogDb full** (**Firewall only**; disabled by default)—Select this option if you want traffic through the firewall to stop when the log database is full.
- **Enable Threat Vault Access** (enabled by default)—Enables the firewall to access the **Threat Vault** to gather the latest information about detected threats. This information is available for threat logs and for top threat activity charted on the ACC.
- **Enable Log on High DP Load** (**Firewall only**; disabled by default)—Select this option to specify that a system log entry is generated when the packet processing load on the firewall is at 100% CPU utilization.



**Enable Log on High DP Load** allows administrators to investigate and identify the cause of high CPU utilization.

A high CPU load can cause operational degradation because the CPU does not have enough cycles to process all packets. The system log alerts you to this issue (a log entry is generated each minute) and allows you to investigate for probable cause.

- **Enable High Speed Log Forwarding** (**PA-5200 Series, PA-5450, and PA-7000 Series firewalls only**; only enabled in the PA-5450 by default)—As a best practice, select this option to forward logs to Panorama at up to a maximum rate of 120,000 logs per second. When disabled, the firewall forwards logs to Panorama at a maximum rate of only 80,000 logs per second.  
If you enable this option, the firewall does not store logs locally or display them in the **Dashboard**, **ACC**, or **Monitor** tabs. Additionally, you must [configure log forwarding to Panorama](#) to use this option.
- **Log Collector Status**—Displays status of whether the firewall successfully established a connection to the Distributed Log Collection architecture and is sending logs to it. If the firewall is also configured to send logs to the Logging Service, verify the **Logging Service Status**, in the Logging Service section.

(**Panorama only**)

- **Buffered Log Forwarding from Device** (enabled by default)—Allows the firewall to buffer log entries on its hard disk (local storage) when it loses connectivity to Panorama. When the connection to Panorama is restored, the firewall forwards the log entries to Panorama; the disk space available for buffering depends on the log storage quota for the firewall model and the volume of logs that are pending roll over. If the available space is consumed, the oldest entries are deleted to allow logging of new events.  
 **Enable Buffered Log Forwarding from Device** to help prevent loss of logs if the connection to Panorama goes down.
- **Get Only New Logs on Convert to Primary** (disabled by default)—This option applies only to a Panorama virtual appliance in Legacy mode that writes logs to a Network File System (NFS). With NFS logging, only the primary Panorama is mounted to the NFS. Therefore, the firewalls send logs only to the active primary Panorama. This option enables you to configure firewalls to send newly generated logs only to Panorama when an HA failover occurs and the secondary Panorama resumes logging to the NFS (after it is promoted as primary). This option is typically enabled to prevent firewalls from sending a large volume of buffered logs when connectivity to Panorama is restored after a significant period of time.
- **Only Active Primary Logs to Local Disk** (disabled by default)—This option applies only to a Panorama virtual appliance in Legacy mode. This option enables you to configure only the active Panorama to save logs to the local disk.

- **Pre-Defined Reports** (enabled by default)—Pre-defined reports for application, traffic, threat, URL Filtering, and Stream Control Transmission Protocol (SCTP) are available on the firewall and on Panorama. Pre-defined reports for SCTP are available on the firewall and Panorama after SCTP Security is enabled in **Device > Setup > Management > General Settings**.

Because the firewalls consume memory resources in generating the results hourly (and forwarding it to Panorama where it is aggregated and compiled for viewing), to reduce memory usage, you can disable the reports that are not relevant to you. To disable a report, disable this option for the report.

Click **Select All** or **Deselect All** to entirely enable or disable the generation of pre-defined reports.



Before disabling a report, verify that there isn't a Group Report or a PDF Report using it. If you disable a predefined report assigned to a set of reports, the entire set of reports will have no data.

- **Log Admin Activity** (disabled by default)—Specify whether to generate an audit log when an administrator executes an operational command in the firewall CLI or navigates through the web interface. You must first successfully configure a syslog server before you can generate and forward an audit log.
  - **Operational Commands**—Generate an audit log when an administrator executes an operational or debug command in the CLI or an operational command that is triggered from the web interface. See the [CLI Operational Command Hierarchy](#) for a full list of PAN-OS operational and debug commands.
  - **UI Actions**—Generate an audit log when an administrator navigates throughout the web interface. This includes navigation between configuration tabs, as well as between individual objects within a tab. For example, an audit log is generated when an administrator navigates from the **ACC** to the **Policies** tab. Additionally, an audit log is generated when an administrator navigates from **Objects > Addresses to Objects > Tags**.
  - **Syslog Server**—Select the target syslog server profile to forward audit logs.

## 5.1.8 References

Monitoring:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring>

Device > Setup > Management

[https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-setup-management.html#/id008c489e-9f57-4e0c-a430-e2a2c3420bcf\\_id9eebf60f-ec76-480e-9922-489e214c37de](https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-setup-management.html#/id008c489e-9f57-4e0c-a430-e2a2c3420bcf_id9eebf60f-ec76-480e-9922-489e214c37de)

CLI Cheat Sheet: Networking:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking>

Configure Log Forwarding:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/configure-log-forwarding>

Cortex Data Lake:

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake>

What Data Center Traffic to Log and Monitor:

<https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/log-and-monitor-data-center-traffic/what-data-center-traffic-to-log-and-monitor>

### 5.1.9 Sample Questions

1. Dynamic tags can be assigned to which kind of data in a log event?
  - a. source and destination address, source and destination zone name
  - b. source and destination address
  - c. interface, zone name
  - d. DNS name, zone name
2. How can an administrator use dynamically tagged objects to block traffic?
  - a. Add the object to an enforcement list of a data filtering object that then is attached to a Security policy rule.
  - b. Assign the object to a dynamic list, which then is included in the destination address matching condition of a Security policy rule.
  - c. Assign the object to a Dynamic Address Group object, which then is added to the destination address matching condition of a Security policy rule.
  - d. Add the object to an Application Group and use it in Security policy rules.
3. A tag can be dynamically assigned to data in which four types of logs? (Choose four.)
  - a. Traffic
  - b. Threat
  - c. URL Filtering
  - d. HIP Match
  - e. Tunnel Inspection
  - f. Configuration
  - g. System
4. Dynamic tagging activity is recorded in which log?
  - a. System
  - b. Configuration
  - c. IP-Tag
  - d. Data Filtering
5. A firewall can forward log events to which two types of log formats? (Choose two.)
  - a. XES
  - b. SNMP
  - c. HTTP
  - d. databases using XML format
  - e. NCSA
6. How does a firewall forward log events to an external destination?
  - a. Log events are sent in batches at the frequency specified in the destination's Server Profile.
  - b. Log events are queued and sent in batches at differing intervals, depending on the event severity.

- c. Log events are sent as quickly as the required QoS policy rule governing log event traffic allows.
  - d. Log events are sent in real time as the firewall generates them.
7. Which two firewall logs can be exported using the Scheduled Log Export function? (Choose two.)
- a. Configuration
  - b. System
  - c. Traffic
  - d. URL

## 5.2 Plan and execute the process to update a Palo Alto Networks system

For non-HA firewalls, software updates fall into two categories: subscription updates and PAN-OS upgrades.

### 5.2.1 Update a single firewall

#### *Standalone Firewalls*

Subscription updates are enabled through application of various licenses to the firewall. These updates are managed under **Device > Dynamic Updates**. Updates can be transferred directly from Palo Alto Networks on demand or by schedule control. In cases where the firewall does not have internet connectivity, these updates can be downloaded from the **Dynamic Updates** section of the Support portal site onto an administrator's system, uploaded through a management web interface connection, and then applied.

PAN-OS updates are managed in the **Device > Software** section of the web interface. New PAN-OS versions can be downloaded and installed without user disruption. A final system reboot must be performed to put the new PAN-OS software into production. This reboot is disruptive and should be done during a change control window.

A firewall does not need to upgrade to each released PAN-OS software in sequence. To ensure that software upgrades function as expected, you are required to install the latest dynamic updates before upgrading PAN-OS software.

Updates to App-ID signature information sometimes can reclassify previously labeled traffic, which might impact user access to critical applications. The firewall provides several mechanisms to review changes to App-IDs prior to or immediately after their installation.

### 5.2.2 Update HA pairs

#### *HA Firewalls*

Dynamic updates are the responsibility of the individual firewalls to manage, even when they are in passive mode while members of an active/passive HA pair. This task can be difficult if dynamic updates have no network path to the Palo Alto Networks update servers. Dynamic updates in HA clusters include an option to "sync-to-peer" for use when the secondary firewall has no network route to update firewalls in HA pairs or clusters. In active/passive HA pairs, a firewall typically is put into suspend mode and then upgraded. After the

upgrade is complete, the firewall is made active, and the partner firewall enters suspend mode and is upgraded.

### 5.2.3 Perform Panorama push

#### *Upgrading Firewalls Under Panorama Management*

Firewalls managed by Panorama can get dynamic updates from Panorama, including scheduled updates. PAN-OS upgrades also can be managed from Panorama. A pair of Panorama instances can be used to download software updates. One Panorama with a trusted internet connection can transfer updates to an SCP server, while the second Panorama deployed in an isolated network can use the SCP server as a software update server. The second Panorama can then download any updates and then send them to all managed devices.

#### *HA Cluster Firewall Updates Managed by Panorama*

Panorama treats managed firewalls in HA pairs as individual firewalls for software update purposes.

### 5.2.4 Schedule and manage dynamic updates

Palo Alto Networks frequently publishes dynamic updates to your firewall. This allows for security updates without the need to upgrade firmware.

### 5.2.5 References

Schedule Dynamic Content Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/schedule-dynamic-content-updates>

Software and Content Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates>

Determine the Upgrade Path to PAN-OS 10.2:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path>

Downgrade PAN-OS:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/downgrade-pan-os>

Manage New and Modified App-IDs:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases>

Scheduled Dynamic Updates in an HA Environment:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClrnCAC>

Upgrade an HA Firewall Pair:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-an-ha-firewall-pair>

Manage Software and Content Updates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/manage-software-and-content-updates>

Upgrade Firewalls Using Panorama:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-firewalls-using-panorama>

Automatic Content Updates Through Offline Panorama:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-panorama/install-content-and-software-updates-for-panorama/install-updates-automatically-for-panorama-without-an-internet-connection>

## 5.2.6 Sample Questions

1. Match the upgrade step description with the correct step number.

- |                                    |        |
|------------------------------------|--------|
| a. Upgrade PAN-OS software.        | Step 3 |
| b. Reboot the firewall.            | Step 4 |
| c. Update dynamic content.         | Step 2 |
| d. Activate subscription licenses. | Step 1 |

2. Match each component with the order in which the component should be upgraded to a new version of PAN-OS software.

- |                        |        |
|------------------------|--------|
| a. HA active firewall  | Step 4 |
| b. Panorama            | Step 1 |
| c. Log Collector       | Step 2 |
| d. HA passive firewall | Step 3 |

3. How do you upgrade an active/passive HA firewall pair to PAN-OS 10.1 while maintaining internet access?

- a. Upgrade the active firewall first, then the passive one.

- b. Upgrade the passive firewall first, then the active one.
- c. Run the upgrade on the active firewall. It will manage the process and upgrade the passive firewall.
- d. You must upgrade both members of the pair at the same time, which requires an upgrade window that allows downtime.

## 5.3 Manage HA functions

### 5.3.1 Link monitoring

#### *Settings Related to Critical HA Functions*

An HA pair configuration is created when two firewalls are placed in a group and have their configurations synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover if a peer becomes non-operational. Configure two firewalls in an HA pair to provide redundancy and to ensure business continuity.

An HA cluster can be configured with up to 16 firewalls or HA pairs acting in an all-active manner. HA clusters require an HA4 link to synchronize session state information, and they use link and path monitoring to determine the up/down state of cluster members. HA4 and potential HA4 backup links determine HA cluster member functionality.

#### *HA Functionality*

Network monitoring applications use SNMP to query network components such as the NGFW. The firewall has additional information that is specific to HA. You can monitor the dedicated HA1, HA2, HA2 backup, and HA3 interfaces. Use the IF-MIB and the interface's Management information base (MIB) to see SNMP statistics for dedicated HA2 interfaces.

Panorama includes *Managed Device Health Monitoring*, which displays limited HA status information in the summary display in the Panorama management web interface.

### 5.3.2 Path monitoring

It is same as Link monitoring.

### 5.3.3 HA links

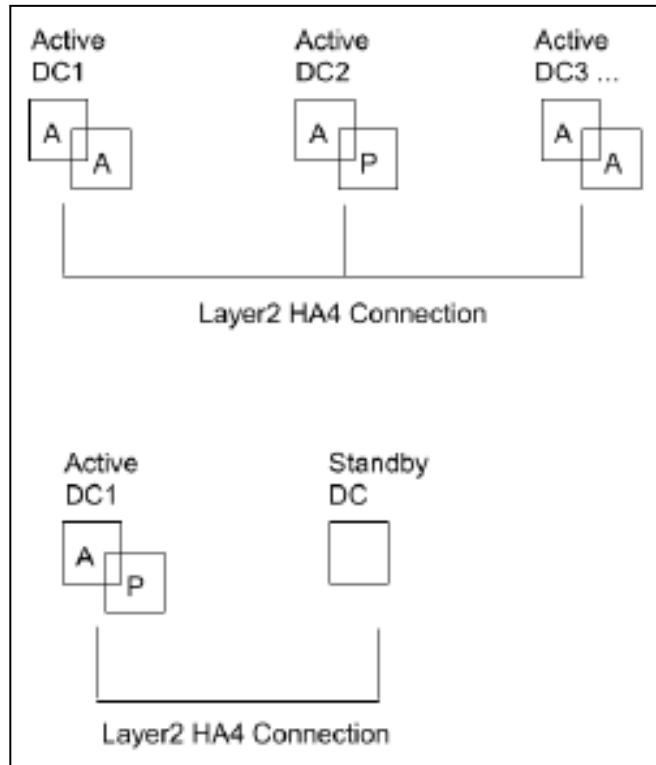
#### *HA Clustering*

Several Palo Alto Networks ML-powered NGFW models support session state synchronization in an HA cluster of up to 16 firewalls. The HA cluster peers synchronize sessions to protect against data center or large security inspection point failure with horizontally scaled firewalls. In the case of a network outage or a down firewall, the sessions fail over to a different firewall in the cluster.

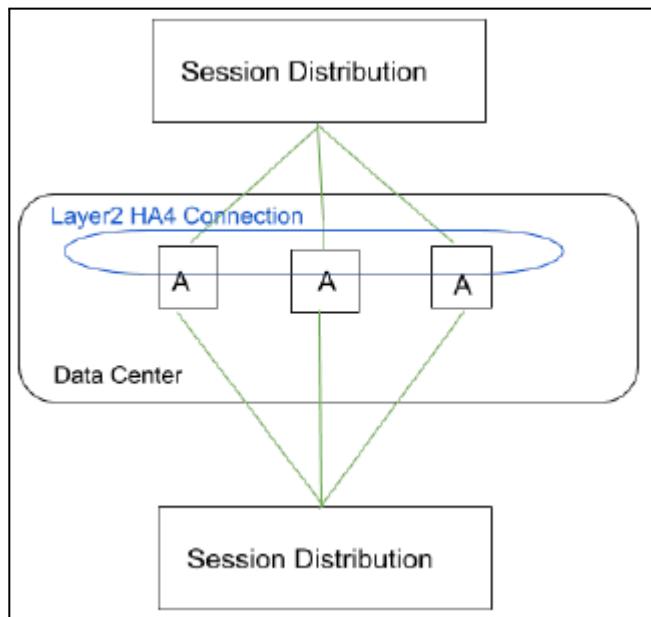
This synchronization is especially helpful in the following use cases:

- When HA peers are spread across multiple data centers

- When one data center is active and the other is on standby in a multi-data center deployment



- When you need to scale horizontally by adding HA cluster members to a single data center



All cluster members share session state. When a new firewall joins an HA cluster, it triggers all firewalls in the cluster to synchronize all existing sessions. HA4 and HA4 backup connections are the dedicated cluster links that synchronize session state among all cluster members with the same cluster ID. The HA4 link between cluster members detects connectivity failures between cluster members. HA1 (control link), HA2 (data link), and HA3 (packet-forwarding link) are not supported between cluster members that are not HA pairs.

### ***Choosing an HA Pair Type***

***When choosing an HA pair type, keep the following considerations in mind:***

- Active/passive mode has a simple design; it is significantly easier to troubleshoot routing and traffic flow issues in active/passive mode.
- Both active/active and active/passive mode support a virtual wire deployment.
- Active/active mode uses advanced design concepts that can result in more complex networks. Depending on how you implement active/active HA, it might require additional configuration, such as activating networking protocols on both firewalls, replicating NAT pools, and deploying floating IP addresses to provide proper failover. Because both firewalls are actively processing traffic, the firewalls use additional concepts of session owner and session setup to perform Layer 7 content inspection.
- Active/active mode is recommended if each firewall needs its own routing instances and you require full, real-time redundancy out of both firewalls all the time. Active/active mode has faster failover and can handle peak traffic flows better than active/passive mode because both firewalls are actively processing traffic.
- In active/active mode, the HA pair can be used to temporarily process more traffic than what one firewall normally can handle. However, this situation should not be standard because a failure of one firewall causes all traffic to be redirected to the remaining firewall in the HA pair. Your design must allow the remaining firewall to process the maximum capacity of your traffic loads with content inspection enabled. If the design oversubscribes the capacity of the remaining firewall, high latency or application failure can occur.
- In cases of virtual firewall deployments, the cloud architecture might limit your deployment choices. Consult the design and deployment documentation specific to your chosen cloud vendor.

### **5.3.4 Failover**

#### ***HA Pairs***

You can set up two Palo Alto Networks firewalls as an HA pair. HA allows you to minimize downtime by ensuring that an alternative firewall is available if the peer firewall fails. HA pairs comprise two firewalls of identical model, configuration, and licensing. They should be physically close to each other, but geographical separation also is supported. 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 configurations (such as the management interface IP address, administrator profiles,

HA-specific configurations, log data, and ACC information are not shared between peers. To get a consolidated application and log view across the HA pair, you must use Panorama. 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 as follows:

- 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 and Hello messages (heartbeat and Hello monitoring).
- A critical chip or software component fails (packet path health monitoring).

### 5.3.5 Active/active and active/passive

#### HA Pair Modes

Palo Alto Networks firewalls support stateful *active/passive* or *active/active* HA with session and configuration synchronization with a few exceptions:

- The VM-Series firewall in Amazon Web Services supports active/passive HA only; if the firewall is deployed with Amazon Elastic Load Balancing (ELB), it does not support HA. (In this case, ELB provides the failover capabilities.)
- The VM-Series firewall in Microsoft Azure does support active/passive HA in PAN-OS 9x or later.
- The VM-Series firewall deployed in Google Cloud Platform supports both active/active and active/passive HA.

Public cloud deployments of VM-Series firewalls also are supported in each vendor's version of a "scaled" implementation, thus allowing virtual firewalls to share the traffic load through a deployment of parallel firewall instances and providing the option to create or remove firewall instances with changing traffic loads. These deployments all include the cloud vendor's load balancer deployed in front of the firewall "scale set" to manage the spreading of the traffic across the available firewalls. This same deployment practice also creates an HA scenario in the sense that failing firewall instances can be removed from the scale set automatically using various detection abilities within the load balancer. A limitation of the scale set methods of HA is that there typically is no synchronization between firewalls, so failovers are disruptive in the sense that existing sessions are terminated.

#### Active/Passive Pairs

Active/passive HA usually is the recommended deployment method. One firewall actively manages traffic while the other is synchronized and ready to transition to the active state if a failure occurs. In this mode, both firewalls share the same configuration settings, and one actively manages traffic until a path, link, or system failure occurs. When the active firewall fails, the passive firewall transitions to the active state, takes over seamlessly, and enforces the same policies to maintain network security. The firewalls synchronize their session state tables, thus allowing the passive partner to become active and continue servicing active sessions at failover. Active/passive HA is supported in virtual wire, Layer 2, and Layer 3 deployments.

Because one firewall is handling traffic and both firewalls share the same traffic interface configuration, active/passive usually is much easier to manage.

### ***Active/Active Pairs***

In active/active HA, both firewalls in the pair are active and processing traffic. They work synchronously to handle session setup and session ownership. Both firewalls individually maintain session tables and routing tables and synchronize to each other. Active/active HA is supported in virtual wire and Layer 3 deployments.

In active/active HA mode, the firewall HA interfaces cannot receive addresses via DHCP. Furthermore, only the active-primary firewall's traffic interface can function as a DHCP relay. The active-secondary firewall that receives DHCP broadcast packets drops them.

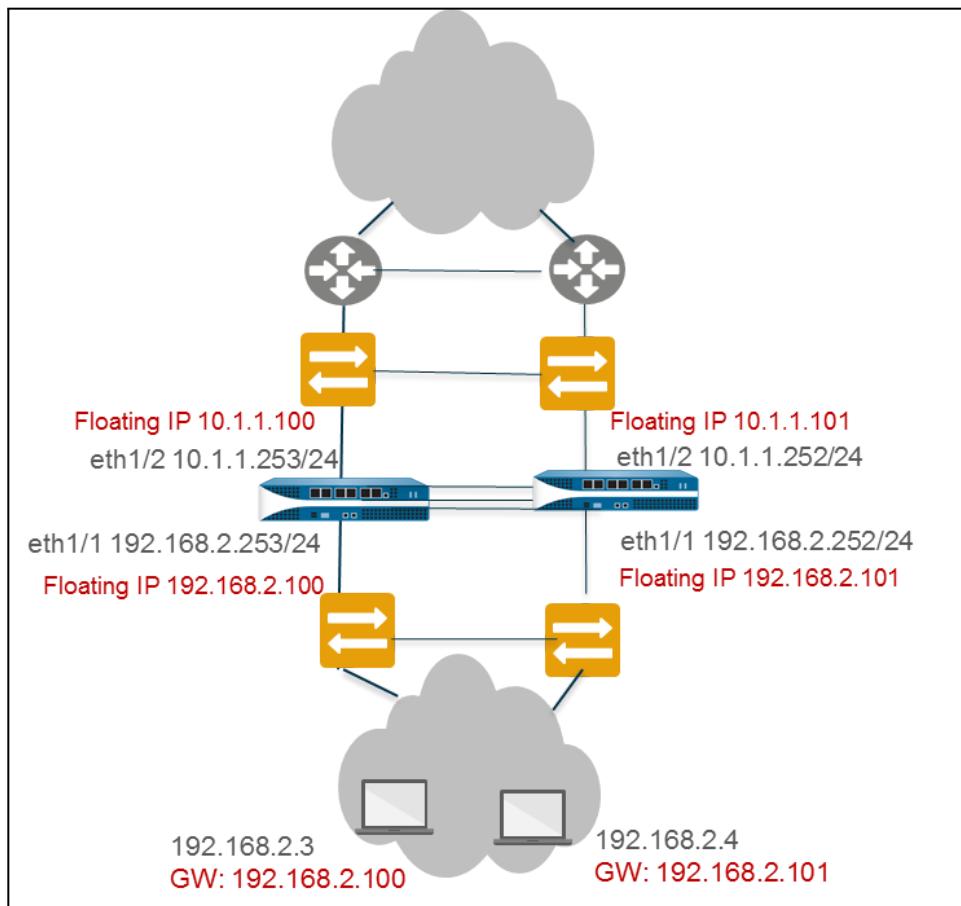
In a Layer 3 deployment of HA active/active mode, you can assign floating IP addresses that move from one HA firewall to the other if a link or firewall fails. The interface on the firewall that owns the floating IP address responds to ARP requests with a virtual MAC address.

Floating IP addresses are recommended when you need functionality such as the Virtual Router Redundancy Protocol. Floating IP addresses also can be used to implement VPNs and source NAT, thus allowing for persistent connections when a firewall offering those services fails.

Each HA firewall interface has its own IP address and floating IP address. The interface IP address remains local to the firewall, but the floating IP address moves between the firewalls upon firewall failure. You configure the end hosts to use a floating IP address as its default gateway, thus allowing you to load balance traffic to the two HA peers. You also can use external load balancers to load balance traffic.

If a link or firewall fails or a path monitoring event causes a failover, the floating IP address and virtual MAC address move over to the functional firewall. (In the figure that follows, each firewall has two floating IP addresses and virtual MAC addresses; they all move over if the firewall fails.) The functioning firewall sends a gratuitous ARP to update the MAC tables of the connected switches to inform them of the change in floating IP address and MAC address ownership to redirect traffic to itself.

After the failed firewall recovers, by default the floating IP address and virtual MAC address move back to the firewall with the Device ID (0 or 1) to which the floating IP address is bound. More specifically, after the failed firewall recovers, it becomes online. The currently active firewall determines that the firewall is back online and checks whether the floating IP address that it is handling belongs natively to itself or to the other firewall. If the floating IP address originally was bound to the other Device ID, the firewall automatically gives it back. An example of a floating IP deployment follows:



Each firewall in the HA pair creates a virtual MAC address for each of its interfaces that has a floating IP address or ARP load-sharing IP address.

### 5.3.6 HA interfaces

#### *HA Links and Backup Links*

The firewalls in an HA pair and cluster use HA links to synchronize data and maintain state information. Some firewall models have dedicated HA ports — control link (HA1) and data link (HA2) — and others require you to use the in-band ports as HA links. Firewalls in an HA cluster use an in-band Layer 3 HA4 interface for cluster session synchronization as follows:

- For firewalls with dedicated HA ports, use these ports to manage communication and synchronization between the firewalls.
- For firewalls without dedicated HA ports, use a data plane port for the HA port and use the management port as the HA1 backup.

Because the HA ports synchronize data that is critical to proper HA failover, implementation of backup HA paths is a recommended best practice. In-band ports can be used for backup links for HA1, HA2, and HA3

connections when dedicated backup links are not available. Consider the following guidelines when you configure 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 ports 28770 and 28260.

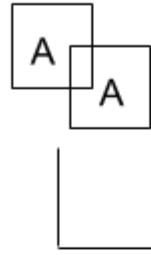
### 5.3.7 Clustering

A number of Palo Alto networks firewall models support session state synchronization among firewalls in an HA cluster of up to 16 firewalls. The HA cluster peers synchronize sessions to protect against data center or large security inspection point failure with horizontally scaled firewalls. In the case of a network outage or a down firewall, the sessions fail over to a different firewall in the cluster.

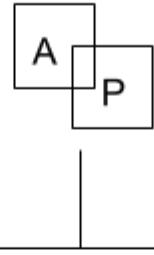
Such synchronization is especially helpful in the following use cases:

- When HA peers are spread across multiple data centers
- When one data center is active and the other is on standby

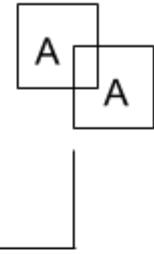
Active  
DC1



Active  
DC2

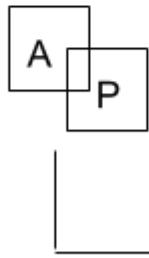


Active  
DC3 ...



Layer2 HA4 Connection

Active  
DC1

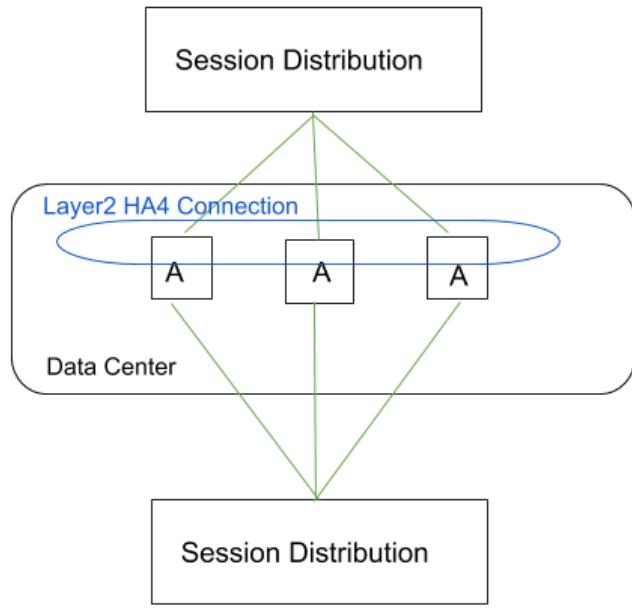


Standby  
DC



Layer2 HA4 Connection

A third HA clustering use case is horizontal scaling, in which you add HA cluster members to a single data center to scale security and ensure session survivability.



HA clusters support a Layer 3 or virtual wire deployment. HA peers in the cluster can be a combination of HA pairs and standalone cluster members. In an HA cluster, all members are considered active; there is no concept of passive firewalls except for HA pairs, which can keep their active/passive relationship after you add them to an HA cluster.

All cluster members share session state. When a new firewall joins an HA cluster, that triggers all firewalls in the cluster to synchronize all existing sessions. HA4 and HA4 backup connections are the dedicated cluster links that synchronize session state among all cluster members with the same cluster ID. The HA4 link between cluster members detects connectivity failures between cluster members. HA1 (control link), HA2 (data link), and HA3 (packet-forwarding link) are not supported between cluster members that aren't HA pairs.

For a normal session that has not failed over, only the firewall that is the session owner creates a traffic log. For a session that failed over, the new session owner (the firewall that receives the failed over traffic) creates the traffic log.

The firewall models that support HA clustering and the maximum number of members supported per cluster are described in the following table.

FIREWALL MODEL	NUMBER OF MEMBERS SUPPORTED PER CLUSTER
----------------	---

PA-3200 Series	6
PA-5200 Series	16
PA-7000 Series firewalls that have at least one of the following cards: PA-7000-100G-NPC, PA-7000-20GQXM-NPC, and PA-7000-20GXM-NPC	PA-7080: 4 PA-7050: 6
VM-300	6
VM-500	6
VM-700	16

### 5.3.8 Election setting

Specify or enable the following settings:

- **Device Priority:** Enter a priority value to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall (range is 0 to 255) when the preemptive capability is enabled on both firewalls in the pair.
- **Preemptive:** Enables the higher-priority firewall to resume active (active/passive) or active-primary (active/active) operation after recovering from a failure. You must enable the preemption option on both firewalls for the higher-priority firewall to resume active or active-primary operation upon recovery after a failure. If this setting is disabled, then the lower-priority firewall remains active or active-primary even after the higher-priority firewall recovers from a failure.
- **Heartbeat Backup:** Uses the management ports on the HA firewalls to provide a backup path for heartbeat and Hello messages. The management port IP address will be shared with the HA peer through the HA1 control link. No additional configuration is required.

### 5.3.9 References

HA Concepts:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts>

What is HA-Lite on Palo Alto Networks PA-200?:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUzCAK>

HA Clustering Overview:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-clustering-overview>

HA Links and Backup Links:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links>

Set Up Active/Passive HA:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha>

Set Up Active/Active HA:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha>

Configure HA Clustering:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/configure-ha-clustering>

HA Clustering Best Practices and Provisioning:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-clustering-best-practices-and-provisioning>

SNMP Support:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/snmp-monitoring-and-traps/snmp-support>

Monitor Statistics Using SNMP:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/snmp-monitoring-and-traps/monitor-statistics-using-snmp>

Supported MIBs:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/snmp-monitoring-and-traps/unsupported-mibs>

Monitor Device Health:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/device-monitoring-on-panorama/monitor-device-health>

Use Case: Configure Active/Active HA with Floating IP Address Bound to Active-Primary Firewall:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-address-bound-to-active-primary-firewall>

Information Synchronized in an HA Pair:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIXGCA0>

What Settings Don't Sync in Active/Passive HA?:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/reference-ha-synchronization/what-settings-dont-sync-in-activepassive-ha>

HA General Settings:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-high-availability/ha-general-settings>

### 5.3.10 Sample Question

1. Which feature is an intended advantage of an active/active firewall pair versus an active/passive pair?

- a. increased throughput
- b. support of asynchronous routing
- c. increased session count
- d. shared dynamic updates

2. Which location does a firewall use to forward HA-related events to an external monitoring technology?

- a. Device > Log Settings > System Log Settings
- b. Objects > Log Forwarding Profile > System Log Type
- c. Device > High Availability > General > Event Forwarding
- d. Dashboard > High Availability Widget > Notification

3. Which two Panorama objects can display current HA state information about a managed firewall? (Choose two.)

- a. firewall listings in Monitor > HA Status
- b. firewall-specific information in Managed Devices > Health
- c. firewall listings in Managed Devices > Summary
- d. firewall HA Status widget in Dashboard > Widgets
- e. firewall HA status in Panorama > High Availability

4. Why would you recommend an active/active firewall pair instead of an active/passive firewall pair?

- a. Active/active is the preferred solution when the firewall pair is behind a load balancer that randomizes routing, thus requiring both firewalls to be active.
- b. Active/active usually is the preferred solution because it allows for more bandwidth while both firewalls are up.
- c. Active/active is the preferred solution when the PA-7000 Series is used. Use active/passive with the PA-5200 Series or smaller form factors.
- d. Active/active is the preferred solution when the PA-5200 Series or smaller form factors are used. Use active/passive with the PA-7000 Series.

5. Which two events can trigger an HA pair failover event? (Choose two.)

- a. An HA1 cable is disconnected from one of the firewalls.

- b. A dynamic update fails to download and install.
  - c. The firewall fails to successfully ping a path-monitored destination address.
  - d. OSPF implemented on the firewall determines that an available route is now down.
  - e. RIP implemented on the firewall determines that an available route is now down.
6. Which two firewall features support floating IP addresses in an active/active HA pair? (Choose two.)
- a. data plane traffic interfaces
  - b. source NAT
  - c. VPN endpoints
  - d. loopback interfaces
  - e. management port
7. How are firewall configurations in an active/passive HA pair synchronized if the firewalls are not under Panorama control?
- a. An administrator commits the changes to one, then commits them to the partner, and the changes are sent to the other.
  - b. An administrator pushes the configuration file to both firewalls, then commits them.
  - c. An administrator commits changes to one, which automatically synchronizes with the other.
  - d. An administrator schedules an automatic sync frequency in the firewall configurations.
8. In which two ways is an active/passive HA pair configured in virtual firewalls deployed in public clouds? (Choose two.)
- a. The virtual firewalls are deployed in a cloud scale set with a cloud-supplied load balancer in front to detect and manage failover.
  - b. The virtual firewalls rely on a VM-Series plugin to map appropriate cloud functions to the firewall's HA settings.
  - c. Virtual firewalls use PAN-OS HA configuration combined with appropriate cloud deployments of interfaces for HA use.
  - d. The virtual firewalls use an HA compatibility module for the appropriate cloud technology.

# Domain 6- Troubleshooting

## *Troubleshooting Using the Web Interface and CLI Tools*

Palo Alto Networks firewall troubleshooting involves a wide range of specific knowledge that depends on the type of issue involved. This section introduces a few principal tools and methods available for troubleshooting. The end of this section includes references for other tools and topics. Dedicated training classes for firewall troubleshooting also are available from Palo Alto Networks and Training Partners.

### **6.1 Troubleshoot site-to-site tunnels**

#### **6.1.1 IPsec**

##### *CLI Troubleshooting Commands*

The CLI has **test** and **debug** commands for additional troubleshooting when configuring and maintaining one or more tunnels. VPN events, including errors, are posted to the System log. Error messages are more useful when the firewall receives VPN negotiation requests from other endpoints.

#### **6.1.2 GRE**

##### *GRE Tunnels*

A GRE tunnel connects two endpoints (a firewall and another device) in a point-to-point, logical link. The firewall can terminate GRE tunnels, and you can route or forward packets to a GRE tunnel. GRE tunnels are simple to use and often are the tunneling protocol of choice for point-to-point connectivity, especially to services in the cloud or to partner networks.

Create a GRE tunnel when you want to direct packets that are destined for an IP address to take a certain point-to-point path — for example, to a cloud-based proxy or to a partner network. The packets travel in the GRE tunnel (over a transit network such as the internet) to the cloud service while on their way to the destination address. Thus, the cloud service can enforce its services or policies on the packets.

After the firewall allows a packet (based on a policy match) and the packet egresses to a GRE tunnel interface, the firewall adds GRE encapsulation; it does not generate a session. The firewall performs no Security policy rule lookup for the GRE-encapsulated traffic; therefore, you do not need a Security policy rule for the GRE traffic that the firewall encapsulates. However, after the firewall receives GRE traffic, it generates a session and applies all policies to the GRE IP header in addition to the encapsulated traffic. The firewall treats the received GRE packet as it would any other packet.

If the firewall receives the GRE packet on an interface that has the same zone as the tunnel interface associated with the GRE tunnel (e.g., tunnel.1), the source zone is the same as the destination zone. By default, traffic is allowed within a zone (intrazone traffic), so the ingress GRE traffic is allowed by default.

However, if you configured your own intrazone Security policy rule to deny such traffic, you must explicitly allow GRE traffic.

Likewise, if the zone of the tunnel interface that is associated with the GRE tunnel (e.g., tunnel.1) is different from the zone of the ingress interface, you must configure a Security policy rule to allow the GRE traffic.

Because the firewall encapsulates the tunneled packet in a GRE packet, the additional 24 bytes of GRE header automatically results in a smaller MSS in the MTU. If you do not change the IPv4 MSS adjustment size for the interface, by default the firewall reduces the MTU by 64 bytes (40 bytes of IP header + 24 bytes of GRE header).

This reduction means that if the default MTU is 1,500 bytes, the MSS will be 1,436 bytes ( $1,500 - 40 - 24 = 1,436$ ). If you configure an MSS adjustment size of 300 bytes, for example, the MSS will be only 1,176 bytes ( $1,500 - 300 - 24 = 1,176$ ).

Routing of a GRE or IPsec tunnel to a GRE tunnel is not supported. However, you can route a GRE tunnel to an IPsec tunnel. A GRE tunnel does not support QoS. The firewall does not support a single interface acting as both a GRE tunnel endpoint and a decryption broker. GRE tunneling does not support NAT between GRE tunnel endpoints.

### 6.1.3 One-to-one and one-to-many tunnels

Palo Alto Networks supports the following VPN deployments:

- **Site-to-Site VPN:** This deployment provides a simple VPN that connects a central site and a remote site. This is also commonly referred to as a hub-and-spoke VPN that connects a central (gateway) site with multiple remote (branch) sites.
- **Remote-User-to-Site VPN:** This deployment provides an endpoint client to use GlobalProtect agent for a secure remote user access connection through the firewall gateway.
- **Large Scale VPN:** This deployment uses Palo Alto Networks GlobalProtect Large Scale VPN (LSVPN). It provides a scalable mechanism to provide hub-and-spoke VPN for up to 1,024 branch offices.

### 6.1.4 Route-based versus policy-based remote hosts

#### Policy-based VPNs

- The IPsec tunnel is invoked during policy lookup for traffic matching the interesting traffic.
- There are no tunnel interfaces. The remote end of the interesting traffic has a route pointed out through the default gateway.
- As there are no tunnel interfaces, we cannot route traffic over VPNs.
- The policies and access lists configured for the interesting traffic serve as the proxy-IDs for the tunnels.
- Firewalls that support policy-based VPNs include Juniper SRX, Juniper NetScreen, Cisco ASA, and Check Point.

## Route-based VPNs

- The IPsec tunnel is invoked during route lookup for the remote end of the proxy-IDs.
- The remote end of the interesting traffic has a route pointing out through the tunnel interface.
- These do support routing over VPNs.
- Proxy-IDs are configured as part of the VPN setup.
- Firewalls that support route-based VPNs include Palo Alto Networks firewalls, Juniper SRX, Juniper NetScreen, and Check Point.

Palo Alto Networks firewalls do not support policy-based VPNs. Policy-based VPNs have specific Security rules, policies, or access lists (source addresses, destination addresses, and ports) configured to permit interesting traffic through IPsec tunnels. These rules are referenced during the quick mode/IPsec phase 2 and are exchanged in the first or second messages as the proxy-ids. If the Palo Alto Networks firewall is not configured with the proxy-id settings, the ikemgr daemon sets the proxy-id with the default values of source ip 0.0.0.0/0, destination ip 0.0.0.0/0 and application any. These values are exchanged with the peer during the first or second message of the quick mode. A successful phase 2 negotiation requires not only that the security proposals match, but also that the proxy-ids on either peer be a mirror image of each other.

It is mandatory to configure proxy-IDs whenever you establish a tunnel between a Palo Alto Networks firewall and the firewalls configured for policy-based VPNs.

### 6.1.5 Tunnel monitoring

The following table lists some of the common VPN error messages that are logged in the system log.

#### Syslog Error Messages for VPN Issues

IF ERROR IS THIS:	TRY THIS:
<pre>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]</pre>	<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>
<pre>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.</pre>	Check the IKE Crypto profile configuration to verify that the proposals on both sides have a common encryption, authentication, and DH Group proposal.
<pre>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.</pre>	<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>
<pre>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.</pre>	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="#">Create a Proxy ID to identify the VPN peers..</a>

## 6.1.6 References

VPN Deployments

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/vpn-deployments>

Site-to-Site VPN Overview

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/site-to-site-vpn-overview>

GlobalProtect Administrator's Guide

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin.html>

Large Scale VPN (LSVPN)

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/large-scale-vpn-lsvpn>

How to Troubleshoot IPSec VPN Connectivity Issues:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC>

How to Troubleshoot IPSec VPN connectivity issues:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC>

How to enable debug on a single VPN Peer? :

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClcKCAS>

How to check Status, Clear, Restore, and Monitor an IPSec VPN Tunnel:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVGCA0>

Resource List: IPSec Configuring and Troubleshooting:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clh5CAC>

IKEv1 VPN error logs – Troubleshooting:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PORsCAO>

View Tunnel Information in Logs:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/tunnel-content-inspection/view-tunnel-information-in-logs>

Interpret VPN Error Messages:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages#id05d1c8c1-0719-40fa-8aa1-4806a5f5fedd>

Proxy ID Mismatch:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClzzCAC>

## 6.2 Troubleshoot interfaces

### Objective

Troubleshoot physical port flap or link down issues.

## Environment

- All PaloAlto Hardware-based Firewalls.
- PAN-OS 7.1 and above.
- Copper or Fiber media types.

## Procedure

### For Copper ports:

Check for link lights: The status of the link light should be solid green if the link is up. If the link is not up or the LED is not solid green then,

1. Check for the Physical damage on the cable
2. Check if the cable used is of is correct type such as cat5,cat6.
3. Try using a known working cable between the devices.
4. If using a patch panel, try different patch interfaces, Patch panels may have crossed receive and transmit, especially if jumping multiple patch panel pairs.
5. Verify the speed/duplex setting on both sides of the link and modify the same if required.
6. Check if the distance specification of the cable is within the limits for the connection type
7. If another interface is available, move the existing non-working connection to that port. (try that on both ends)

### For Fiber ports:

If the connection is Fiber, in addition to the steps described above perform the following:

8. Ensure fiber connections are clean
9. Try another transceiver and cable if fiber(SM or MM)
10. Check power levels for fiber links to ensure the cable does not have signal loss
11. Is it the correct type of transceiver? GBIC, SFP, XFP, SFP+, QSFP, QSFP+, etc.
12. Check for the transceiver's transmit light on by using the power meter
13. Verify of the optics are supported by Palo Alto. A list of supported optics can be found [here](#).

## Additional Information

Additionally, the following steps can be performed

- Check system logs for any errors using 'show log system direction equal backward' Normally the port flaps are recorded in system logs.
- brdaent.log provides more details on the port issues. This can be verified using 'less mp-log brdagagent.log'
- Use show interface ethernet x/y and check for any errors incrementing. Run this command multiple times.

- Use `show system state filter sys.s1.* | match crc` to check for CRC errors incrementing.
- Changing of optics or cable on either side normally fixes the issues. If the issue is not fixed with the above troubleshooting steps then contact paloAlto support.

## 6.2.1 Transceivers

You can monitor the status of transceivers in your physical appliance or device to enable easier installation and troubleshooting. Diagnostics that can be viewed are transmitted bias current, transmitted power, received power, transceiver temperature, and power supply voltage.

For more information on monitoring transceivers, refer to the docs here:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/monitoring/monitor-transceivers.html>

## 6.2.2 Settings

### *Troubleshooting and Configuring Interface Components*

PAN-OS supports various interface configuration options. There are two general types of network interfaces on a firewall: traffic ports and the management port.

#### *Traffic Ports*

Traffic ports provide multiple configuration options and the ability to pass traffic through to other ports via traffic-handling objects (e.g., virtual routers, virtual wires, and VLANs).

#### *Management Port*

The management port is isolated from internal connectivity for security purposes. If the management port requires internet access, its traffic must be routed out of the firewall and through other network infrastructure that provides this connectivity. The traffic often is routed back to a traffic port on the firewall requiring appropriate Security policy rules for access. This traffic is treated like any other transit traffic, which means that you must configure Security policy rules to allow the traffic to pass.

### *Troubleshooting Tools*

There are several important tools for troubleshooting traffic flow through the firewall. A best practice in troubleshooting is to separate general connectivity issues from security issues. Connectivity issues should be resolved before security processing is evaluated.

The web interface provides several important tools. The path **Monitor > Logs > Traffic** provides session summary information. Log entries for traffic are generated as specified in Security policy rules. The typical configuration specifies that log entries are created when a session ends. Use the magnifying glass icon to examine this log entry for detail:

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. In the left sidebar under 'Logs', 'Traffic' is expanded, and a log entry is selected, highlighted with a black box. A callout bubble points to this entry with the text: 'Click for detailed information for this log entry.' The main pane displays the 'Detailed Log View' for the selected entry. The view is divided into three sections: General, Source, and Destination. The General section includes fields like Session ID (48755), Action (allow), Application (dns), and Rule (Users\_to\_Internet). The Source section shows details like Source User (192.168.1.20) and Source DAG. The Destination section shows details like Destination User (4.2.2.2) and Destination DAG. Below the detailed view is a table titled 'PCAP' with columns for RECEIVE TIME, TYPE, APPLICATION, ACTION, RULE, RULE UUID, BY..., SEVERI..., CATEG..., URL CATEG..., LIST, VERDI..., URL, and FILE NAME.

### Log Entry Detail

Log entry details include many types of information for troubleshooting: the Security action, the firewall policy allowing the traffic through, the assigned App-ID, the zones, and the ingress and egress interfaces. Log entries also include NAT details and flags for other handling details. Examine this data to get valuable insight into the firewall's processing of traffic from both connectivity and security processing views.

This data typically is written at session end, but logging settings can specify that log entries be created at session initiation time. This practice drives more log volume, but it can provide critical data in certain situations. Configure the Log at Session Start option temporarily during troubleshooting to provide more information and gain insight, as shown in the following image.

The screenshot shows the 'Security Policy Rule' configuration screen. At the top, there are tabs for General, Source, Destination, Application, Service/URL Category, Actions (which is selected and highlighted with a black box), and Usage. In the 'Actions' section, the 'Action Setting' is set to 'Allow'. In the 'Log Setting' section, there is a checkbox for 'Log at Session End' which is checked (highlighted with a black box). A callout bubble points to this checkbox with the text: 'Default of Traffic log entry creation at session end shown. A Traffic log entry can be written at session start as well.' Other settings in the rule configuration include Profile Setting, Log Forwarding (None), and Other Settings (Schedule: None, Disable Server Response Inspection).

You can also display open sessions using the **Monitor > Session Browser** display, as shown here:

You can use the **Clear** check box at the end of a session summary line to end the session immediately, which often generates the desired log entry.

The CLI **show** commands can also help with troubleshooting. The web interface traffic capture and CLI **pcap** and **debug** functions give greater visibility to system-level operations.

Connectivity issues often arise from unexpected traffic forwarding decisions. You can view forwarding decisions after you display the Layer 3 routing and forwarding tables in the web interface, as shown in the following figure.

You can see the specific virtual router's routing and forwarding tables by clicking the **More Runtime Stats** link.

Note that PBF policy rules can override routing decisions and must be considered when you troubleshoot connectivity. The routing and forwarding tables mentioned do *not* show the effects of existing PBF policy rules. PBF troubleshooting is best done on the CLI; **show** commands can display existing PBF policies and whether they are active. The **test pbf-policy-match** command will show the application of existing PBF policies on modeled traffic.

### 6.2.3 Aggregate interfaces and Link Aggregation Control Protocol

An aggregate interface group uses IEEE 802.1AX link aggregation to combine multiple Ethernet interfaces into a single virtual interface that connects the firewall to another network device or firewall. An aggregate group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy; when one interface fails, the remaining interfaces continue supporting traffic.

By default, interface failure detection is automatic only at the physical layer between directly connected peers. However, if you enable Link Aggregation Control Protocol (LACP), failure detection is automatic at the physical and data link layers, regardless of whether the peers are directly connected. LACP also enables automatic failover to standby interfaces if you configured hot spares. All Palo Alto Networks firewalls except VM-Series models support aggregate groups. The Product Selection tool indicates the number of aggregate groups each firewall supports. Each aggregate group can have up to eight interfaces.

### 6.2.4 Counter

#### Resolution

Counters are a very useful set of indicators for the processes, packet flows and sessions on the PA firewall and can be used to troubleshoot various scenarios.

To troubleshoot dropped packets show counter global filter severity drop can be used. Repeating the command multiple times helps narrow down the drops.

```
> show counter global filter severity drop
```

Global counters:

```
Elapsed time since last sampling: 34.999 seconds
```





Using the above command with delta option allows viewing packets dropped since the last time the command was issued.

```
> show counter global filter delta yes severity drop
```

Global counters:

```
Elapsed time since last sampling: 55.446 seconds
```

---

---

Apart from the severity drop, there are various other severities that this command can be used for based on the scenario. A few examples are: error, informational and warning.

To troubleshoot Management Server Statistics, use `show counter management-server`.

The counters can be used to view management server statistics (number of logs written to trigger counters assigned to each management server process)

This command is useful when suspecting a hardware issue that would require RMA replacement.

```
> show counter management-server
```

Log action not taken	:	0
Logs dropped because not logging:	:	0
User information from AD read	:	2
Certificates information read	:	0
License information fetched from update server:		0
Sighash refcount	:	1
Tunnelhash refcount	:	1
URLcat refcount	:	1
ip2loc refcount	:	1

To view management interface statistics use `show counter interface management` command.  
This is used to assist in troubleshooting connectivity.

```
> show counter interface management
```

Interface: Management Interface

```
-----  
--
```

Logical interface counters:

```
-----  
--
```

bytes received	505700037
bytes transmitted	295080711
packets received	772181
packets transmitted	874087
receive errors	0
transmit errors	0
receive packets dropped	0

```
transmit packets dropped          0  
multicast packets received      0
```

---

-  
The same counter can be used to check data plane interface statistics as well. Use the command `show counter interface <interface id>`. Example below.

```
> show counter interface tunnel.51
```

Interface: tunnel.51

---

-  
Logical interface counters read from CPU:

---

```
bytes received                  0  
bytes transmitted               0  
packets received                0  
packets transmitted              0  
receive errors                  0  
packets dropped                 0  
packets dropped by flow state check 0  
forwarding errors                0  
no route                        0  
arp not found                   0  
neighbor not found               0  
neighbor info pending             0  
mac not found                   0  
packets routed to different zone 0  
land attacks                     0  
ping-of-death attacks            0
```

teardrop attacks	0
ip spoof attacks	0
mac spoof attacks	0
ICMP fragment	0
layer2 encapsulated packets	0
layer2 decapsulated packets	0

---

-

Layer two troubleshooting can be dealt with in term of the irregularities in the ARP entries received by using the arp aspect of the global counter with the command show counter global filter aspect arp

```
> show counter global filter aspect arp
```

Global counters:

Elapsed time since last sampling: 8.330 seconds

.....  
.....

Various other counters are helpful when troubleshooting, here are a few examples

```
> show counter global name
```

aho_alloc_lookup_failed	warn	failed to alloc regex lookup
aho_fpga	info	The total requests to FPGA for AHO
aho_fpga_invalid_wqe	error	when getting result from fpga, wqe index was not valid
aho_fpga_ret_error	error	Dropped results from FPGA caused by unexecpted type
aho_fpga_ret_invalid_fid	error	Dropped results from FPGA caused by invalid flow id
aho_fpga_ret_length_error	error	Dropped results from FPGA caused by short length
aho_fpga_ret_multi_bufs	info	Aho fpga result with multiple buffers
aho_fpga_ret_offset_error	error	Dropped results from FPGA caused by invalid offset
aho_fpga_ret_wrong_size	error	Dropped results from FPGA caused by wrong packet size
aho_fpga_state_verify_failed	info	when getting result from fpga, session's state was changed
aho_fpga_unmatched_type	error	when getting result from fpga, type in session was not matched
aho_fpga_unmatched_wqe	warn	when getting result from fpga, wqe was not matched in session
aho_match_overflow	info	number of aho matches overflow
aho_sw	info	The total usage of software for AHO
aho_sw_fpga_fail	warn	Usage of software AHO caused by failure for sending fpga request
aho_sw_fpga_full	info	Usage of software AHO caused by fpga requests threshold
aho_sw_fpga_unavailable	warn	Usage of software AHO caused by fpga unavailable
aho_too_many_matches	info	too many signature matches within one packet
aho_too_many_mid_res	info	too many signature middle results within one packet
appid_dfa_invalid_result	error	The invalid dfa result for appid
appid_exceed_pkt_limit	warn	App. identification failed caused by limitation of total queued packe
appid_exceed_queue_limit	warn	App. identification failed caused by limitation of session queued pac
appid_exceed_queue_limit_post	warn	App. identification failed caused by limitation of session queued pac
appid_fini_with_wqe_2_fpga	info	session ends with wqe in fpga
appid_flow_state_fail	info	The session's state was changed
appid_ident_by_cache	info	Application identified by cache
appid_ident_by_dport	info	Application identified by L4 dport
appid_ident_by_dport_first	info	Application identified by L4 dport first

appid_ident_by_heuristics	info	Application identified by heuristics
appid_ident_by_icmp	info	Application identified by icmp type
appid_ident_by_ip	info	Application identified by ip protocol
appid_ident_by_sport	info	Application identified by L4 sport
appid_ident_by_sport_first	info	Application identified by L4 sport first
appid_ident_by_supernode	info	Application identified by supernode
appid_lookup_invalid_flow	drop	Packets dropped: invalid session state
appid_match_overflow	info	The dfa matches overflow
appid_no_policy	error	App. identification failed because of no policy
appid_override	info	Application identified by override rule
appid_proc	info	The number of packets processed by Application identification
appid_reset_sess_top_reass	error	reset sess failed at top reassembly
appid_result_id_changed	info	The session's appid status was changed
appid_result_no_policy	info	The session's policy was changed during appid proc
appid_skip_terminal	info	The dfa result is terminal
appid_ssl_no_cert_no_reset	info	ssl sessions with unknown server certificate but no previous reset
appid_stop_by_ager	info	Application identification terminated by session ager
appid_stop_by_ager_nopkts	info	Ager can't stop appid because no packets were queued
appid_unknown_by_stop	info	The number of unknown applications because of being stopped

## 6.2.5 Tagging

Tags allow you to group objects using keywords or phrases. Tags can be applied to address objects, address groups (static and dynamic), zones, services, service groups, and policy rules. You can use a tag to sort or filter objects and to visually distinguish objects with individual colors. When a color is applied to a tag, the Policy tab displays the object with a background color.

A predefined tag named **Sanctioned** is available to tag applications (**Objects > Applications**). These tags are required to accurately monitor SaaS application usage.

WHAT DO YOU WANT TO KNOW?	SEE:
How do I create tags?	<a href="#">Create Tags</a>
What is the tag browser?	<a href="#">Use the Tag Browser</a>
How do I search for rules that are tagged, group rules using tags, view tags used in policy, or apply tags to policy?	<a href="#">Manage Tags</a>
Where can I go for general tag information?	<a href="#">See Policy</a>

## 6.2.6 References

How to Troubleshoot Using Counters via the –LI - Knowledge B-se - Palo Alto Networks

[Use CLI Commands for SD-WAN Tasks \(paloaltonetworks.com\)](#)

How to Troubleshoot Physical Port Flap or Link Down Issue:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNcB>

How to Troubleshoot Physical Port Flap or Link Down Issue:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNcB>

For more information, refer to the following link:

[Configure an Aggregate Interface Group \(paloaltonetworks.com\)](#)

Setting a Service Route for Services to Use a Dataplane Interface from the Web UI and CLI:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGJCA0>

Take Packet Captures:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/take-packet-captures>

### 6.2.7 Sample Questions

1. Where in the firewall web interface can you see whether sessions are going through a specific interface?
  - a. Dashboard
  - b. Application Command Center
  - c. Session Log node on the Monitor tab
  - d. Session Browser node on the Monitor tab
2. Communication through a specific interface works most of the time but fails when traffic throughput is at its highest. Which policy would you consider implementing to identify the problem?
  - a. Security
  - b. DoS Protection
  - c. QoS
  - d. Application Override
3. Which interface type allows you to control traffic with the least disruption to a network?
  - a. tap
  - b. Layer 3
  - c. Layer 2
  - d. virtual wire

### 6.3 Troubleshoot Decryption

A new Decryption Log and new Application Command Center (ACC) widgets provide enhanced visibility into TLS traffic, which enables you to troubleshoot and monitor decryption issues and identify traffic that uses weak algorithms and protocols. Use the new ACC widgets to identify traffic for which decryption causes issues and then use the new Decryption Log to drill down into details and gain context about that traffic.

The new **ACC > SSL Activity** widgets show you details about both successful and unsuccessful SSL Decryption activity in your network. They identify traffic—applications and Server Name Identifications (SNIs)—that cause decryption issues and that use weak ciphers and algorithms. Use that knowledge to identify misconfigured Decryption policies and profiles and to make informed decisions about what traffic to allow and what traffic to block. You can view SSL/TLS traffic in the ACC in multiple ways:

- **Traffic Activity Widget**—Shows SSL/TLS activity compared to non-SSL/TLS activity by total number of sessions or bytes.
- **Successful TLS Version Activity Widget**—Shows successful TLS connections by TLS version and application or SNI. This widget helps you understand how much risk you are taking on by allowing weaker TLS protocol versions. Identifying applications and SNIs that use weak protocols enables you to evaluate each one and decide whether you need to allow access to it for business reasons. If you don't need the application for business purposes, you may want to block the traffic instead of allowing it. Click an application or an SNI to drill down and see detailed information.
- **Decryption Failure Reasons Widget**—Shows the reasons for decryption failures, such as certificate or protocol issues, by SNI. Use this information to detect problems caused by Decryption policy or profile misconfiguration or by traffic that uses weak protocols or algorithms. Click a failure reason to drill down and isolate the number of sessions per SNI or click an SNI to see the failures for that SNI.
- **SSL/TLS Traffic Widget**—Shows the amount of decrypted and non-decrypted traffic by sessions or bytes. Traffic that was not decrypted may be excepted from decryption by policy, policy misconfiguration, or by being on the Decryption Exclusion List (**Device > Certificate Management > SSL Decryption Exclusion**).
- **Successful Key Exchange Activity**—Shows successful key exchange activity per algorithm, by application or by SNI. Click a key exchange algorithm to see the activity for just that algorithm or click an application or SNI to view the key exchange activity for that application or SNI.

The new Decryption Log (**Monitor > Logs > Decryption**) provides comprehensive information about sessions that match a Decryption policy. You can view log information such as application, SNI, Decryption Policy Name, error index, TLS version, key exchange version, encryption algorithm, certificate key types, and many other characteristics by selecting which columns to display:

	RECEIVE TIME	APPLICATION	DESTINATION ADDRESS	RULE	POLICY NAME	ROOT STATUS	ERROR INDEX	ERROR	SOURCE ADDRESS	SUBJECT COMMON NAME	SERVER NAME IDENTIFICATION	CERTIFICATE END DATE	ISSUER COMMON NAME	ROOT COMMON NAME	SESSION ID	PROXY TYPE
🔗	02/07/11:44:54	web-browsing	51.143.106.177	web-browsing	web-decryption	trusted	None		172.23.11.11	settings-win.data.microsoft.com		2020/05/21 00:36:44	Microsoft Secure Server CA 2011	DigiCert SHA2 High Assurance Server CA	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Application <input type="checkbox"/> Destination Zone <input type="checkbox"/> Dynamic Address Group <input type="checkbox"/> Destination Address <input type="checkbox"/> Source Country <input type="checkbox"/> Source Port <input checked="" type="checkbox"/> Rule <input checked="" type="checkbox"/> Policy Name <input checked="" type="checkbox"/> Root Status <input checked="" type="checkbox"/> Error Index <input checked="" type="checkbox"/> Error <input type="checkbox"/> Certificate Start Date <input checked="" type="checkbox"/> Source Address <input checked="" type="checkbox"/> Subject Common Name <input checked="" type="checkbox"/> Server Name Identification <input checked="" type="checkbox"/> Certificate End Date <input checked="" type="checkbox"/> Issuer Common Name <input checked="" type="checkbox"/> Root Common Name <input checked="" type="checkbox"/> Session ID <input checked="" type="checkbox"/> Proxy Type <input checked="" type="checkbox"/> Certificate Serial Number <input type="checkbox"/> Source User <input checked="" type="checkbox"/> Certificate Fingerprint <input checked="" type="checkbox"/> TLS Version <input checked="" type="checkbox"/> Key Exchange <input checked="" type="checkbox"/> Encryption Algorithm <input checked="" type="checkbox"/> Negotiated EC Curve <input checked="" type="checkbox"/> Authentication Algorithm <input checked="" type="checkbox"/> Certificate Key Type <input checked="" type="checkbox"/> Certificate Key Size <input type="checkbox"/> Destination Dynamic Address Group <input type="checkbox"/> Destination Country <input type="checkbox"/> Destination EDL <input type="checkbox"/> Destination Port <input type="checkbox"/> Destination User <input type="checkbox"/> Device Name <input type="checkbox"/> Generate Time <input type="checkbox"/> Inbound Interface <input type="checkbox"/> IP Protocol <input type="checkbox"/> Outbound Interface <input type="checkbox"/> Source EDL <input type="checkbox"/> Type <input type="checkbox"/> Virtual System <input type="checkbox"/> Virtual System Name	
🔗	02/07/11:41:24	dropbox-base	52.203.155.34	Web app moderate risk	web-decryption	trusted	None		172.23.11.11	*.dropbox.com	di-debug.dropbox.com	2020/11/05 12:00:00	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Application <input type="checkbox"/> Destination Zone <input type="checkbox"/> Dynamic Address Group <input checked="" type="checkbox"/> Destination Address <input type="checkbox"/> Source Country <input type="checkbox"/> Source Port <input checked="" type="checkbox"/> Rule <input checked="" type="checkbox"/> Policy Name <input checked="" type="checkbox"/> Root Status <input checked="" type="checkbox"/> Error Index <input checked="" type="checkbox"/> Error <input type="checkbox"/> Certificate Start Date <input checked="" type="checkbox"/> Source Address <input checked="" type="checkbox"/> Subject Common Name <input checked="" type="checkbox"/> Server Name Identification <input checked="" type="checkbox"/> Certificate End Date <input checked="" type="checkbox"/> Issuer Common Name <input checked="" type="checkbox"/> Root Common Name <input checked="" type="checkbox"/> Session ID <input checked="" type="checkbox"/> Proxy Type <input checked="" type="checkbox"/> Certificate Serial Number <input type="checkbox"/> Source User <input checked="" type="checkbox"/> Certificate Fingerprint <input checked="" type="checkbox"/> TLS Version <input checked="" type="checkbox"/> Key Exchange <input checked="" type="checkbox"/> Encryption Algorithm <input checked="" type="checkbox"/> Negotiated EC Curve <input checked="" type="checkbox"/> Authentication Algorithm <input checked="" type="checkbox"/> Certificate Key Type <input checked="" type="checkbox"/> Certificate Key Size <input type="checkbox"/> Destination Dynamic Address Group <input type="checkbox"/> Destination Country <input type="checkbox"/> Destination EDL <input type="checkbox"/> Destination Port <input type="checkbox"/> Destination User <input type="checkbox"/> Device Name <input type="checkbox"/> Generate Time <input type="checkbox"/> Inbound Interface <input type="checkbox"/> IP Protocol <input type="checkbox"/> Outbound Interface <input type="checkbox"/> Source EDL <input type="checkbox"/> Type <input type="checkbox"/> Virtual System <input type="checkbox"/> Virtual System Name	
🔗	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🔗	02/07/11:38:44	ssl	162.125.7.3	web-browsing	web-decryption	trusted	None		172.23.11.11	*.dropbox.com		2020/11/05 12:00:00	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Application <input type="checkbox"/> Destination Zone <input type="checkbox"/> Dynamic Address Group <input type="checkbox"/> Destination Address <input type="checkbox"/> Source Country <input type="checkbox"/> Source Port <input type="checkbox"/> Rule <input type="checkbox"/> Policy Name <input type="checkbox"/> Root Status <input type="checkbox"/> Error Index <input type="checkbox"/> Error <input type="checkbox"/> Certificate Start Date <input type="checkbox"/> Source Address <input type="checkbox"/> Subject Common Name <input type="checkbox"/> Server Name Identification <input type="checkbox"/> Certificate End Date <input type="checkbox"/> Issuer Common Name <input type="checkbox"/> Root Common Name <input type="checkbox"/> Session ID <input type="checkbox"/> Proxy Type <input type="checkbox"/> Certificate Serial Number <input type="checkbox"/> Source User <input type="checkbox"/> Certificate Fingerprint <input type="checkbox"/> TLS Version <input type="checkbox"/> Key Exchange <input type="checkbox"/> Encryption Algorithm <input type="checkbox"/> Negotiated EC Curve <input type="checkbox"/> Authentication Algorithm <input type="checkbox"/> Certificate Key Type <input type="checkbox"/> Certificate Key Size <input type="checkbox"/> Destination Dynamic Address Group <input type="checkbox"/> Destination Country <input type="checkbox"/> Destination EDL <input type="checkbox"/> Destination Port <input type="checkbox"/> Destination User <input type="checkbox"/> Device Name <input type="checkbox"/> Generate Time <input type="checkbox"/> Inbound Interface <input type="checkbox"/> IP Protocol <input type="checkbox"/> Outbound Interface <input type="checkbox"/> Source EDL <input type="checkbox"/> Type <input type="checkbox"/> Virtual System <input type="checkbox"/> Virtual System Name	
🔗	02/07/11:38:44	ssl	162.125.7.3	web-browsing	web-decryption	trusted	None		172.23.11.11	*.dropbox.com		2020/11/05 12:00:00	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Application <input type="checkbox"/> Destination Zone <input type="checkbox"/> Dynamic Address Group <input type="checkbox"/> Destination Address <input type="checkbox"/> Source Country <input type="checkbox"/> Source Port <input type="checkbox"/> Rule <input type="checkbox"/> Policy Name <input type="checkbox"/> Root Status <input type="checkbox"/> Error Index <input type="checkbox"/> Error <input type="checkbox"/> Certificate Start Date <input type="checkbox"/> Source Address <input type="checkbox"/> Subject Common Name <input type="checkbox"/> Server Name Identification <input type="checkbox"/> Certificate End Date <input type="checkbox"/> Issuer Common Name <input type="checkbox"/> Root Common Name <input type="checkbox"/> Session ID <input type="checkbox"/> Proxy Type <input type="checkbox"/> Certificate Serial Number <input type="checkbox"/> Source User <input type="checkbox"/> Certificate Fingerprint <input type="checkbox"/> TLS Version <input type="checkbox"/> Key Exchange <input type="checkbox"/> Encryption Algorithm <input type="checkbox"/> Negotiated EC Curve <input type="checkbox"/> Authentication Algorithm <input type="checkbox"/> Certificate Key Type <input type="checkbox"/> Certificate Key Size <input type="checkbox"/> Destination Dynamic Address Group <input type="checkbox"/> Destination Country <input type="checkbox"/> Destination EDL <input type="checkbox"/> Destination Port <input type="checkbox"/> Destination User <input type="checkbox"/> Device Name <input type="checkbox"/> Generate Time <input type="checkbox"/> Inbound Interface <input type="checkbox"/> IP Protocol <input type="checkbox"/> Outbound Interface <input type="checkbox"/> Source EDL <input type="checkbox"/> Type <input type="checkbox"/> Virtual System <input type="checkbox"/> Virtual System Name	Forward

Click the magnifying glass icon (  ) to see the Detailed Log View of a session:

**Detailed Log View**

General

Session ID	111408
Application	dropbox-base
Rule	Web app moderate risk
Policy Name	web-decryption
Proxy Type	Forward
IP Protocol	tcp
Generated Time	2020/02/07 11:41:24
Receive Time	2020/02/07 11:41:24

Source

Source User	Source 172.23.11.11
Country	172.16.0.0-172.31.255.255
Port	50890
Zone	inZone
Interface	ethernet1/4

Destination

Destination User	Destination 52.203.155.34
Country	United States
Port	443
Zone	outZone
Interface	ethernet1/1

Certificate Details

Handshake Details

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2020/02/07 11:41:09	url	dropbox-base	alert	Web app moder...	ee9bb...		informa...	online-stora...	online-stora...		dl-deb...	
	2020/02/07 11:41:09	url	dropbox-base	alert	Web app moder...	ee9bb...		informa...	online-stora...	online-stora...		dl-deb...	

**Close**

After using the ACC to identify decryption issues, filter the Decryption Log to see detailed information about issues. Common troubleshooting tasks include:

- Filtering for weak cipher suites to identify SNIIs and applications that use older, less secure protocols and algorithms. For example, the filter (`tls_version leq TLS1.1`) shows you all traffic that uses TLS versions lower than TLSv1.2. You can then make an informed decision about how you want to handle traffic that uses weaker TLS versions.

In the same way, you can filter for weak key exchange and encryption algorithms. For example, the filter (`tls_keyxchg eq RSA`) identifies all traffic that uses the RSA key exchange algorithm. The filter (`tls_auth eq MD5`) identifies all traffic that uses the MD5 authentication algorithm. The filter (`tls_enc eq 3DES_EDE_CBC`) identifies the traffic that uses that encryption algorithm.

- Filtering for expired certificates. The filter (`error eq 'Expired server certificate'`) identifies traffic that generates an “Expired server certificate” error. You can check the results at [SSL Labs](#) and see the validity dates of the certificate.

You can also filter for certificates that will expire soon. For example, to filter for certificates that expire after July 1st, 2020, use the filter (`notafter leq '2020/7/01 12:00:00'`).

- Filtering for revoked certificates (you must first enable [Certificate Revocation Checking](#) to do this). Use the filter (`error eq 'OCSP/CRL check: certificate revoked'`)

There are many ways to filter the extensive information in the Decryption Logs to drill down into the details of any issue or potential issue.

### 6.3.1 Inbound decryption

Troubleshooting tools provide enhanced visibility into TLS traffic so you can monitor your decryption deployment. The tools enable you to diagnose and resolve decryption issues quickly and easily, tighten weaknesses in your decryption deployment, and fix decryption issues to improve your security posture. For example, you can:

- Identify traffic that causes decryption failures by Service Name Identification (SNI) and application.
- Identify traffic that uses weak protocols and algorithms.
- Examine successful and unsuccessful decryption activity in the network.
- View detailed information about individual sessions.
- Profile decryption usage and patterns.
- Monitor detailed decryption statistics and information about adoption, failures, versions, algorithms, etc.

The following tools provide full visibility into the TLS handshake and help you troubleshoot and monitor your decryption deployment:

- **ACC > SSL Activity**—The five ACC widgets on this tab (introduced in PAN-OS 10.0) provide details about successful and unsuccessful decryption activity in your network, including decryption failures, TLS versions, key exchanges, and the amount and type of decrypted and undecrypted traffic.
- **Monitor > Logs > Decryption**—The Decryption Log (introduced in PAN-OS 10.0) provides comprehensive information about individual sessions that match a Decryption policy (use a No Decryption policy for traffic you don't decrypt) and about GlobalProtect sessions when you enable Decryption logging in GlobalProtect Portal or GlobalProtect Gateways configuration. Select which columns to display to view information such as application, SNI, Decryption Policy Name, error index, TLS version, key exchange version, encryption algorithm, certificate key types, and many other characteristics. Filter the information in columns to identify traffic that uses particular TLS versions and algorithms, particular errors, or any other characteristics you want to investigate. By default, Decryption policies log only unsuccessful TLS handshakes. Depending on the available log storage, you can configure Decryption policies to log successful TLS handshakes as well.
- **Local Decryption Exclusion Cache**—There are two constructs for sites that break decryption for technical reasons such as client authentication or pinned certificates and therefore need to be excluded from decryption: the SSL Decryption Exclusion List and the Local Decryption Exclusion Cache. The SSL Decryption Exclusion List contains the sites that Palo Alto Networks has identified that break decryption technically. Content updates keep the list up-to-date and you can add sites to the list manually. The Local Decryption Exclusion Cache automatically adds sites that local users encounter that break decryption for technical reasons and excludes them from decryption, providing that the Decryption profile applied to the traffic allows unsupported modes (if unsupported modes are blocked, then the traffic is blocked instead of added to the local cache).
- **Custom Report Templates for Decryption**—You can create custom reports (**Monitor > Manage Custom Reports**) using four predefined templates that summarize decryption activity (introduced in PAN-OS 10.0).

The general troubleshooting methodology is to use the new ACC widgets to identify traffic that causes decryption issues and then use the new Decryption Log and custom report templates to drill down into details and gain context about that traffic, which enables you to diagnose issues accurately and much more easily than in the past. Understanding decryption issues and their causes enables you to select the appropriate way to fix each issue, such as:

- Modify Decryption policy rules (a policy rule defines traffic that the rule affects, the action taken on that traffic, log settings, and the Decryption profile applied to the traffic)
- Modify Decryption profiles (acceptable protocols and algorithms for the traffic that a Decryption policy rule defines, plus failure checks, unsupported mode checks for items such as unsupported ciphers and versions, certificate checks, etc.)
- Add sites that break decryption for technical reasons to the SSL Decryption Exclusion List
- Evaluate security decisions about which sites your employees, customers, and partners really need to access and which sites you can block when sites use weak decryption protocols or algorithms

The goals should be to decrypt all the traffic you can decrypt ([a decryption best practice](#)) so that you can inspect it and to properly handle traffic that you don't decrypt.

When you upgrade to PAN-OS 10.0, the device takes 1% of the log space and allocates it to Decryption logs. [Step 3 in Configure Decryption Logging](#) shows you how to modify the log space allocation to provide more space for Decryption logs.

If you downgrade from PAN-OS 10.0 or later to PAN-OS 9.1 or earlier, the features introduced in PAN-OS 10.0 (Decryption Log, SSL Activity widgets in the ACC, custom report Decryption templates) are removed from the UI. References to Decryption logs are also removed from Log Forwarding profiles. In addition, the Local Decryption Exclusion Cache is only viewable using the CLI in PAN-OS 9.1 and earlier (PAN-OS 10.0 added the local cache to the UI).

If you push configurations from Panorama on PAN-OS 10.0 or later to devices that run PAN-OS 9.1 or earlier, Panorama removes the features introduced in PAN-OS 10.0.

### 6.3.2 SSL forward proxy

#### Troubleshooting SSL Decryption Failures

PAN-OS can decrypt and inspect inbound and outbound SSL connections going through the Palo Alto Networks firewall. SSL decryption can occur on interfaces in virtual wire, Layer 2, or Layer 3 mode by using the SSL rulebase to configure which traffic to decrypt. Decryption can be based on URL categories, source users, and source or target addresses. After traffic is decrypted, tunneled applications can be detected and controlled, and the decrypted data can be inspected for threats, URL filtering, file blocking, or data filtering. Decrypted traffic never is sent off the device.

A Palo Alto Networks firewall has a dedicated log for decryption events, which allows you to troubleshoot decryption operations.

### 6.3.3 SSH proxy

The SSH Proxy Decryption profile (**Objects > Decryption Profile > SSH Proxy**) controls the session mode checks and failure checks for SSH traffic defined in the SSH Proxy Decryption policies to which you attach the profile. The following figure shows the general best practice recommendations for SSH Proxy Decryption profile settings, but the settings you use also depend on your company's security compliance rules and local

laws and regulations.

The screenshot shows the 'Decryption Profile' configuration window. At the top, it displays the name 'best-practice-ssl-decryption'. Below this, there are three tabs: 'SSL Decryption', 'No Decryption', and 'SSH Proxy', with 'SSH Proxy' being the active tab. Under the 'Unsupported Mode Checks' section, two checkboxes are checked: 'Block sessions with unsupported versions' and 'Block sessions with unsupported algorithms'. In the 'Failure Checks' section, two checkboxes are present but unchecked: 'Block sessions on SSH errors' and 'Block sessions if resources not available'. A note at the bottom states: 'Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.' At the bottom right are 'OK' and 'Cancel' buttons.

**Unsupported Mode Checks.** The firewall supports SSHv2. If you don't block sessions with unsupported modes, users receive a warning message if they connect with potentially unsafe servers, and they can click through that message and reach the potentially dangerous site. Blocking these sessions protects you from servers that use weak, risky protocol versions and algorithms:

1. **Block sessions with unsupported versions**—The firewall has a set of predefined supported versions. Checking this box blocks traffic with weak versions. Always check this box to block sessions with the weak protocol versions to reduce the attack surface.
2. **Block sessions with unsupported algorithms**—The firewall has a set of predefined supported algorithms. Checking this box blocks traffic with weak algorithms. Always check this box to block sessions with unsupported algorithms to reduce the attack surface.

**Failure Checks:**

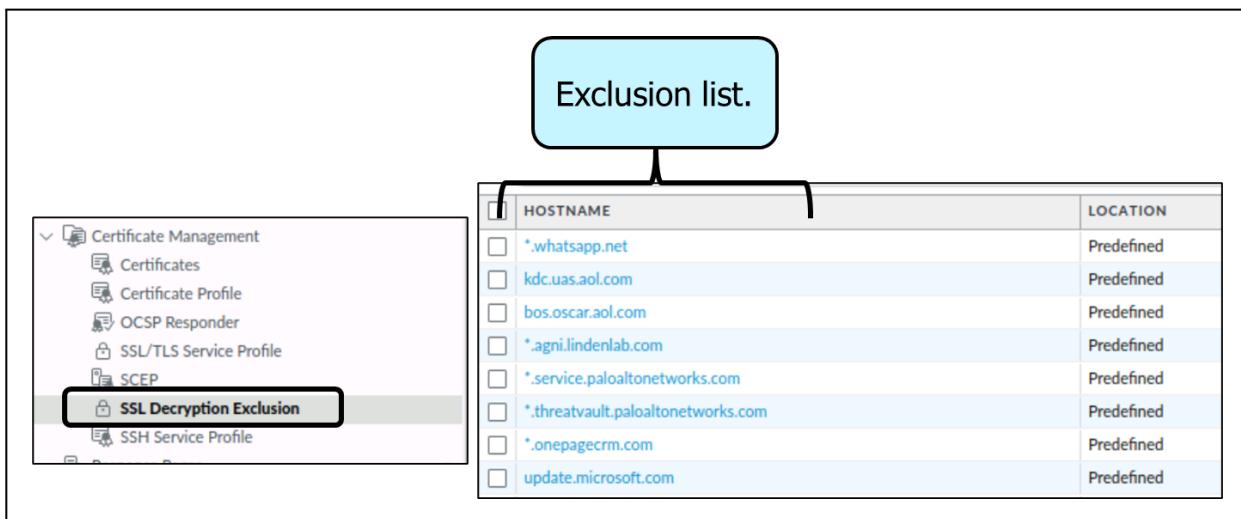
- **Block sessions on SSH errors**—Checking this box terminates the session if SSH errors occur.
- **Block sessions if resources not available**—If you don't block sessions when firewall processing resources aren't available, then encrypted traffic that you want to decrypt enters the network still encrypted, risking allowing potentially dangerous connections. However, blocking sessions when firewall processing resources aren't available may affect the user experience by making sites that users normally can reach temporarily unreachable. Whether to implement failure checks depends on your company's security compliance stance and the importance to your business of the user experience, weighed against tighter security. Alternatively, consider using firewall models with more processing power so that you can decrypt more traffic.

### 6.3.4 Identify what cannot be decrypted and configure exclusions and bypasses

#### Decryption Exclusions

A developer using SSL decryption can take extra programmatic steps to interrogate the certificate received at the client for specific characteristics present in the original certificate. When these characteristics are not found, the author often assumes that a decrypting process is in the middle of the conversation and may act to prevent full functionality and consider this presence a security risk. These products typically are not fully functional in a decrypting environment and must be added as exceptions to decryption policy rules.

Palo Alto Networks recognizes this situation and provides a mechanism to mark certain encrypted traffic for decryption bypass. A list of SSL sites with known decryption issues is predefined on the Palo Alto Networks firewall. You can add sites to this list using the **SSL Decryption Exclusion** option in the management web interface. The firewall does not attempt to decrypt traffic to or from these sites.



### 6.3.5 Certificates

#### Troubleshoot Expired Certificates

If you follow Decryption best practices and **Block sessions with expired certificates** in the Forward Proxy Decryption profile or in the No Decryption profile, then if a server presents an expired certificate, the firewall blocks the session. However, if site that you need to access for business reasons allows its certificate to expire, connections to that site may be blocked and you may not know why.

You can use the Decryption log to check for expired certificates and to check for certificates that will expire soon so you can be aware of the situation and take appropriate action.

**Step 1:** Filter the Decryption log for expired certificates using the query (error eq 'Expired server certificate').

Q [error eq 'Expired server certificate']

	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	POLICY NAME
Q	06/04 16:19:49	121352	incomplete	172.30.100.10	34.225.62.221	TLS1.3	Certificate	Expired server certificate	www.stanford.edu	Big Brother
Q	06/04 13:43:26	117747	incomplete	172.30.100.155	104.197.149.89	TLS1.3	Certificate	Expired server certificate	phone.com	Big Brother
Q	06/04 13:41:03	117572	incomplete	172.30.100.155	208.117.9.16	TLS1.3	Certificate	Expired server certificate	netcarshow.com	Big Brother
Q	06/04 13:38:51	117379	ssl	172.30.100.155	69.172.200.184	TLS1.2	Certificate	Expired server certificate	royal.gov.uk	Big Brother
Q	06/04 13:36:27	117150	ssl	172.30.100.155	107.21.104.61	TLS1.2	Certificate	Expired server certificate	www.uthscsa.edu	Big Brother
Q	06/04 13:34:53	117004	incomplete	172.30.100.155	66.115.56.251	TLS1.3	Certificate	Expired server certificate	gunsamerica.com	Big Brother
Q	06/04 13:33:17	116853	incomplete	172.30.100.155	34.107.140.234	TLS1.3	Certificate	Expired server certificate	skiplagged.com	Big Brother
Q	06/04 13:32:45	116798	ssl	172.30.100.155	104.236.4.58	TLS1.2	Certificate	Expired server certificate	uploading.com	Big Brother
Q	06/04 13:31:28	116655	incomplete	172.30.100.155	35.186.201.59	TLS1.3	Certificate	Expired server certificate	shared.com	Big Brother
Q	06/04 13:29:32	116507	ssl	172.30.100.155	147.139.136.53	TLS1.2	Certificate	Expired server certificate	beautynesia.id	Big Brother
Q	06/04 13:28:56	116426	incomplete	172.30.100.155	45.55.105.190	TLS1.3	Certificate	Expired server certificate	designbundles.net	Big Brother

This query identifies servers that generate **Expired server certificate** errors. The firewall blocks access to these servers because of the expired certificate.

**Step 2:** (Optional) Double-check the certificate expiration date at the Qualys SSL Labs site.

Enter the hostname of the server (**Server Name Identification** column of the Decryption log) in the **Hostname** field and **Submit** it to view certificate information for the host.

**Step 3:** Filter the Decryption log (**Monitor > Logs > Decryption**) for certificates that will expire soon using a query that identifies upcoming certificate end dates.

For example, if today's date is February 1, 2020 and you want to give yourself two months to evaluate and prepare in case sites don't update their certificates, query the Decryption log for certificates that expire April 1 2020 or earlier (`notafter leq '2020/4/01'`):

Q [notafter leq '2020/4/01']

	RECEIVE TIME	APPLICATION	POLICY NAME	PROXY TYPE	SERVER NAME IDENTIFICATION	ROOT STATUS	TLS VERSION	CERTIFICATE START DATE	CERTIFICATE END DATE
Q	01/09 14:25:38	incomplete	Test 2	Forward	a4.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
Q	01/09 14:25:38	incomplete	Test 2	Forward	a2.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
Q	01/09 14:25:38	incomplete	Test 2	Forward	a3.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43
Q	01/09 14:25:38	incomplete	Test 2	Forward	a.espncdn.com	uninspected	TLS1.2	2019/11/14 04:44:43	2020/02/13 04:44:43

The **Certificate End Date** column shows the exact date on which the certificate expires.

**Step 4:** Determine the action to take for sites with expired certificates.

- If you don't need to access the site for business purposes, the safest action is to continue to block access to the site.
- If you need to access the site for business purposes, take one of the following actions:
  - Contact the administrator of the site with the expired certificate and notify them that they need to update or renew their certificate.
  - Create a Decryption policy that applies only to the sites with expired certificates that you need for business purposes and a Decryption profile that allows sites with expired certificates. Do not apply the policy to any sites that you don't need for business purposes. When a site updates its certificate, remove it from the policy.

### Identify Untrusted CA Certificates

Blocking access to sites with untrusted CA certificates and certificates self-signed by an untrusted root CA is a best practice because sites with untrusted CAs may indicate a man-in-the-middle attack, a replay attack, or other malicious activity.

**Step 1.** Ensure that you **Block sessions with untrusted issuers** in the Forward Proxy Decryption profile (**ObjectsDecryptionDecryption Profiles**) to block sites with untrusted CAs.

The screenshot shows the 'Decryption Profile' configuration window. At the top, there's a 'Name' field containing 'strict-decryption-profile'. Below it, there are tabs for 'SSL Decryption' (selected), 'No Decryption', and 'SSH Proxy'. Under 'SSL Decryption', there are two main sections: 'Server Certificate Verification' and 'Unsupported Mode Checks'. In 'Server Certificate Verification', several checkboxes are checked: 'Block sessions with expired certificates', 'Block sessions with untrusted issuers' (highlighted in yellow), 'Block sessions with unknown certificate status', 'Restrict certificate extensions' (with a 'Details' link), and 'Append certificate's CN value to SAN extension'. In 'Unsupported Mode Checks', checkboxes include 'Block sessions with unsupported versions', 'Block sessions with unsupported cipher suites', and 'Block sessions with client authentication'. There are also 'Failure Checks' and 'Client Extension' sections with checkboxes. A note at the bottom states: 'Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.' At the bottom right are 'OK' and 'Cancel' buttons.

When you block sessions with untrusted issuers in the Decryption profile, the Decryption log (**MonitorLogsDecryption**) logs the error.

**Step 2.** Filter the log to identify sessions that failed due to revoked certificates using the query (`error eq 'Untrusted issuer CA'`).

	[error eq 'Untrusted issuer CA']									
	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION
🕒	06/04 13:43:07	117709	ssl	172.30.100.155	184.172.23.30	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dealscove.com
🕒	06/04 13:35:38	117074	ssl	172.30.100.155	204.236.227.206	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	foxsearchlight.com
🕒	06/04 13:17:10	115350	incomplete	172.30.100.155	69.163.152.152	TLS1.3	Certificate	Untrusted Issuer CA	Big Brother	famfamfam.com
🕒	06/04 13:07:18	114451	ssl	172.30.100.155	52.209.190.138	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bbva.com
🕒	06/04 12:52:46	113115	ssl	172.30.100.155	204.108.65.8	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	lausd.net
🕒	06/04 12:39:10	111870	ssl	172.30.100.155	34.90.228.231	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dumpert.nl
🕒	06/04 12:23:05	110460	incomplete	172.30.100.155	75.119.204.133	TLS1.3	Certificate	Untrusted Issuer CA	Big Brother	any.do
🕒	06/04 12:16:02	109894	ssl	172.30.100.155	217.21.43.35	TLS1.2	Certificate	Untrusted Issuer CA	Big Brother	bsu.by
🕒	06/04 11:56:42	108205	incomplete	172.30.100.155	45.223.17.206	TLS1.3	Certificate	Untrusted Issuer CA	Big Brother	imss.gob.mx

**Step 3. (Optional)** Double-check the certificate expiration date at the Qualys [SSL Labs](#) site.

Enter the hostname of the server (**Server Name Identification** column of the Decryption log) in the **Hostname** field and **Submit** it to view certificate information for the host.

### Troubleshoot Pinned Certificates

Certificate pinning forces the client application to validate the server's certificate against a known copy to ensure that certificate really comes from the server. The intent of pinned certificates is to protect against [man-in-the-middle \(MITM\)](#) attacks where a device between the client and the server replaces the server certificate with another certificate.

Although this prevents malicious actors from intercepting and manipulating connections, it also prevents [forward proxy decryption](#) because the firewall creates an impersonation certificate instead of the server certificate to present to the client. Instead of one session that connects the client and server directly, forward proxy creates two sessions, one between the client and the firewall and another between the firewall and the server. This establishes trust with the client so that the firewall can decrypt and inspect the traffic.

However, when a certificate is pinned, the firewall cannot decrypt the traffic because the client does not accept the firewall's impersonation certificate—the client only accepts the certificate that is pinned to the application.

**Step 1:** Filter the Decryption log (**Monitor > Logs > Decryption**) to find pinned certificates using the query (`error contains 'UnknownCA'`).

🔍 [error contains 'UnknownCA']

	RECEIVE TIME	APPLICATION	PROXY TYPE	SOURCE ADDRESS	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	TLS VERSION	POLICY NAME
🕒	06/02 11:25:30	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
🕒	06/02 11:16:53	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	telemetry.dropb...	TLS1.2	Big Brother
🕒	06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
🕒	06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
🕒	06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
🕒	06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
🕒	06/02 10:51:34	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother

The application generates a TLS error code (Alert) when it fails to verify the server's certificate. Different applications may use different error codes to indicate a pinned certificate. The most common error indicators for pinned certificates are UnknownCA and BadCertificate. After running the `(error contains 'UnknownCA')` query, run the query `(error contains 'BadCertificate')` to catch more pinned certificate errors.

### Step 2: Decide what to do about pinned certificates.

If you don't need access for business purposes, you can let the firewall continue to block access. If you need access, then you can [Exclude a Server from Decryption for Technical Reasons](#) by adding it to the SSL Decryption Exclusion List ([Device Certificate Management](#)[SSL Decryption Exclusion](#)).

The firewall bypasses decryption for sites on the SSL Decryption Exclusion List. The firewall cannot inspect the traffic, but the traffic is allowed.

### Troubleshoot Revoked Certificates

A revoked certificate is no longer valid. It may indicate that there are security issues with a site and that the certificate is not trustworthy, although there are also benign reasons why a certificate may be revoked.

In order to drop sessions with revoked certificates and troubleshoot revoked certificates, you need to enable certificate revocation checking. If you don't enable [certificate revocation](#) checking, the firewall doesn't check for revoked certificates and you won't know if a site has a revoked certificate.

### Step 1: Enable certificate revocation checking if you haven't already enabled it.

1. Go to **Device > Setup > Session > Decryption Settings**.
2. Enable both OCSP and CRL certificate checking.

The screenshot shows the Palo Alto Networks Device interface with the 'DEVICE' tab selected. In the 'Management' section, there are several configuration parameters:

- Latency Alert (ms) 50
- Latency Activate (ms) 200
- Latency Max Tolerate (ms) 500
- Block Countdown Threshold (ms) 500

A modal dialog titled "Certificate Revocation Checking" is open, containing two sections: CRL and OCSP.

**CRL**

- Enable
- Use CRL to check certificate status
- Receive Timeout (sec)

**OCSP**

- Enable
- Use OCSP to check certificate status
- Receive Timeout (sec)
- Certificate Status Timeout (sec)
- Certificate CRL status query timeout value

At the bottom of the modal are "OK" and "Cancel" buttons.

Below the modal, in the main interface, there are sections for "TCP Settings" and "Decryption Settings". Under "Decryption Settings", the "Certificate Revocation Checking" option is highlighted.

If you **Block sessions on certificate status check timeout** in the Forward Proxy Decryption profile and are concerned that 5 seconds is not enough time and may result in too many sessions blocked by timeouts, set the **Receive Timeout (sec)** to a longer amount of time.

**Step 2:** Filter the Decryption log (**Monitor > Logs > Decryption**) to find certificate revocation errors using the query (error eq 'OCSP/CRL check: certificate revoked').

Q [error eq 'OCSP/CRL check: certificate revoked'] → X

	RECEIVE TIME	APPLICATION	SOURCE ZONE	DESTINA... ZONE	PROXY TYPE	SOURCE ADDRESS	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	TLS VERSION	ROOT STATUS	POLICY NAME
05/22 11:55:19	incomplete	Inside	Outside	Forward		172.30.100.155	Certificate	OCSP/CRL check: certificate revoked	www.norway.no	TLS1.3	trusted	Big Brother

### Step 3: (Optional) Double-check the certificate expiration date at the Qualys [SSL Labs](#) site.

Enter the hostname of the server (**Server Name Identification** column of the Decryption log) in the **Hostname** field and **Submit** it to view certificate information for the host.

### Repair Incomplete Certificate Chains

Not all websites send their complete certificate chain even though the [RFC 5246 TLSv1.2 standard](#) requires authenticated servers to provide a valid certificate chain leading to an acceptable certificate authority. When you enable decryption and apply a Forward Proxy Decryption profile that enables Block sessions with untrusted issuers in the Decryption policy, if an intermediate certificate is missing from the certificate list the website's server presents to the firewall, the firewall can't construct the certificate chain to the top (root) certificate. In these cases, the firewall presents its Forward Untrust Certificate to the client because the firewall cannot construct the chain to the root certificate and trust cannot be established without the missing intermediate certificate.

If a website you need to communicate with for business purposes has one or more missing intermediate certificates and the Decryption profile blocks sessions with untrusted issuers, then you can find and download the missing intermediate certificate and install it on the firewall as a Trusted Root CA so that the firewall trusts the site's server. (The alternative is to contact the website owner and ask them to configure their server so that it sends the intermediate certificate during the handshake.)

#### Step 1: Find websites that cause incomplete certificate chain errors.

1. Filter the Decryption log to identify Decryption sessions that failed because of an incomplete certificate chain.

In the filter field, type the query (`err_index eq Certificate`) and (`error contains 'http'`). This query filters the logs for Certificate errors that contain the string "http", which finds all of the error entries that contain the CA Issuer URL (often called the URI). The CA Issuer URL is the Authority Information Access (AIA) information for the CA Issuer.

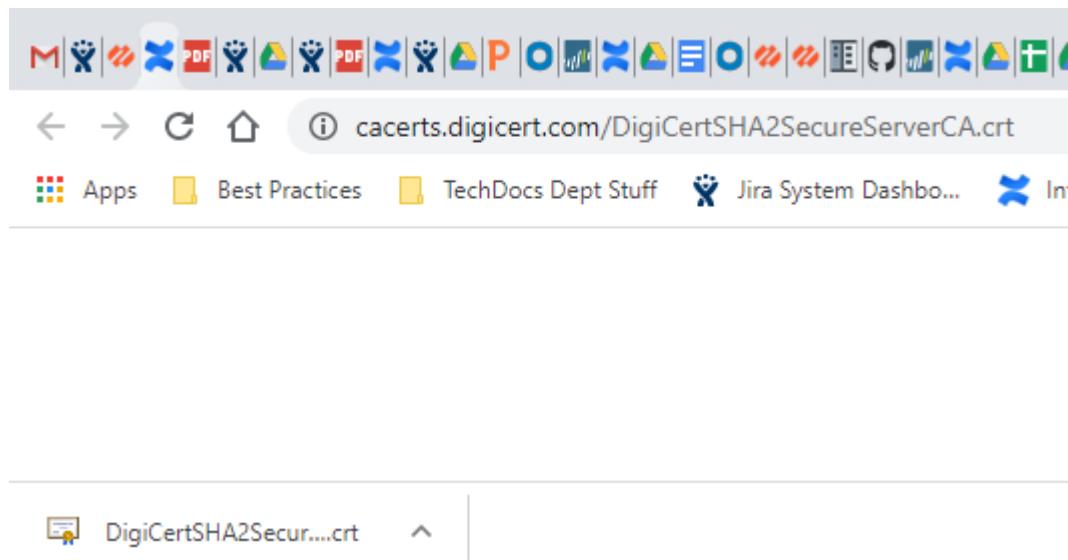
2. Click an **Error** column entry that begins "Received fatal alert UnknownCA from client. CA Issuer URL:" followed by the URI.

Received fatal alert UnknownCA from client. CA Issuer URL: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.cer ] → X ⊞ ⊖ ⊕

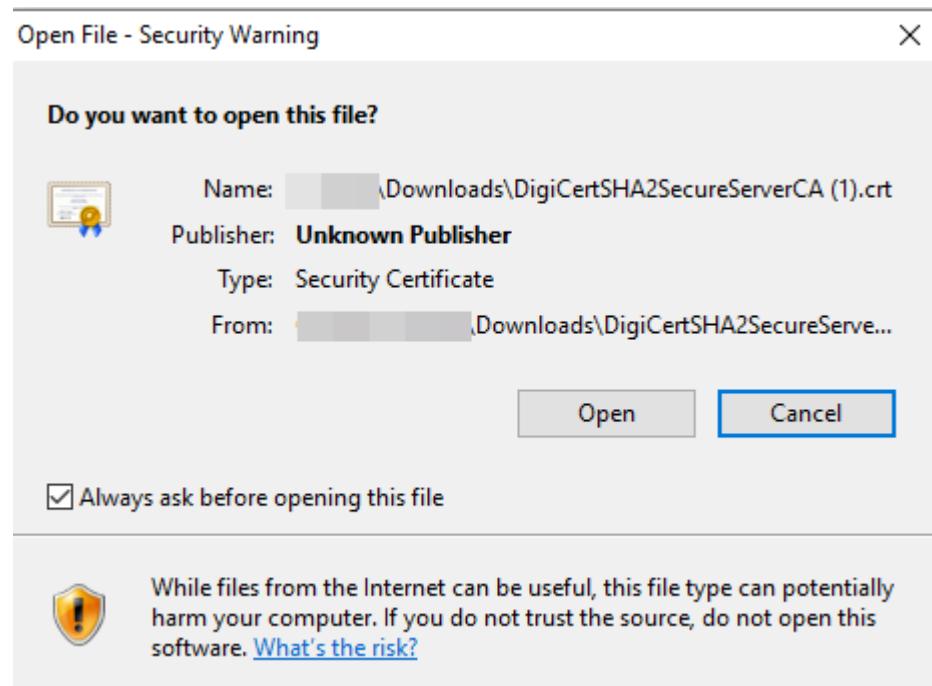
ROOT STATUS	SUBJECT COMMON NAME	ISSUER COMMON NAME	CERTIFICATE KEY TYPE	CERTIFICATE KEY SIZE	SERVER NAME IDENTIFICATION	TLS VERSION	KEY EXCHANGE	ENCRYPTION ALGORITHM	NEGOTIATED EC CURVE	AUTHENTICATION ALGORITHM	ERROR	ERROR INDEX
untrusted	*.badssl.com	DigiCert SHA2 Secure Server CA	RSA	2048	incomplete-chain.badssl.com	TLS1.2	ECDHE	AES_128_GCM	secp256r1	SHA256	Received fatal alert UnknownCA from client. CA Issuer URL: http://cacerts.digicert...	Certificate

The firewall automatically adds the selected error to the query and shows the full URI path (the full URI path may be truncated in the **Error** column).

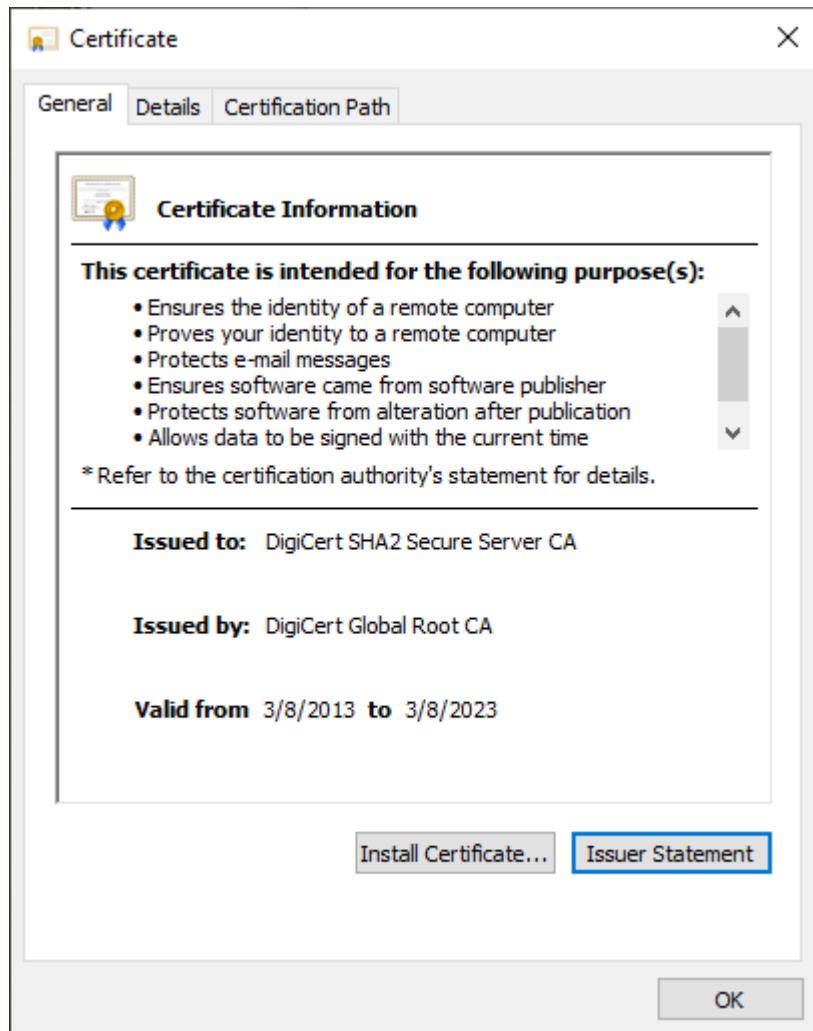
**Step 2:** Copy and paste the URI into your browser and then press Enter to download the missing intermediate certificate.



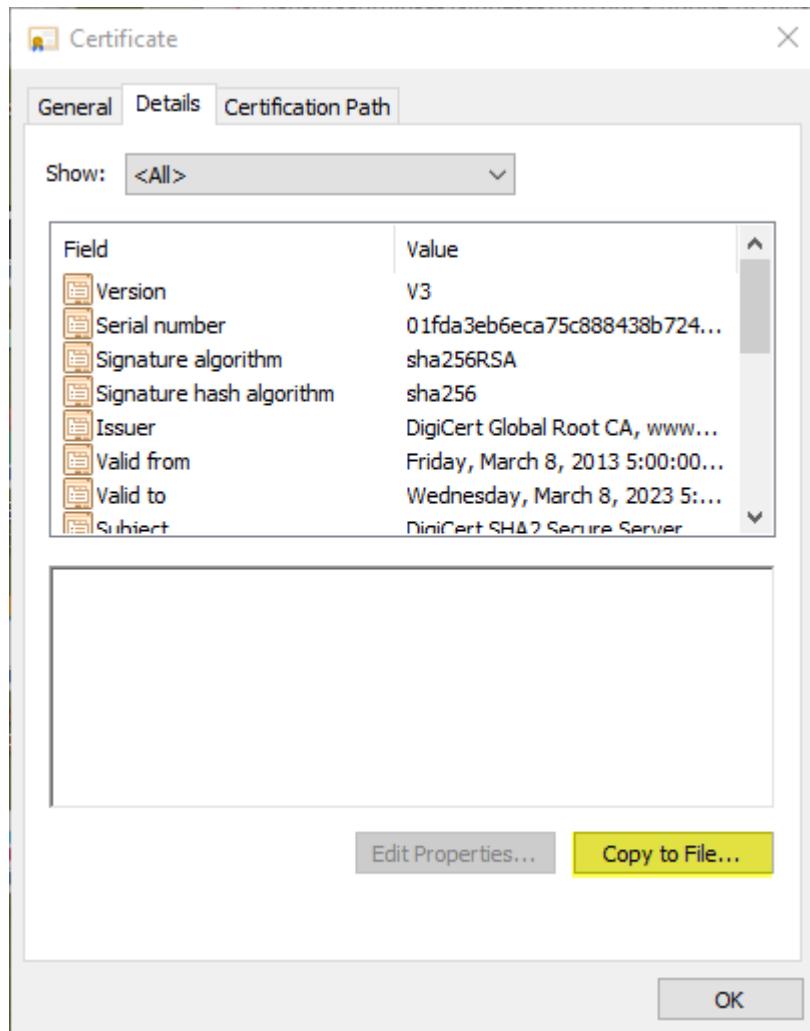
**Step 3:** Click the certificate to open the dialog box.



**Step 4:** Click Open to open the certificate file.



**Step 5:** Select the **Details** tab and then click **Copy to File....**



Follow the export directions. The certificate is copied to the folder you designated as your default download folder.

**Step 6:** Import the certificate into the firewall.

1. Navigate to **Device > Certificate Management > Certificates** and then select **Import**.
2. **Browse** to the folder where you stored the missing intermediate certificate and select it. Leave the **File Format as Base64 Encoded Certificate (PEM)**.

**Import Certificate**

(?)

Certificate Type  Local  SCEP

Certificate Name

Certificate File  [Browse...](#)

File Format  [▼](#)

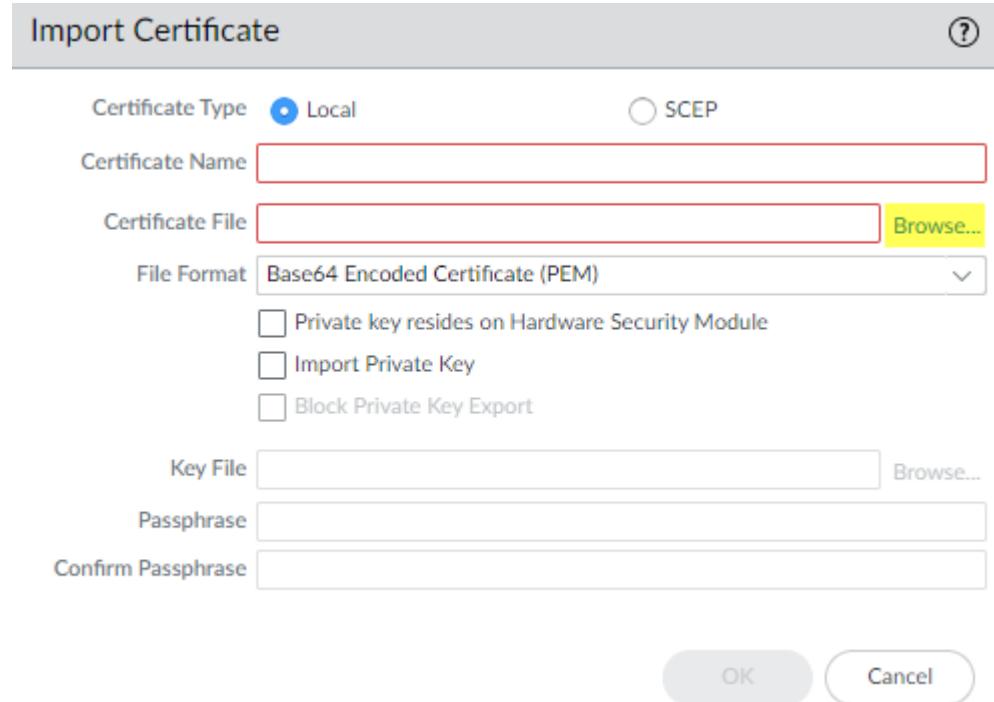
Private key resides on Hardware Security Module  
 Import Private Key  
 Block Private Key Export

Key File  [Browse...](#)

Passphrase

Confirm Passphrase

[OK](#) [Cancel](#)



3. Name the certificate and specify any other options you want to use, then click **OK**.

**Step 7:** When the certificate has imported, select the certificate from the **Device Certificates** list to open the Certificate Information dialog.

**Step 8:** Select **Trusted Root CA** to mark the certificate as a Trusted Root CA on the firewall and then click **OK**.

Certificate information (?)

Name	missing-intermediate-certificate-example
Subject	/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
Issuer	/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
Not Valid Before	Mar 8 12:00:00 2013 GMT
Not Valid After	Mar 8 12:00:00 2023 GMT
Algorithm	RSA
<input checked="" type="checkbox"/> Certificate Authority <input type="checkbox"/> Forward Trust Certificate <input type="checkbox"/> Forward Untrust Certificate <input checked="" type="checkbox"/> Trusted Root CA	

Revoke
OK
Cancel

In **Device > Certificate Management > Certificates > Device Certificates**, the imported certificate now appears in the list of certificates. Check the **Usage** column to confirm that the status is **Trusted Root CA Certificate** to verify that the firewall considers the certificate to be a trusted root CA.

**Step 9: Commit** the configuration.

**Step 10:** You have now repaired the broken certificate chain.

The firewall doesn't block the traffic because the CA issuer is not untrusted anymore. Repeat this process for all missing intermediate certificates to repair their certificate chains.

### 6.3.5 References

Enhanced Decryption Troubleshooting:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption>

Proxy Decryption Profile:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts/ssh-proxy-decryption-profile>

Decryption Overview

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-overview>

How to Implement and Test SSL Decryption

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEZCA0>

Troubleshoot and Monitor Decryption:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption>

Troubleshoot Expired Certificates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/troubleshoot-certificate-expiration-issues>

Identify Untrusted CA Certificates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/identify-untrusted-certificateAuthorities>

Troubleshoot Pinned Certificates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/troubleshoot-pinned-certificates>

Troubleshoot Revoked Certificates:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/troubleshoot-revoked-certificates>

Repair Incomplete Certificate Chains:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs/repair-incomplete-certificate-chains>

### 6.3.6 Sample Questions

1. Why would SSL decryption that has been working for a customer suddenly stop?

- a. The firewall's CA certificate expired.
- b. The firewall's IP address, which is encoded in the certificate, changed.
- c. The firewall has been upgraded to a different model.
- d. The firewall's decryption subscription expired.

2. A company uses a small SaaS application provider. This application is accessed through HTTPS but suddenly stops working through the firewall. However, when the application is accessed from home, users receive an error about the certificate. Which two situations would explain this behavior? (Choose two.)

- a. The SaaS certificate had expired. The firewall's decryption policy is configured to block connections with expired certificates.
- b. The SaaS certificate had expired. The firewall's decryption policy is configured to use the untrusted CA with expired certificates.

- c. The SaaS certificate was replaced with one whose CA is not known to the firewall. The firewall's decryption policy is configured to block connections with certificates whose CA is not trusted.
  - d. The SaaS certificate was replaced with one whose CA is not known to the firewall. The firewall's decryption policy is configured to use the untrusted certificate for certificates whose CA is not trusted.
  - e. The firewall's own CA certificate needs to be updated.
3. Which encryption algorithm is not supported by the firewall and causes the firewall to drop the connection?
- a. DES
  - b. 3DES
  - c. AES256-CBC
  - d. AES256-GCM

## 6.4 Troubleshoot routing

The NGFW uses several methods and configurations to route traffic. They are described in the following sections.

### 6.4.1 Dynamic routing

- **RIP** is an 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. The protocol limits routes to a maximum of 15 hops and thus 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.
- **OSPF** is an IGP that most often is used to dynamically manage network routes in a large enterprise network. It determines routes dynamically by obtaining information from other routers and advertising routes to other routers with Link State Advertisements (LSAs). The information gathered from the LSAs is used to construct a topology map of the network. Each router builds its own topology map from received LSAs, and the map is used to populate the IP routing table with available routes.

Changes in the network topology are detected dynamically and are used to generate a new topology map within seconds. A shortest path tree is computed for each route. Metrics associated with each routing interface are used to calculate the best route. These metrics can include distance, network throughput, and link availability. These metrics also can be configured statically to direct the outcome of the OSPF topology map.

- **BGP** is the primary internet routing protocol. BGP determines network reachability based on IP prefixes that are available within autonomous systems, where an asynchronous system is a set of IP prefixes that a network provider has designated to be part of a single routing policy.

## 6.4.2 Redistribution profiles

Route redistribution on the firewall is the process of making routes that the firewall learned from one routing protocol (or a static or connected route) available to a different routing protocol, thereby increasing accessibility of network traffic. Without route redistribution, a router or virtual router advertises and shares routes only with other routers that run the same routing protocol. You can redistribute IPv4 or IPv6 BGP, connected, or static routes into the OSPF RIB and redistribute OSPFv3, connected, or static routes into the BGP RIB.

This means, for example, you can make specific networks that were once available only by manual static route configuration on specific routers available to BGP autonomous systems or OSPF areas. You can also advertise locally connected routes, such as routes to a private lab network, into BGP autonomous systems or OSPF areas.

You might want to give users on your internal OSPFv3 network access to BGP so they can access devices on the internet. In this case you would redistribute BGP routes into the OSPFv3 RIB.

Conversely, you might want to give your external users access to some parts of your internal network, so you make internal OSPFv3 networks available through BGP by redistributing OSPFv3 routes into the BGP RIB.

To [Configure Route Redistribution](#), begin by creating a redistribution profile.

## 6.4.3 Static routes

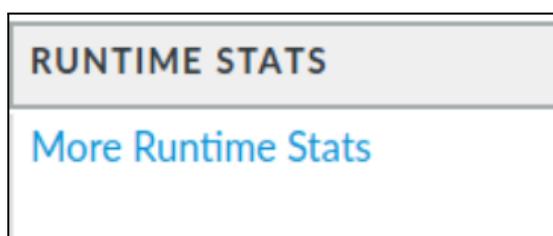
### *Troubleshooting Traffic Routing Issues*

Static routes require manual configuration on every router in the network, rather than a routing protocol automatically entering dynamic routes into the firewall's routing table. Even though static routes require manual configuration on all routers, they may be simpler and easier to troubleshoot in small networks.

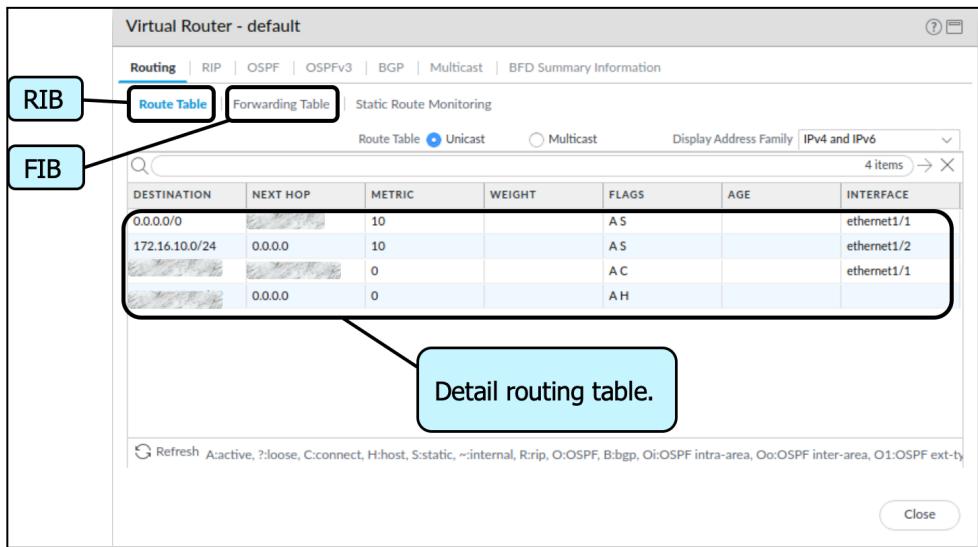
## 6.4.4 Route monitoring

### *Routing Troubleshooting*

Routing decisions made by a virtual router can be diagnosed easily. A virtual router maintains a RIB and a FIB, which can be displayed in the management web interface using the **Runtime Stats** link displayed on the virtual router summary line:



Click the **More Runtime Stats** link to access the RIB and FIB, plus additional displays that contain the status of any enabled dynamic routing protocols.



### Troubleshooting Routing

The CLI has advanced troubleshooting for routing functions. Output from the debug **routing...** command provides insight into router processing, including advanced debugging logs and routing-specific packet captures.

### 6.4.5 PBF

The firewall in most cases uses the destination IP address in a packet to determine the egress interface. The firewall uses the routing table associated with the virtual router to which the interface is connected to perform the route lookup. PBF allows you to override the routing table. You can specify the egress interface-based set parameters (such as destination IP address) or type of traffic.

When you create a PBF rule, you must specify:

- A name for the rule
- A source zone or interface
- An egress interface

You can specify the source and destination addresses using an IP address, an address object, or a FQDN. Note that application-specific rules are not recommended for use with PBF because PBF rules may be applied before the firewall has determined the application.

### 6.4.6 Multicast routing

Add multicast routing profiles to efficiently configure IPv4 multicast for a logical router.

MULTICAST ROUTING PROFILES	DESCRIPTION
----------------------------	-------------

<b>Multicast IPv4 PIM Interface Timer Profile</b>	
Name	Enter a name for the profile (maximum of 31 characters). The name must start with an alphanumeric character, underscore (_), or hyphen (-), and contain zero or more alphanumeric characters, underscore (_) or hyphen(-). No dot (.) or space is allowed.
Assert Interval	Enter the number of seconds between PIM Assert messages that the logical router sends to other PIM routers on the multiaccess network when they are electing a PIM forwarder. Range is 0 to 65,534; default is 177.
Hello Interval	Enter the number of seconds between PIM Hello messages that the logical router sends to its PIM neighbors from each interface in the interface group. Range is 1 to 180; default is 30.
Join Prune Interval	Enter the number of seconds between PIM Join messages (and between PIM Prune messages) that the logical router sends upstream toward a multicast source. Range is 60 to 600; default is 60.
<b>Multicast IPv4 IGMP Interface Query Profile</b>	
Name	Enter a name for the profile (maximum of 31 characters). The name must start with an alphanumeric character, underscore (_), or hyphen (-), and contain zero or more alphanumeric characters, underscore (_) or hyphen(-). No dot (.) or space is allowed.
Max Query Response Time	Enter the maximum number of seconds allowed for a receiver to respond to an IGMP membership Query message before the logical router determines that the receiver no longer wants to receive multicast packets for the group. Range is 1 to 25; default is 10.
Query Interval	Enter the number of seconds between IGMP membership Query messages that the logical router sends to a receiver to determine whether the receiver still wants to receive the multicast packets for a group. Range is 1 to 1,800; default is 125.

Last Member Query Interval	Enter the number of seconds allowed for a receiver to respond to a Group-Specific Query that the logical router sends after a receiver sends a Leave Group message. Range is 1 to 25; default is 1.
leave group immediately when a leave message is received	If you enable this, when there is only one member in a multicast group and the logical router receives an IGMP Leave message for that group, this setting causes the logical router to remove that group and outgoing interface from the multicast routing information base (mRIB) and multicast forwarding information base (mFIB) immediately, rather than waiting for the Last Member Query Interval to expire. Enabling this setting saves network resources. Default is disabled.

#### 6.4.7 Service routes

Configure service routes globally for the firewall. 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.

#### 6.4.8 References

Route Redistribution:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/route-redistribution>

Understanding Redistribution Profile Behavior if Using Destination Filter:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfnCAC>

Network > Routing > Routing Profiles > Multicast:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-routing-routing-profiles/network-routing-routing-profiles-multicast>

Service Routes:

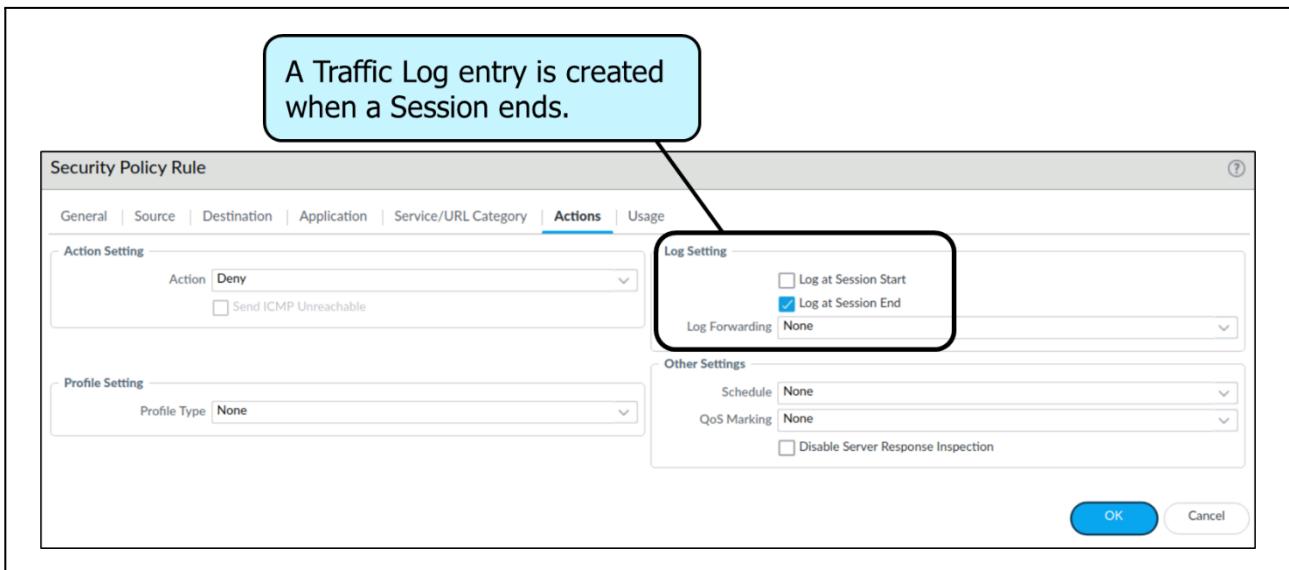
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service-routes>

## 6.5 Use logs, reports, and graphs to troubleshoot

### 6.5.1 Identify system and traffic issues using the web interface and CLI tools

#### *Transit Traffic Not Passing Through as Expected*

If traffic is not transiting a firewall as expected, three primary information sources are available in the management web interface: the Traffic log, the Session Browser, and traffic capture features. These sources are described in the following sections.



If you believe that the traffic to be evaluated has been received by the firewall, initial investigation should begin with the Traffic log. The Traffic log can be found at **Monitor > Logs > Traffic**. The default behavior of the firewall is to create a summary entry for each session when it ends. This behavior is controlled by the Log Setting field on the Actions tab of each Security policy rule. Because each Security policy rule has its own logging configuration, different rules can be configured to log information in different ways.

If the traffic in question includes at least one closed session, then an entry for the session should appear in the Traffic log. You can display detailed information about that session by clicking the magnifying glass icon in the left column:

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. In the 'Logs' section, under 'Traffic', there is a list of log entries. One specific entry is highlighted with a magnifying glass icon. A callout bubble with the text 'Click on magnifying glass icon for detailed information about this log entry.' points to this icon.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	APPLICATION	ACTION
	05/18 16:37:12	end	Users	Internet	192.168.1.20	ssl	allow
	05/18 16:36:26	end	Users	Internet	192.168.1.20	dns	allow
	05/18 16:36:26	end	Users	Internet	192.168.1.20	dns	allow
	05/18 16:36:26	end	Users	Internet	192.168.1.20	dns	allow
	05/18 16:36:04	end	Users	Internet	192.168.1.20	dns	allow

The following screenshot shows the details of one of the entries listed:

The screenshot shows a detailed view of a log entry. The title bar says 'Detailed Log View'. A callout bubble says 'Detailed view of a log entry.' The main area is divided into three sections: General, Source, and Destination. The General section contains session details like Session ID, Action, and Rule. The Source section contains source user and DAG details. The Destination section contains destination user and interface details. Below these sections is a table with columns for PCAP, RECEIVE TIME, TYPE, APPLICATION, ACTION, RULE, RULE UUID, BY..., SEVERI..., CATEG..., URL CATEG..., LIST, VERDI..., URL, and FILE NAME. A single row of data is shown in the table.

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2020/05/18 16:36:26	end	dns	allow	Users_...	7a2d1...	484		any				

The presence of a log entry confirms that properly formed traffic has reached the firewall and has been evaluated by a Security policy rule. Traffic could be processed without reaching a session end, which would result in no log entry yet. The Session Browser allows troubleshooting of open sessions that might not have been logged yet.

The detailed session information should be used to evaluate the handling of the traffic. The **Source** and **Destination** sections display header data and confirm potential NATs being applied. The **General** section confirms the action taken by the Security policy rule and the rule's name, App-ID, protocol, time seen, and the reason the session ended. The **Details** section shows the packet summary for the reported session, including counts and size.

Examination of this information often confirms the firewall's handling of the traffic. It also might show unexpected behavior to correct, as required.

If a session has not ended and no Traffic log entry has been made, you can use the Session Browser to display all open sessions currently known to the firewall. You can expand each session and examine details.

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM	CLEAR
06/27/00:20:10	Users_Net	Internet	192.168.1.254	130.211.6.196	47542	443	6	paloalto-dns-security	Allow-Internet-Access	ethernet1/2	ethernet1/1	16533	vsys1	
06/27/00:24:46	Users_Net	Internet	192.168.1.20	172.217.1.138	37510	443	6	google-base	Allow-Internet-Access	ethernet1/2	ethernet1/1	10927	vsys1	
06/27/00:24:55	Users_Net	Internet	192.168.1.20	152.199.5.24	57066	443	6	ssl	Allow-Internet-Access	ethernet1/2	ethernet1/1	984	vsys1	
06/27/00:24:52	Users_Net	Internet	192.168.1.20	4.2.2.2	44800	53	17	dns	Allow-Internet-Access	ethernet1/2	ethernet1/1	362	vsys1	
06/27/00:24:40	Users_Net	Internet	192.168.1.20	4.2.2.2	44380	53	17	dns	Allow-Internet-Access	ethernet1/2	ethernet1/1	246	vsys1	
06/27/00:24:13	Users_Net	Internet	192.168.1.254	35.222.124.72	45850	443	6	paloalto-wildfire-cloud	Allow-Internet-Access	ethernet1/2	ethernet1/1	10384	vsys1	
06/27/00:24:42	Users_Net	Internet	192.168.1.20	4.2.2.2	50720	53	17	dns	Allow-Internet-Access	ethernet1/2	ethernet1/1	353	vsys1	
06/27/00:24:54	Users_Net	Internet	192.168.1.20	23.11.218.15	39652	443	6	ssl	Allow-Internet-Access	ethernet1/2	ethernet1/1	85627	vsys1	
06/27/00:24:52	Users_Net	Internet	192.168.1.20	4.2.2.2	60359	53	17	dns	Allow-Internet-Access	ethernet1/2	ethernet1/1	185	vsys1	
06/27/00:24:51	Users_Net	Internet	192.168.1.20	52.22.231.198	52326	443	6	ssl	Allow-Internet-Access	ethernet1/2	ethernet1/1	8236	vsys1	
06/27/00:24:53	Users_Net	Internet	192.168.1.20	4.2.2.2	38692	53	17	dns	Allow-Internet-Access	ethernet1/2	ethernet1/1	428	vsys1	
06/27/00:24:55	Users_Net	Internet	192.168.1.20	84.37.72.32	38484	443	6	ssl	Allow-Internet-Access	ethernet1/2	ethernet1/1	3943	vsys1	
06/27/00:24:53	Users_Net	Internet	192.168.1.20	99.84.173.146	60520	443	6	ssl	Allow-Internet-Access	ethernet1/2	ethernet1/1	50426	vsys1	

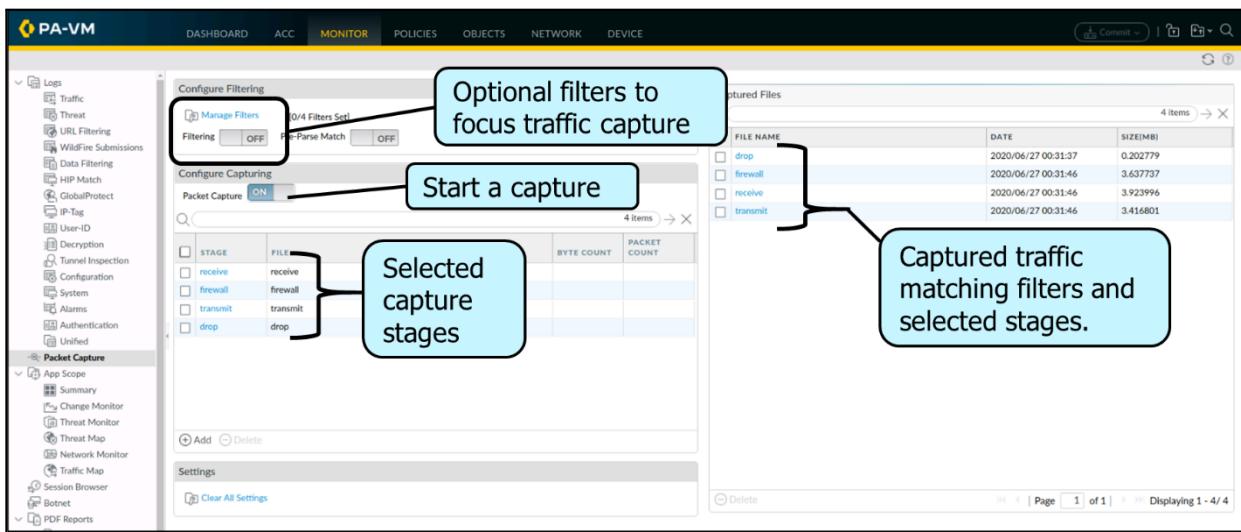
## Performing a Packet Capture

Palo Alto Networks firewalls can capture traffic automatically in response to threat detection, or you can manually perform a packet capture on network threats. Packet capture tools are available in the web interface and CLI.

When troubleshooting requires the examination of actual packet contents, a packet capture can be performed on the firewall and subsequently downloaded as a pcap-formatted file ready for external software consumption. Packet capture settings are found under **Monitor > Packet Capture**.

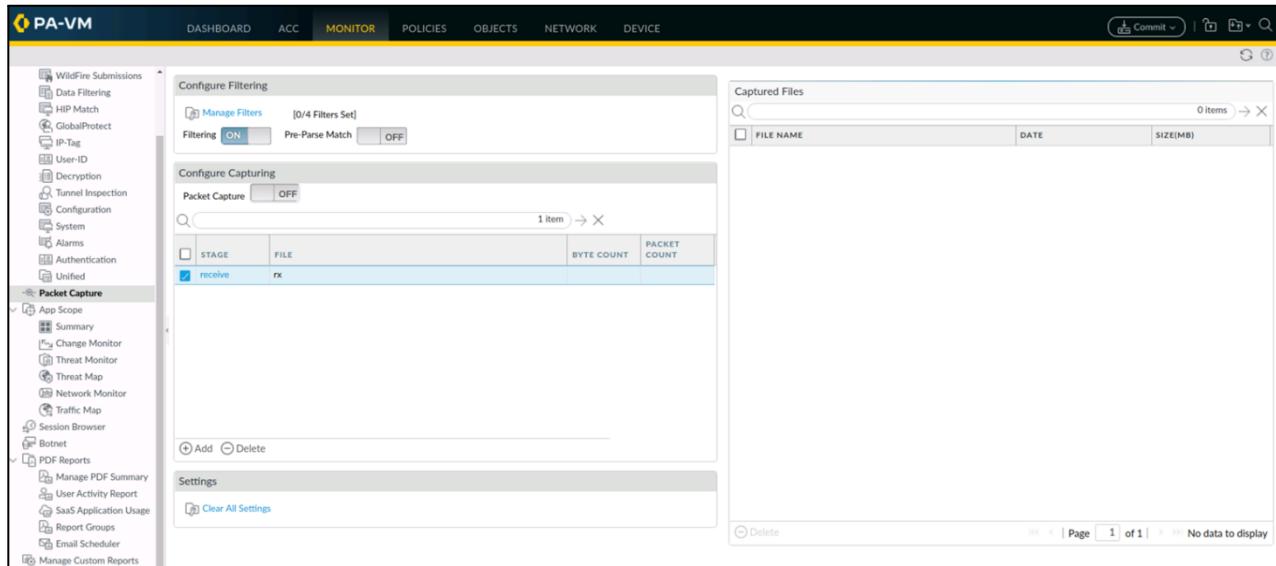
## Manual Packet Captures

Packet captures can be conducted on demand both from the web interface and the CLI. Web interface captures are configured using the **Monitor > Packet Capture** option. This packet capture process will *not* capture management interface traffic. The following image shows configuration options to create a web interface capture and turn it on or off. Captured traffic is stored on the firewall and is available for download as a pcap file usable by many protocol analysis software packages. The capture configuration follows:



The PAN-OS web interface provides access to traffic packet captures. Additional pcap and debug tools are available through the CLI.

**Note:** Some Palo Alto Networks firewalls include a Hardware Offload feature that optimizes the handling of traffic. Offloaded traffic will not appear in packet captures in either the web interface or the CLI. PA-3050, PA-3060, PA-5000 Series, PA-5200 Series, and PA-7000 Series firewalls have this feature. To guarantee that all packets are available for capture, a CLI command must be run to temporarily disable Hardware Offload. Note that management interface traffic cannot be captured by the previously mentioned CLI tools. The **tcpdump** command is the only tool with visibility to this traffic.



### Clearing Existing Settings

The **Clear All Settings** option turns off packet capture and clears all packet capture settings, including filters and capture stages. It also clears settings for any advanced debug-level packet-diagnostics features, such as

flow basic, for which there are no controls or status indicators in the web interface. Use of **Clear All Settings** does not turn off automated packet captures associated with any active Security Profiles.

**Warning:** If you manually clear just the filters while another firewall administrator is actively running a capture, the running capture will start to capture all packets with no filters. Before you clear any existing filters, confirm that the filters are not being used. If another administrator has saved filters that are meant to be used later, you can disable those filters rather than delete them. Use of **Clear All Settings** will clear all filters and turn off all captures.

### ***Configuring and Turning on the Filters***

You must configure and turn on filtering and then turn on packet capture before any sessions that you want to capture will begin being captured. Existing sessions will not be marked for capture.

### ***Adding Stages and Filenames***

Filtering alone is not resource-intensive, whereas turning on packet capture and turning on debug-level logging is resource-intensive. Therefore, the decision whether to configure your capture stages before or after turning on filtering generally is not that important.

You can, for example, configure your filters, turn them on, and then monitor them using CLI commands for session volume before you complete the rest of the configuration. To monitor the number of marked sessions, use the CLI command **show counter global filter delta yes packet-filter yes**. Execute the command once and then a second time to see the difference (the delta) from the prior execution of the command.

**Tip:** To analyze “internal and “external” sessions within a single file, you can configure the receive and transmit stages to write to the same filename, which will result in a merged pcap file.

When you configure a capture stage, you can specify the maximum number of bytes and the maximum number of packets, after which capturing stops.

A brief description of the four available capture stages follows:

- **Receive stage:** The firewall produces receive-stage packet captures by applying the capture filter(s) on a packet-per-packet basis. Receive-stage captures include all packets captured by the firewall’s logical interfaces. Receive-stage captures can help you determine whether a packet is reaching the firewall.

However, because of potential hardware offloading and pre-parse discards, a receive-stage capture may not produce the same results as physically tapping the wire just outside the correct physical ingress port of the firewall.

The receive stage will not capture both flows of a session unless the filter configuration matches to traffic in each direction.

- **Firewall stage:** On firewalls running PAN-OS 8.0 and earlier, packets captured at the firewall and transmit stages will be captured when the corresponding session has been matched to a capture-filter statement.

Firewalls running PAN-OS 8.1 and later capture packets at the firewall and transmit stages by the same effective logic (though not the same) as the receive stage — that is, only if the individual flow (c2s or s2c) matches the filter configuration.

Firewall-stage capture shows you what is inside the box. The firewall-stage capture point is post-ingress, post-session-setup, and pre-NAT.

The flow logic of the firewall stage itself applies NAT as the last or nearly last step of Layer 2-to-Layer 4 packet processing and before any Layer 7 packet-payload content analysis begins. The IP addresses of packets captured by the firewall stage will match the pre-NAT addressing as defined in the session table. Also, packets that the firewall drops because of Layer 2-to-Layer 4 processing (such as packets dropped because of a session-closed status) will appear in the drop-stage pcap with pre-NAT addressing.

Packets that the firewall drops because of a deny action triggered by a Security policy or Security Profile will appear in the drop-stage pcap with post-NAT addressing.

If NAT is involved, the packet-threading, flow-following, or stream-following features of packet analyzers will not work for firewall-stage pcaps. With NAT, packet threading is possible only if you configure the receive-stage and transmit-stage pcaps and then merge them. You can make the firewall automatically merge receive-stage pcaps and transmit-stage pcaps by configuring them with the same filename.

- **Drop stage:** The drop-stage packet capture is perhaps best thought of as the result of a logging event, instead of a traditional off-the-wire packet capture. Packets in the drop-stage capture are captured after the capture point of the stage that drops the packet. Thus, packets in the drop-stage capture also will be found in the pcap for the stage from which the packet was dropped.

A packet dropped in the receive stage will appear in both the drop-stage pcap and the receive-stage pcap. You also typically will find packets that fail the initial session setup process in both the receive-stage and drop-stage pcaps. Packets dropped by or subsequent to the firewall stage will be found in both the drop-stage and firewall-stage pcaps.

Drop-stage pcaps comprise copies of individual packets that are dropped. Drop-stage pcaps do not include prior or subsequent packets for contextual analysis. Drop-stage pcaps include only the exact packets dropped. If you want to better understand why a packet has been dropped, query the global counters, review log data, and run additional debug-level packet-diagnostic features, such as flow basic.

- **Transmit stage:** Capture of packets at the transmit stage shows you packets as they egress from the firewall's logical interface. In transmit-stage pcaps, you can see block pages, resets, TCP MSS adjustments, and any other packets or packet transformations created by the firewall itself, including post-NAT addressing.

### ***Pre-Parse Match Option***

After a packet enters the ingress port, the firewall performs several basic pre-processing tests to ensure that the packet is viable before it is received for subsequent session setup or additional firewall processing. The firewall discards packets that fail these basic tests before the packet reaches the point where it is matched

against the capture and debug-log filters. For example, if a route lookup fails, a packet never will reach even the initial (receive) capture filter.

To capture packets that normally would be discarded before the filter match, the system emulates an initial, “pre-parse” positive match for every packet entering the system. This initial match allows all packets to be filtered subsequently by the normal receive-stage filtering process. The pre-parse match option is resource-intensive. You should consider using it only for advanced or rare troubleshooting purposes. Palo Alto Networks recommends that you use this option only under direct advice and guidance from technical support.

Troubleshooting route-lookup failures is the typical use case for using the pre-parse match option. However, such errors typically are easy to identify using the firewall’s interface counters.

To enable the pre-parse match option in the CLI, use the command **debug dataplane packet-diag set filter pre-parse-match yes**.

### *Turning On Capture*

After you turn on packet capture, you can monitor capture in a few ways:

- Refresh the Packet Capture page in the web interface and look first for the existence of new capture files, and then for their file size. You can refresh the page repeatedly to monitor any growth in the file size.
- Use the CLI to show the current packet-diagnostics settings by running the **debug dataplane packet-diag show setting** command. The bottom of the settings summary includes the same data displayed in the **Captured Files** section of the Packet Capture page in the web interface.
- Monitor currently marked sessions, in addition to verifying that the capture-stage files are growing.

### *Turning Off Capture and Then Filtering*

Turn off packet capture before turning off filtering to avoid suddenly capturing all packets. You also may want to monitor any currently marked sessions using the CLI to ensure that the session(s) that you want to capture have finished. To show marked sessions, use the **CLI command show counter global filter delta yes packet-filter yes**. To show the detailed status of a session, use the command **show session id [number]**.

### *Exporting and Downloading pcaps*

To export pcaps from the web interface, simply click the hyperlink associated with the filename of the pcap you want to export. You can export pcaps from the CLI and display them in a similar way as you would use **tcpdump** within a Linux console.

The Palo Alto Networks firewall CLI offers access to more debugging information and often is used by experienced administrators for troubleshooting. This section provides only a brief mention of basic CLI tools. See the “References” section for more complete information sources.

Connection to the CLI is possible using a serial console emulator or SSH connecting through the management port. The account used for firewall authenticating into the CLI must have CLI access enabled.

After you log in to the CLI, the command prompt by default is in *operational* mode. The commands available in operational mode include basic networking commands such as **ping** and **traceroute**, basic system commands such as **show**, and more advanced system commands such as **debug**. Debug commands allow you to set parameters that, if improperly used, can cause system failure. Commands to shut down and restart the system also are available from within operational mode.

*Configuration* mode enables you to display and modify the configuration parameters of the firewall, verify candidate configuration, and commit the configuration. Access it by typing the command **configure** while in operational mode.

CLI mode offers access to data not available in the web interface. Additional log files written by various subsystems of the firewall are available. Large files such as log files can be displayed with four principal commands: **show**, **tail**, **less**, and **grep**. A partial list of useful log files for troubleshooting can be found in the “References” section.

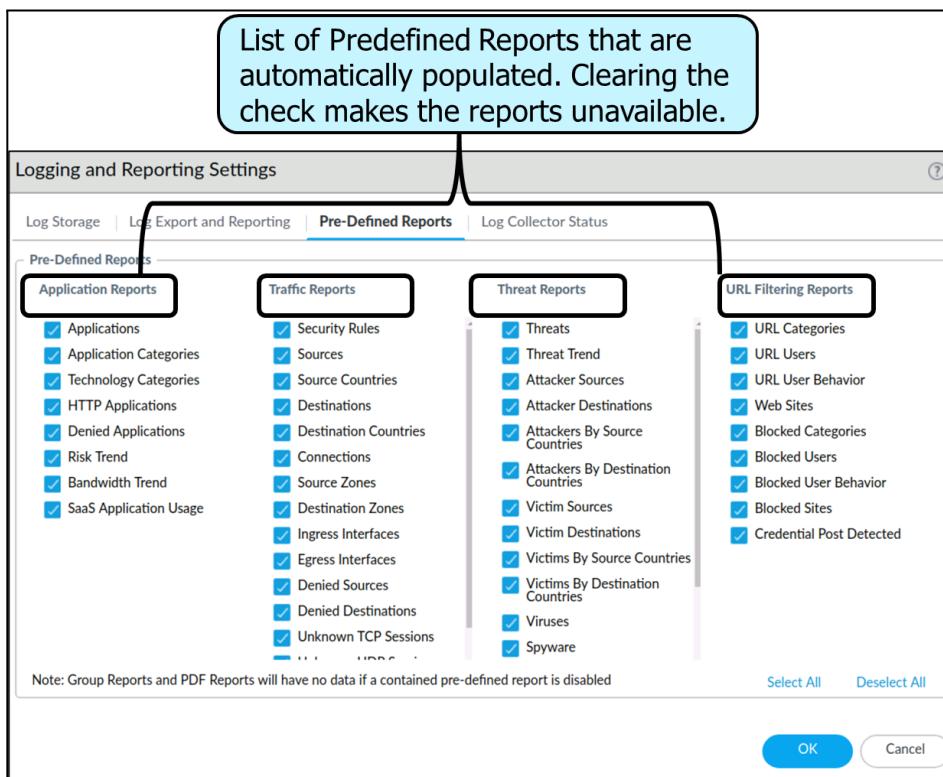
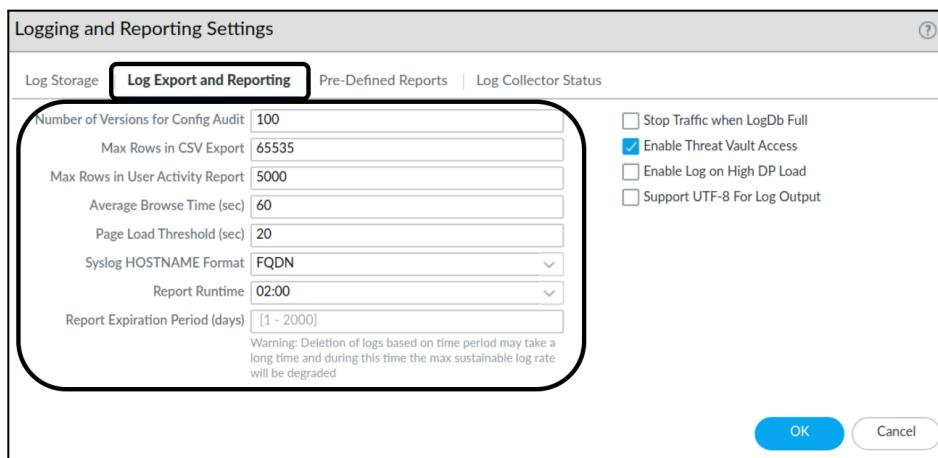
The **show** command is the main method to display values and settings. In operational mode, begin by typing **show**, entering a space, and then pressing the **Tab** key to invoke the autocomplete function, which shows all available options for the **show** command. Examine this list and explore its options to become familiar with accessing settings and values for troubleshooting. The command **show interface all** displays a summary of all configured interfaces, their link status, and assigned zones. The command **show system resources** displays the overall resources utilization status of the firewall. For troubleshooting purposes, the **test** command shows the results when simulated traffic is presented to various subsystems. For example, the command **test security-policy-match...** shows the security processing of the simulated traffic described at the end of the command. The command **test routing...** predicts the virtual router’s handling of the simulated traffic. Many **test** commands are available that can be found by entering **test** followed by a space and then pressing the **Tab** key for the autocomplete listing of options.

Packet captures also can be performed at the command line level. The same packet capture engine explored earlier through the web interface can be accessed from the CLI. Each configuration step used in the web interface has a command line equivalent. See the “References” section for the location of a detailed discussion.

### 6.5.2 Create and interpret reports

While log data is stored in detail in log storage, a firewall summarizes new log entries and adds the results to separate on-board reporting databases used as default sources by ACC, App Scope, PDF Reports, and Custom Reports.

The scope of this summarization process can be controlled with settings on **Device > Setup > Management > Logging and Reporting Settings**:



## PDF Reports

The **PDF Reports** section offers many predefined PDF reports that can be run as a group on a scheduled basis and delivered through email daily or weekly.

By default, these reports typically run once per day and summarize all activity on the firewall. A report browser of predefined reports appears on the right. In the following figure, chosen reports display their results for the previous day's traffic. The predefined report browser shows choices of categories and specific reports on the right:

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left, a sidebar under 'Reports' has 'PDF Reports' expanded, with 'SaaS Application Usage' selected. The main area displays a table titled 'DESTINATION COUNTRY' with the following data:

	DESTINATION COUNTRY	BYTES	SESSIONS
1	192.168.0.0-192.168.255.255	22.0M	152.4k
2	United States	141.0M	18.3k
3	United Kingdom	13.3k	47
4	Ireland	6.2k	1

At the bottom of the main area are three export options: 'Export to PDF', 'Export to CSV', and 'Export to XML'. To the right, a sidebar titled 'Application Reports' shows 'Destination Countries' selected. Below it is a calendar for April 2020, with the 12th highlighted.

The **PDF Reports** section offers other important reporting tools. Custom reports can be created, stored, and run on demand or on a scheduled basis.

#### SaaS Application Usage Report

The App-ID engine identifies SaaS applications and provides additional functionality. A dedicated SaaS Application Usage report under **Monitor > PDF Reports > SaaS Application Usage** will help your organization identify applications storing your data in external locations. The App-IDs for SaaS applications contain additional data about these applications and their providers to help you make decisions allowing access to them at the organizational level.

**Application**

Name: dropbox-base

Standard Ports: tcp/17500, tcp/443, tcp/80, udp/17500

Depends on: google-base

Implicitly Uses: ssl, web-browsing

Deny Action: drop-reset

Additional Information: [Website](#) [Wikipedia](#) [Google](#) [Yahoo!](#)

**Characteristics**

Evasive: yes	Tunnels Other Applications: no
Excessive Bandwidth Use: no	Prone to Misuse: no
Used by Malware: no	Widely Used: yes
Capable of File Transfer: yes	SaaS: yes
Has Known Vulnerabilities: yes	

**Options**

Session Timeout (seconds): 30	<a href="#">Customize...</a>
TCP Timeout (seconds): 3600	<a href="#">Customize...</a>
UDP Timeout (seconds): 30	<a href="#">Customize...</a>
TCP Half Closed (seconds): 120	<a href="#">Customize...</a>
TCP Time Wait (seconds): 15	<a href="#">Customize...</a>
App-ID Enabled: yes	

**Classification**

Category: general-internet
Subcategory: file-sharing
Risk: <span style="background-color: orange; border: 1px solid black; padding: 2px;">4</span> <a href="#">Customize...</a>

**SaaS Characteristics**

Certifications: HIPAA, PCI, SOC I, SOC II, SSAE16
Data Breaches: no
IP Based Restrictions: no
Poor Financial Viability: no
Poor Terms Of Service: no

**Tags**

Web App [Edit](#)

[Close](#)

**Additional information about this SaaS application.**

Palo Alto Networks firewalls include a feature within the URL Filtering engine that provides HTTP header insertion for certain SaaS applications. This feature can prevent users from accessing private instances of a SaaS application while having access to the organization's sanctioned environment.

## User/Group Activity Reports

A predefined User Activity report provides complete application use and browsing activity reports for individuals or groups.

## PDF Summary Reports

A PDF Summary report includes several top-5-oriented reports grouped to provide a general representation of the firewall's traffic during the previous day.

## App Scope Reports

App Scope reports focus on baseline performance comparisons of firewall use. These reports provide powerful tools to characterize changes in detected use patterns. They were designed to be ad hoc reports, not regularly scheduled reports.

### 6.5.3 Create and interpret graphs

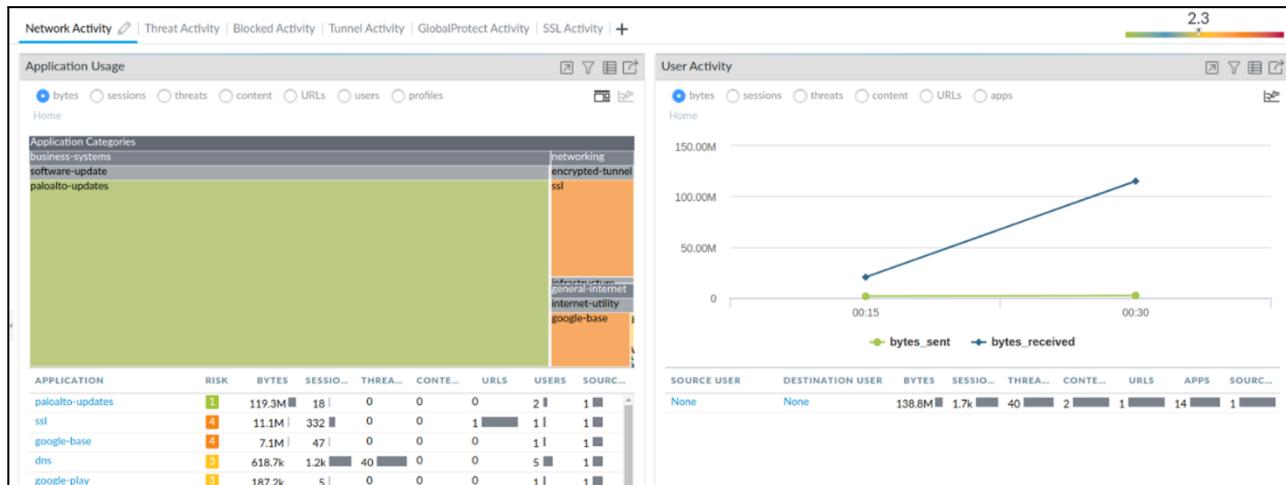
#### ACC

The 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 information about threats that can be acted on. The ACC layout includes a tabbed view of network activity, threat activity, and blocked activity. Each tab includes widgets for better visualization of network traffic. The graphical representation allows you to interact with the data and to see the relationships between events on the network, letting you uncover anomalies or find ways to enhance your network Security rules. For a personalized view of your network, you can add a custom tab and include widgets that allow you to find the information that is most important to you.

Other reports and displays on the firewall often support click-through of data items so you can uncover more detail. This practice often results in a switch to the ACC with preset filters to focus only on the previously displayed data.

#### Network Activity

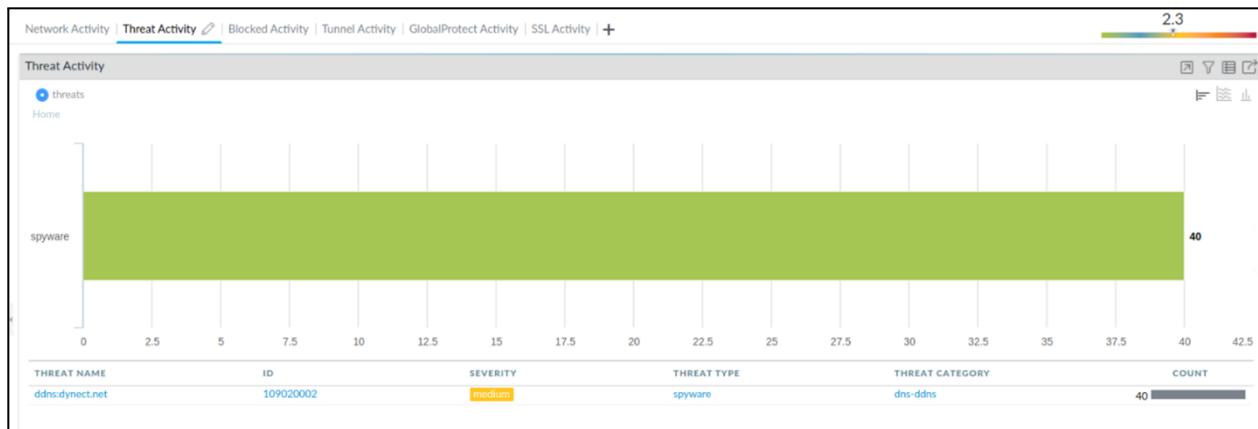
The **Network Activity** tab displays an overview of traffic and user activity on your network, including the top applications in use, the top users who generate traffic, and the most used Security rules against which traffic matches occur. You also can view network activity by source or destination zone, region, IP address, ingress or egress interfaces, and GlobalProtect host information such as the operating systems of the devices most commonly used on the network:



#### Threat Activity

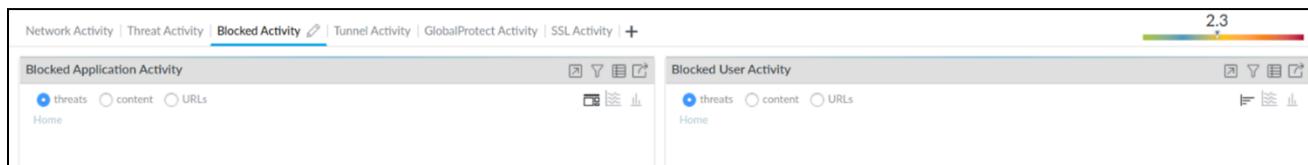
The **Threat Activity** tab displays an overview of the threats on the network, focusing on the top threats: vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top WildFire submissions by file type and application, and applications that use non-standard ports. The Compromised Hosts widget in this tab (not supported on all platforms) supplements detection with better visualization techniques; it uses the information from the **Correlated Events** tab (**Automated Correlation Engine > Correlated Events**) to present

an integrated view of compromised hosts on your network by source users and IP addresses, sorted by severity:



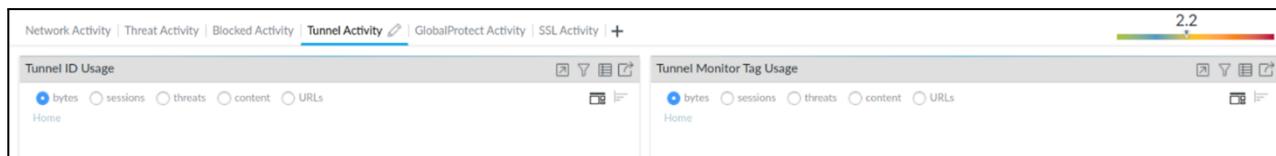
## **Blocked Activity**

The **Blocked Activity** tab 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, and 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.



## **Tunnel Activity**

The **Tunnel Activity** tab displays the activity of tunnel traffic that the firewall inspected based on your tunnel inspection policies. Information includes tunnel usage based on tunnel ID, monitor tag, user, and tunnel protocols, such as GRE, General Packet Radio Service Tunneling Protocol for User Data, and non-encrypted IPsec.



## **GlobalProtect Activity**

The ACC displays a graphical view of user activity in your GlobalProtect deployment on the GlobalProtect Activity tab. The following charts are available:

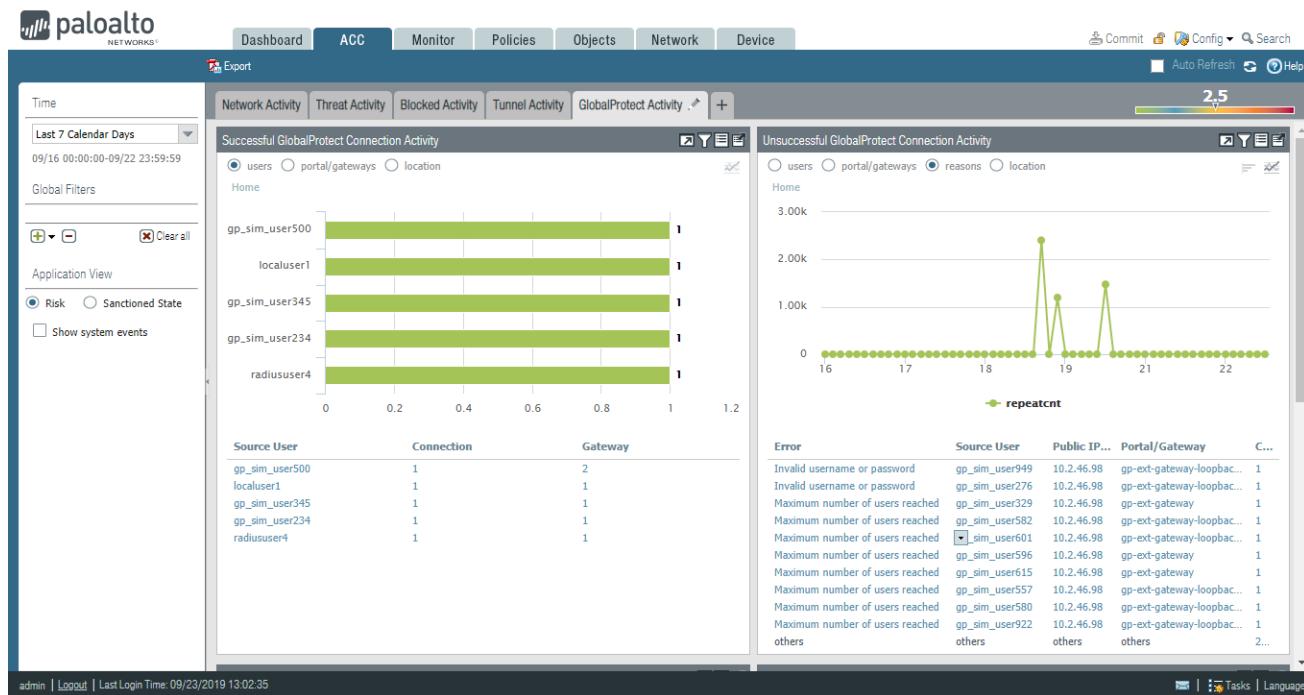
**Successful GlobalProtect Connection Activity**—Chart view of GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location.

**Unsuccessful GlobalProtect Connection Activity**—Chart view of unsuccessful GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location. To help you identify and troubleshoot connection issues, you can also view the reasons chart or graph. For this chart, the ACC indicates the error, source user, public IP address and other information to help you identify and resolve the issue quickly.

**GlobalProtect Deployment Activity**—Chart view summary of your deployment. Use the toggle at the top of the chart to view the distribution of users by authentication method, GlobalProtect app version, and operating system version.

The GlobalProtect Activity charts and graphs are also interactive and support similar drill-down functionality to other ACC charts and graphs.

In addition, the **GlobalProtect Host Information** widget under the Network Activity tab is now renamed **HIP Information**.



## SSL Activity

The new **ACC > SSL Activity** widgets show you details about both successful and unsuccessful SSL Decryption activity in your network. They identify traffic—applications and Server Name Identifications (SNIs)—that cause decryption issues and that use weak ciphers and algorithms. Use that knowledge to identify misconfigured Decryption policies and profiles and to make informed decisions about what traffic to allow and what traffic to block. You can view SSL/TLS traffic in the ACC in multiple ways:

- **Traffic Activity Widget**—Shows SSL/TLS activity compared to non-SSL/TLS activity by total number of sessions or bytes.

- **Successful TLS Version Activity Widget**—Shows successful TLS connections by TLS version and application or SNI. This widget helps you understand how much risk you are taking on by allowing weaker TLS protocol versions. Identifying applications and SNIs that use weak protocols enables you to evaluate each one and decide whether you need to allow access to it for business reasons. If you don't need the application for business purposes, you may want to block the traffic instead of allowing it. Click an application or an SNI to drill down and see detailed information.
- **Decryption Failure Reasons Widget**—Shows the reasons for decryption failures, such as certificate or protocol issues, by SNI. Use this information to detect problems caused by Decryption policy or profile misconfiguration or by traffic that uses weak protocols or algorithms. Click a failure reason to drill down and isolate the number of sessions per SNI or click an SNI to see the failures for that SNI.
- **SSL/TLS Traffic Widget**—Shows the amount of decrypted and non-decrypted traffic by sessions or bytes. Traffic that was not decrypted may be excepted from decryption by policy, policy misconfiguration, or by being on the Decryption Exclusion List (**Device > Certificate Management > SSL Decryption Exclusion**).
- **Successful Key Exchange Activity**—Shows successful key exchange activity per algorithm, by application or by SNI. Click a key exchange algorithm to see the activity for just that algorithm or click an application or SNI to view the key exchange activity for that application or SNI.

#### 6.5.4 References

View and Manage Logs:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-logs>

Generate Custom Reports:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports>

HTTP Header Insertion:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-security-profiles-url-filtering/http-header-insertion>

Generate User/Group Activity Reports:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-reports/generate-usergroup-activity-reports>

Manage PDF Summary Reports:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-reports/manage-pdf-summary-reports>

Use the App Scope Reports:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-app-scope-reports>

Use the Application Command Center:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-application-command-center>

Take a Custom Packet Capture:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/take-packet-captures/take-a-custom-packet-capture>

Disable Hardware Offload:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/take-packet-captures/disable-hardware-offload>

Log Types and Severity Levels:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels>

Monitor > Logs:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/monitor/monitor-logs>

CLI Cheat Sheet: Device Management:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-device-management>

CLI Cheat Sheet: Networking:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking>

Interpret VPN Error Messages:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages>

Virtual Routers:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/virtual-routers>

Site-to-Site VPN with Static and Dynamic Routing:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/site-to-site-vpn-quick-configs/site-to-site-vpn-with-static-and-dynamic-routing>

Static Route Overview:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/static-routes/static-route-overview>

RIP:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/rip>

OSPF:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/ospf>

BGP:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/bgp>

### 6.5.5 Sample Questions

1. Where do you find the dynamic routing configuration in the next-generation firewall's web interface?

- a. Device > Network > Virtual Router
- b. Network > Virtual Router
- c. Device > Network > Interfaces
- d. Network > Interfaces

2. The organization has three redundant connections to the internet, and all three of them are available.

What are two reasons why access to one set of IP addresses through the firewall consistently results in good performance while access to another set of IP addresses consistently results in poor performance? (Choose two.)

- a. The organization uses ECMP routing to the internet and selects which path to use based on the source IP address, and some IP addresses get routed through a slower ISP.
- b. The organization uses PBF and selects which route to use for the internet based on source IP address, and some IP addresses get routed through a slower ISP.
- c. The organization uses RIP, and some IP addresses get routed through a slower ISP.
- d. The organization uses BGP, and some IP addresses get routed through a slower ISP.
- e. The organization uses OSPF, and some IP addresses get routed through a slower ISP.

3. An organization has two links to the internet, one 100Mbps and the other 10Mbps. The firewall balances them using ECMP in the virtual router. Which load balancing ECMP setting does the organization need to use to optimize network resources?

- a. Balanced Round Robin
- b. Weighted Round Robin, with a weight of 10 for the fast connection and 100 for the slow one
- c. IP Hash
- d. Weighted Round Robin, with a weight of 100 for the fast connection and 10 for the slow one

4. Which Security Profile does not have a packet capture option?

- a. Antivirus
- b. Anti-Spyware
- c. Vulnerability Protection
- d. URL Filtering

5. On a PA-7080, which feature do you need to disable to use packet capture?

- a. NAT

- b. hardware offload
  - c. hardware acceleration
  - d. decryption
6. When must you use **tcpdump** to capture traffic on the next-generation firewall?
- a. on tunnel interface traffic
  - b. on data-plane interfaces
  - c. on packets on the management interface
  - d. on IPsec negotiation traffic
7. If users cannot access their Gmail accounts through the firewall, which log and filter do you use to troubleshoot the problem?
- a. Traffic, (app eq gmail)
  - b. Traffic, (app in gmail)
  - c. Configuration, (app eq gmail)
  - d. Configuration, (app in gmail)
8. You cannot access the firewall web interface. From the firewall CLI, how do you check to see if the web service is running?
- a. **ps -aux | grep appweb**
  - b. **ps -aux | match appweb**
  - c. **show system software status | grep appweb**
  - d. **show system software status | match appweb**
9. Which firewall log displays information about connection failures to an external LDAP authentication server?
- a. Traffic
  - b. System
  - c. User-ID
  - d. Authentication

## 6.6 Troubleshoot resource protections

### 6.6.1 Zone Protection profiles

Zone protection is always configured on the ingress interface. To protect against floods or scans from the internet, configure a Zone Protection profile on the zone containing the untrusted internet interface.

### 6.6.2 DoS protections

#### Resolution

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network resource, making it inaccessible to its intended users. Please read more about DoS in [What is a denial of service attack?](#)

This article gives some insight into how to troubleshoot a few situations due to firewall DoS attacks. This article assumes you are aware of DoS/ Zone Protection Profiles and checking resource usage:

## 1. Session Table Full

This can be seen in cases where the DoS traffic is allowed by the firewall policies. If the attacker can find open IPs and ports using **IP Sweep** or **Port Scanning** techniques, it can launch a flood attack. In the case of TCP, a response from the victim leads to a session getting installed on the firewall for 3600 seconds. Further on, more such SYN packets will lead to session table full, thereby causing legitimate traffic to be affected.

*Please note that in these cases ,the rate of flood attack may or may not be high.*

Allowing asymmetric bypass or disabling tcp-reject-non-syn can worsen the situation, as it will lead to any TCP packet to install a session on the firewall if the policy and routing allows it.

### Troubleshooting session table full

- In these kind of cases, the best way would be take a dump of the session table and skim through it. In most cases a particular source IP or a targeted IP will be standing out. Use command "show session all" for the same
- Check if the identified target IP and port , or the source of the traffic is valid and should be allowed through the firewall. If yes, can we restrict the firewall rules.
- Mostly in these cases mitigation is the best way. You should implement DoS Protection/ Zone Protection Profiles to mitigate these cases. SYN Cookie mode in SYN Flood Protection can be very useful in dealing with these situations, as it will prevent firewall from installing a session and will send a SYN/ACK packet to the attacker. Unless the attacker responds with a valid ACK, the session will not be established.
- The threshold of the SYN Flood Protection Mechanism should be tuned in to specific requirements after analysing the normal connection rate to the target IP.

## 2. Packet Buffer/ Packet Descriptors Full

This can be seen in DoS attacks with high packet/ data rate. Can be because of high rate of new connections per second or high packet rate on existing sessions. Even if the connections are getting denied, it would not prevent the buffer to be full as the packets have to be buffered and before sending to the dataplane for processing.

### How to troubleshoot:

- Check ACC tabs and try to use custom filters to see if there is a particular traffic that is exceptionally higher than the other traffic. However ACC tab does not provide good intel against ongoing attack. Reason being, that it takes its feed from the traffic summary, traffic log databases and appstats database.

- If the attack is going on via an ongoing session, it would not have generated a traffic log yet.
- If the attack comprises of new connections, ACC tab might not be able to show sessions which are anyway getting failed.

Some references to using ACC:

- [Tips & Tricks: How to Use the Application Command Center \(ACC\)](#)[FAQ ACC PAN-OS 7.0](#)
- [Video Tutorial: How to Use the Application Command Center \(ACC\) \(ACC\)](#)[FAQ ACC PAN-OS 7.0](#)
- Check for any live sessions with more data than usual. Use min-kb option in the session filter as under:

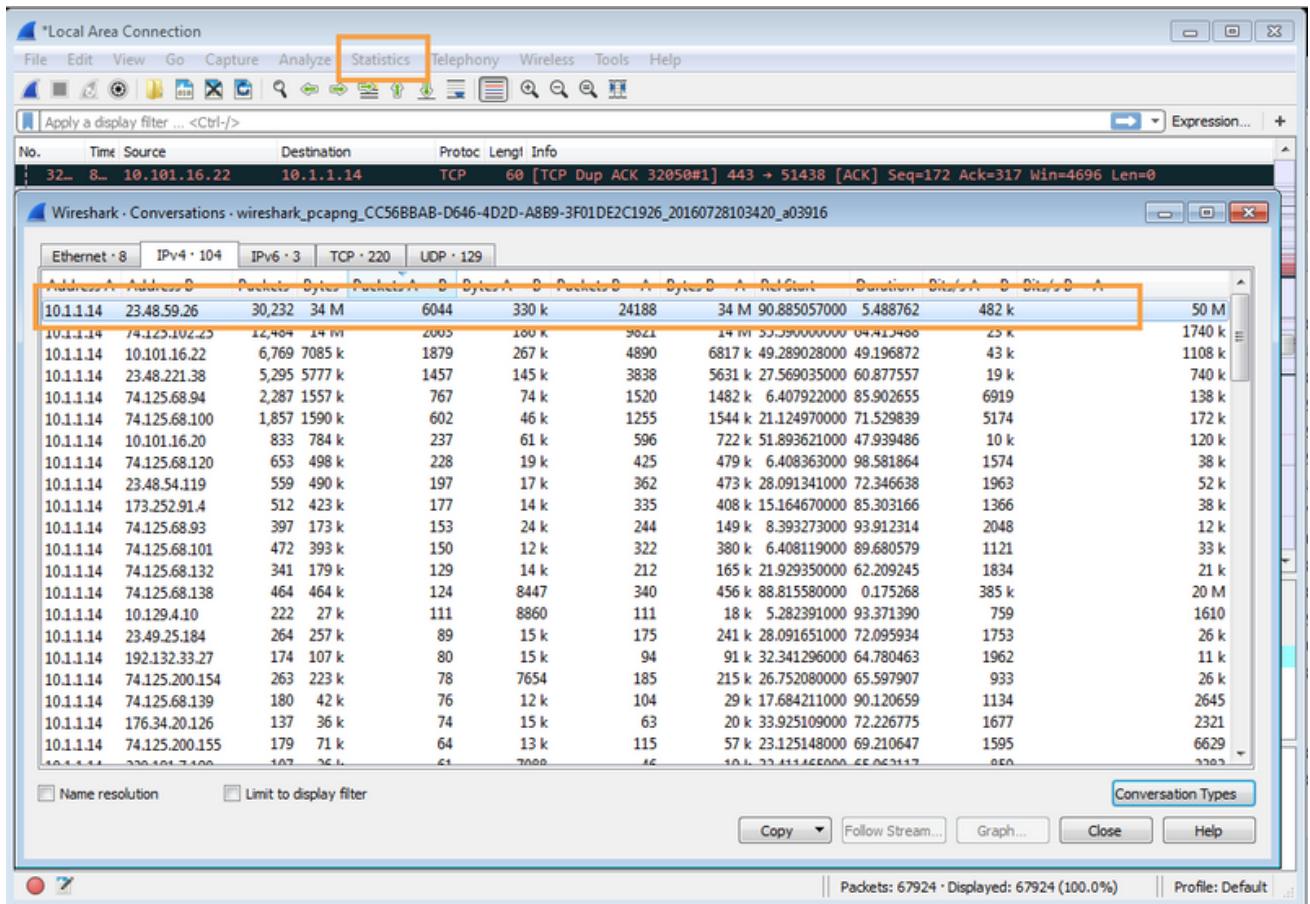
```
admin@PA-200> show session all filter min-kb 5000
```

```
-----
-
ID          Application      State    Type Flag  Src[Sport]/Zone/Proto
(translated IP[Port])                                Dst [Dport] /Zone
Vsys
(translated IP[Port])
-----
-
10216          pcoip           ACTIVE   FLOW    NS
10.1.1.11[50002]/Trust/17  (10.129.15.24[61158])
vsys1
10.101.41.211[4172]/Untrust  (10.101.41.211[4172])
```

The above is just an example, you can use the value of min-kb as anywhere between 1-1048576, i.e. almost upto 1G. This can provide an insight into sessions with top rate of traffic. Look for anything suspicious.

- You can use the following to find sessions which are overusing the buffer:  
[Identify Sessions That Use an Excessive Percentage of the Packet Buffer](#)
- Check the live traffic rate on interfaces and find out which interface is receiving excessive traffic. Use show system state browser for the same as highlighted in the following article: [How to Check Throughput of Interfaces](#).
  - Check for all relevant ports as per your configuration.
  - You should be focussing on the rx-bytes/s or rx-unicast/s or rx-multicast/s. This is the rate being shown in the second column when you enable tracking using 'Y' and 'U'.

- After you identify the port on which the attack traffic is being received, you will need to take a short packet dump of the traffic being received on that port.
    - It is recommended to do this on a connected switch by port mirroring the traffic as packet captures might be more resource intensive.
    - However if no other option is available, enable the captures on the Palo Alto Networks firewall with filter as ingress-interface as identified above and run the captures for 10-15 seconds.
  - Stop the captures and open with wireshark. Under Wireshark look under **Statistics -> Protocol Hierarchy or Conversations**. Check the conversation on IP layer, UDP layer, TCP layer and check for any traffic which is having a high packet count.
    - This can help identify and isolate the attacker (trusted or untrusted). Mostly for trusted source, you can track the affected host and take actions.
    - For an untrusted source, you can ask for help from your ISP to help prevent the source of attack.



### **6.6.3 Packet buffer protections**

Full packet buffers or packet descriptors can be caused by a high rate of new CPS or high packet rate on existing sessions. To troubleshoot this issue, verify the traffic using the ACC tabs. Use custom filters to analyze traffic that is exceptionally higher than other traffic.

### **6.6.4 References**

Zone Protection Recommendations (KB article):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVkCAC>

Zone Protection Profiles (KB article):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clm9CAC>

Zone Protection Profiles:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-de-fense/zone-protection-profiles>

Troubleshooting DOS Attacks (KB article):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClWLCA0>

Troubleshooting DOS Attacks (KB article):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClWLCA0>

Tips & Tricks: How to Use the Application Command Center (ACC):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClcvCAC>

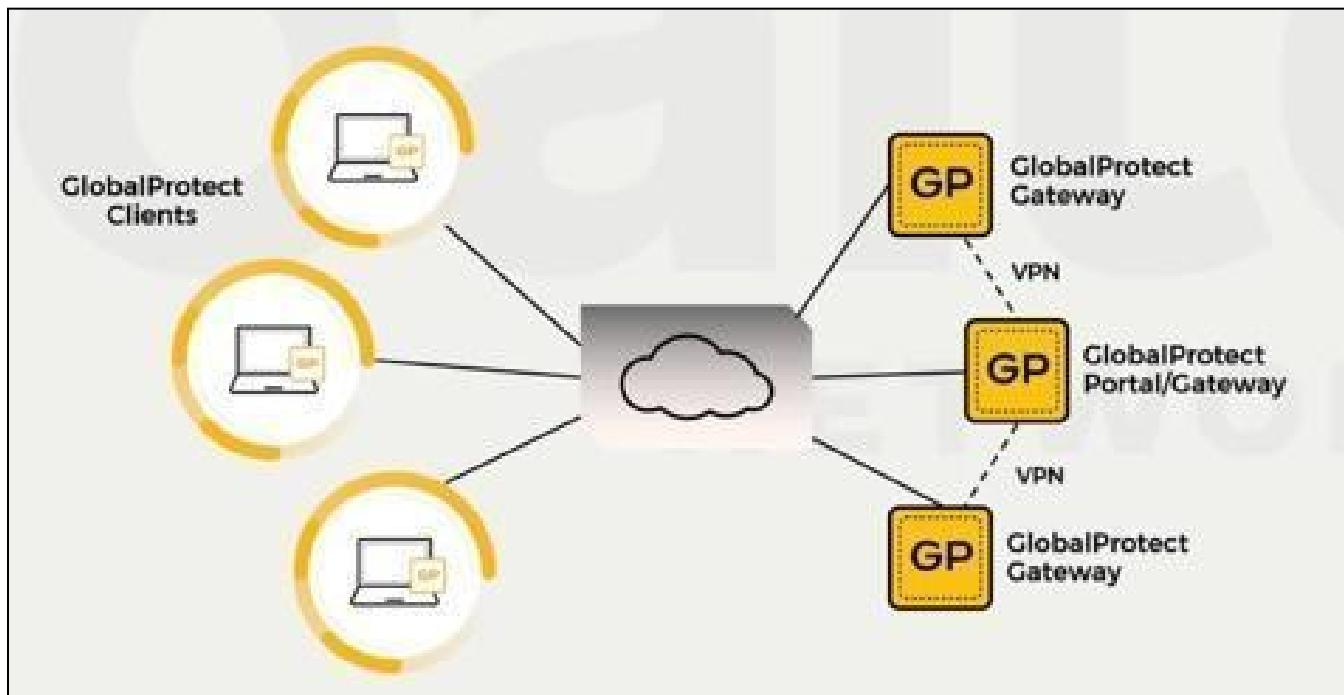
### **6.6.5 Sample Questions**

1. Applying zone protections to all interfaces, both internal and external, for protective measures across the entire environment is an example of \_\_\_\_\_.

- a. the Zero rust approach
- b. an alarm rate
- c. SYN cookies
- d. a maximum CPS rate

### **6.7 Troubleshoot GlobalProtect**

GlobalProtect has three major components: the GlobalProtect portal, GlobalProtect gateways, and GlobalProtect client software. These components provide the management functions for your GlobalProtect infrastructure.



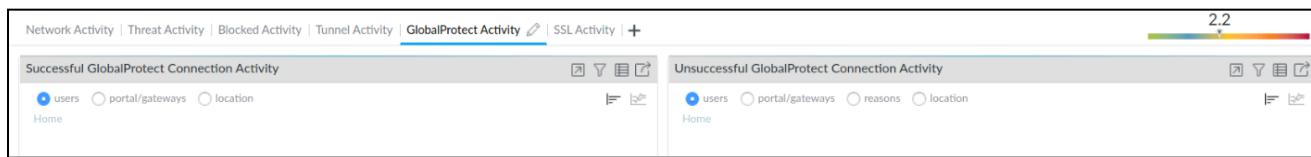
### 6.7.1 Portal and Gateway

#### *Portal*

The ACC displays a graphical view of user activity in your GlobalProtect deployment on the **GlobalProtect Activity** tab.

The following GlobalProtect charts are available:

- **Successful GlobalProtect Connection Activity:** Chart view of GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location.
- **Unsuccessful GlobalProtect Connection Activity:** Chart view of unsuccessful GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location. To help you identify and troubleshoot connection issues, you also can view the reasons chart or graph. For this chart, the ACC indicates the error, source user, public IP address, and other information to help you identify and quickly resolve the issue.
- **GlobalProtect Deployment Activity:** Chart view summary of your deployment. Use the toggle at the top of the chart to view the distribution of users by authentication method, GlobalProtect app version, and operating system version.



**GlobalProtect Activity** charts and graphs also are interactive and support similar drill-down functionality to other ACC charts and graphs.

The GlobalProtect Host Information widget under the **Network Activity** tab displays information about the state of the hosts on which the GlobalProtect agent is running; the host system is a GlobalProtect endpoint. This information is sourced from entries in the HIP match log that are generated when the data submitted by the GlobalProtect app 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.

### *GlobalProtect Log*

GlobalProtect logs display the following logs related to GlobalProtect:

- GlobalProtect system logs.  
GlobalProtect authentication event logs remain in MonitorLogsSystem; however, the Auth Method column of the GlobalProtect logs display the authentication method used for logins.
- LSVN/satellite events.
- GlobalProtect portal and gateway logs.
- Clientless VPN logs.

### *Gateway*

The PA-3020 in the co-location space (mentioned previously) also doubles as a GlobalProtect gateway (the Santa Clara Gateway). 10 additional gateways are deployed in Amazon Web Services (AWS) and the Microsoft Azure public cloud. The regions or POP locations where these AWS and Azure gateways are deployed are based on the distribution of employees across the globe.

- Santa Clara Gateway—Employees and contractors can authenticate to the Santa Clara Gateway (PA-3020 in the co-location space) using 2FA. This gateway requires users to provide their Active Directory credentials and their OTP. Because this gateway protects sensitive resources, it is configured as a manual-only gateway. As a result, users do not connect to this gateway automatically and must manually choose to connect to this gateway. For example, when users connect to AWS-Norcal, which is not a manual-only gateway, some sensitive internal resources are not accessible. The user must then manually switch to and authenticate with the Santa Clara Gateway to access these resources.  
In addition, the Santa Clara Gateway is configured as a Large Scale VPN (LSVPN) tunnel termination point for all satellite connections from gateways in AWS and Azure. The Santa Clara Gateway is also configured to set up an Internet Protocol Security (IPSec) tunnel to the IT firewall

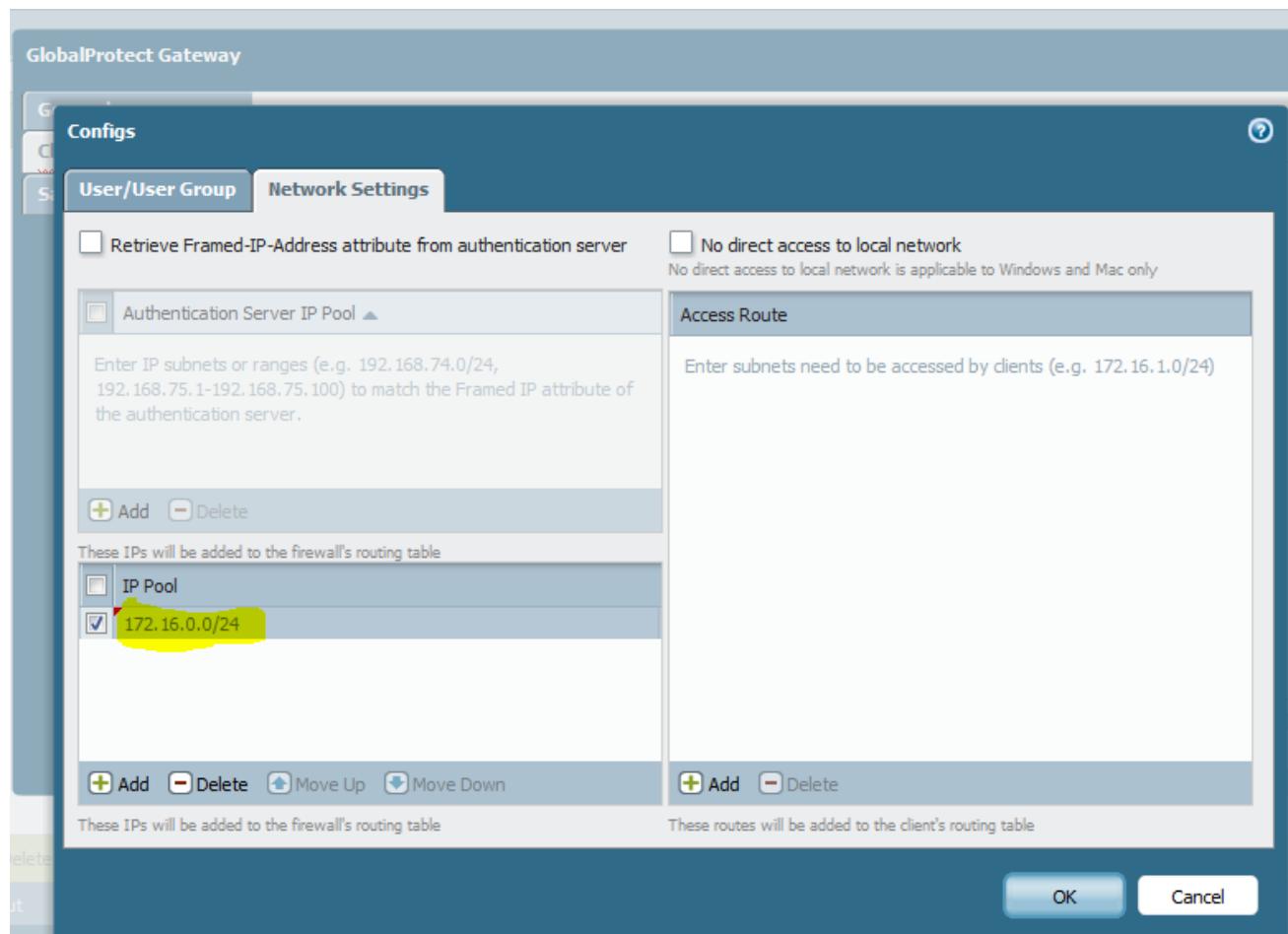
in corporate headquarters. This is the tunnel that provides access to resources in the corporate headquarters.

- Gateways in Amazon Web Services and Microsoft Azure—This gateway requires 2FA: a client certificate and Active Directory credentials. The GlobalProtect portal distributes the client certificate that is required to authenticate with these gateways using the GlobalProtect SCEP feature.  
These gateways in the public cloud also act as GlobalProtect satellites. They communicate with the GlobalProtect portal, download the satellite configuration, and establish a site-to-site tunnel with the Santa Clara Gateway. GlobalProtect satellites initially authenticate using serial number, and subsequently authenticate using certificates.
- Gateways Inside Corporate Headquarters—Within the corporate headquarters, three firewalls function as GlobalProtect gateways. These are internal gateways and do not require endpoints to set up a tunnel. Users authenticate to these gateways using their Active Directory credentials. These internal gateways use GlobalProtect to identify the User-ID and to collect Host Information Profile (HIP) from the endpoints.

## 6.7.2 Access to resources

### *Resolution*

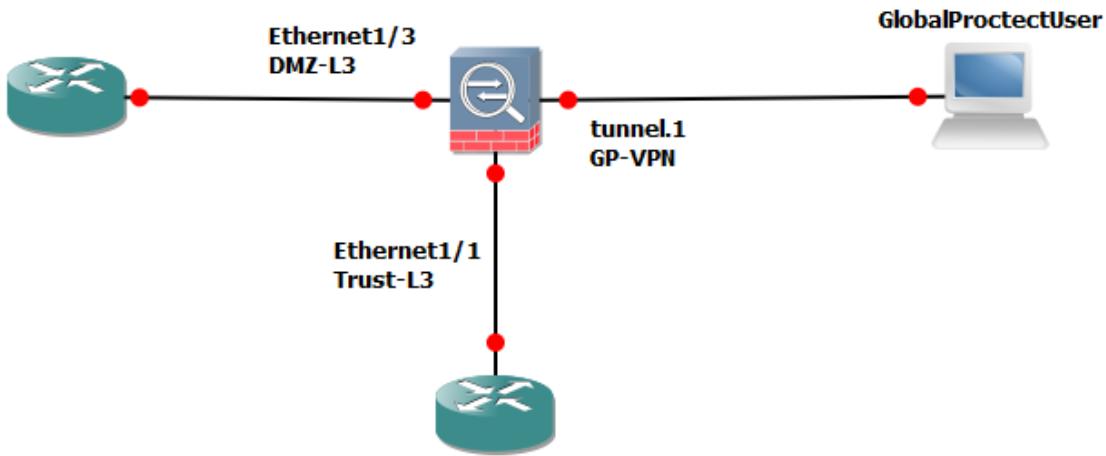
Sometime even if the configuration is correct, GlobalProtect users are unable to access internal resources. This situation may result because the subnet assigned to GlobalProtect is used somewhere in the network or there is a routing issue.



A workaround is to put the tunnel interface used in the GlobalProtect configuration in a different zone (GP-VPN) and do a source NAT for desired traffic. Make sure you have a security policy to allow the traffic.

Following is the topology:

GlobalProtect users are in GP-VPN zone, Servers are in DMZ-L3 zone and internal host are in Trust-L3 zone.



If you are trying to access the resources in the DMZ-L3 zone, then do a source NAT from GP-VPN to DMZ-L3

	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
1	GP-DMZ	none	GP-VPN	DMZ-L3	any	any	any	any	dynamic-ip-and-port ethernet1/3 10.50.242.57/24
2	GP-Trust-L3	none	GP-VPN	Trust-L3	any	any	any	any	dynamic-ip-and-port ethernet1/1 10.50.240.57/24

Security Policy:

	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action
1	GP-VPN To DMZ-L3 or Trust-L3	none	universal	GP-VPN	any	any	any	DMZ-L3 Trust-L3	any	any	any	any	Allow

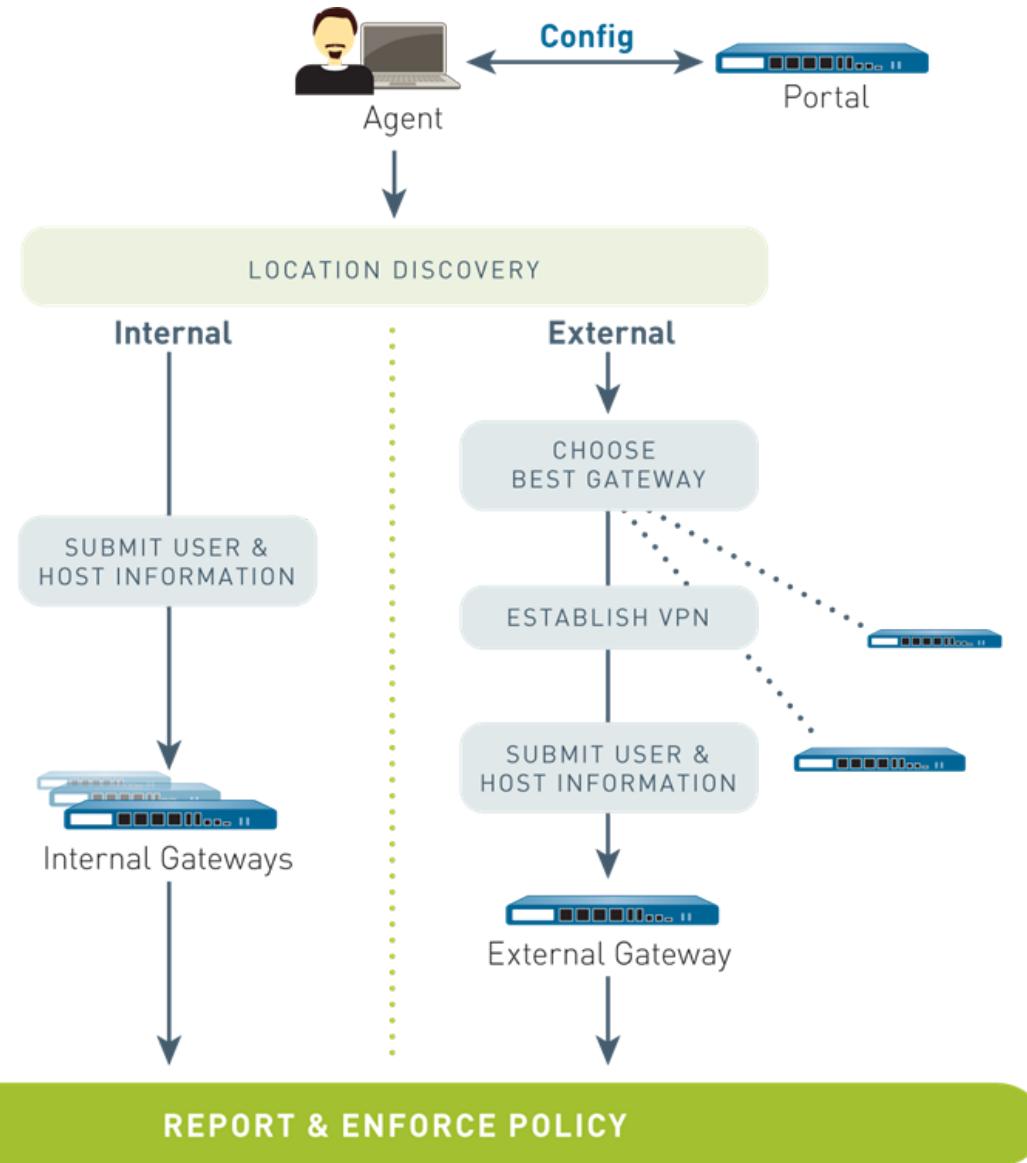
### 6.7.3 GlobalProtect client

The GlobalProtect client software runs on end user systems and enables access to your network resources via the GlobalProtect portals and gateways you have deployed. There are two types of GlobalProtect clients:

- **The GlobalProtect Agent**—Runs on Windows and Mac OS systems and is deployed from the GlobalProtect portal. You configure the behavior of the agent—for example, which tabs the users can see—in the client configuration(s) you define on the portal. See [Define the GlobalProtect Agent Configurations](#), [Customize the GlobalProtect Agent](#), and [Deploy the GlobalProtect Agent Software](#) for details.
- **The GlobalProtect App**—Runs on iOS, Android, Windows UWP, and Chromebook devices. Users must obtain the GlobalProtect app from the Apple App Store (for iOS), Google Play (for Android), Microsoft Store (for Windows UWP), or Chrome Web Store (for Chromebook).

See [What Client OS Versions are Supported with GlobalProtect?](#) for more details.

The following diagram illustrates how the GlobalProtect portals, gateways, and agents/apps work together to enable secure access for all your users, regardless of what devices they are using or where they are located.



#### 6.7.4 References:

GlobalProtect Gateways:

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-gateways/globalprotect-gateways-overview>

Common Issues with Global Protect:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIYGCA0>

GlobalProtect Users and Internal Resources:

<https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000ClAB>

GlobalProtect Remote User Security:

[https://beacon.paloaltonetworks.com/student/path/774588-globalprotect-remote-user-security?sid=3574388&sid\\_i=0](https://beacon.paloaltonetworks.com/student/path/774588-globalprotect-remote-user-security?sid=3574388&sid_i=0)

GlobalProtect Resource List on Configuring and Troubleshooting:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfXCAS>

Troubleshooting GlobalProtect:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClkBCAS>

GlobalProtect Client:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/globalprotect/device-globalprotect-client>

Use the Application Command Center:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-application-command-center>

D-TW - GlobalProtect Troubleshooting Tips:

<https://live.paloaltonetworks.com/t5/blogs/dotw-globalprotect-troubleshooting-tips/ba-p/383911>

## 6.8 Troubleshoot Policies

### 6.8.1 NAT policies

FIELD	DESCRIPTION
Test Configuration	
Select Test	Select the policy match test to execute.
(Panorama only) Select device	Select device/VSYS to specify which devices and virtual systems for which to test the policy functionality. Admin and device group & Template users are presented with the devices and virtual systems based on their access domain. Additionally, you can select the Panorama management server as a device.
(Panorama only) Selected Devices	Lists the devices and virtual systems selected for testing.
From	Enter the zone where the traffic originated.

To	Select the destination zone of the traffic.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Source Port	Enter the specific port the traffic originated from.
Destination Port	Enter the specific destination port for which traffic is intended.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
To Interface	Enter the destination interface on the device for which the traffic is intended.
HA Device ID	<p>Enter the ID of the HA device:</p> <ul style="list-style-type: none"> <li>• 0—Primary HA peer</li> <li>• 1—Secondary HA peer</li> </ul>
Results	<p>Select to view the Result Details of the executed test.</p> <p>(Panorama only) When executing the test for multiple managed devices, the Results display the following information for each device tested:</p> <ul style="list-style-type: none"> <li>• Device Group—Name of the device group to which the firewall that is processing traffic belongs.</li> <li>• Firewall—Name of the firewall that is processing traffic</li> <li>• Status—Indicates the status of the test: Success or Failure.</li> <li>• Result—Displays the test result. If the test could not be performed, one of the following is displayed: <ul style="list-style-type: none"> <li>○ N/A—Test was not applicable to the device.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ Device not connected—Device connection was dropped.</li> <li>○ Shared policy disabled on device—The Panorama settings on the device do not allow for the policy to be pushed from Panorama.</li> </ul>
--	---

## 6.8.2 Security policies

Refer to the security policies below.

- On the Windows or macOS machine, use **ipconfig /all** or **ifconfig** to find the private IP address of the local machine that will be used to test the Security policy.
- In the source address field, enter the IP address of the test machine.
- Place the Security policy rule at the top.
- Leave everything else set to any. If possible, also remove the Security Profile.
- Before committing, be aware of any security issues that might occur. The Security rule will be open and only contains a source IP address to prevent the rule from being completely open.
- Clear the session for the test user by using the following command: **>clear session all filter source <IP address of test machine goes here>**
- Initiate the test, and see if you are able to reach the destination.
- If you are able to reach the destination, then clear the session again. This time, add the destination IP address (if known), and test again after doing a commit.
- Add the source zone and repeat.
- Add the destination zone and repeat.
- Keep adding additional fields, such as applications, source user, service ports, and URL filtering, until the Security policy stops working. If security permits, add the Security Profile at the very end.
- Once you determine which field is causing the issue, begin troubleshooting using advanced troubleshooting debug commands (**flow basic**, **appid basic**, **ctd basic**, **url\_trie**, **proxy all**, **ssl all**, etc.).

Please be aware that using the advanced debug commands can be very resource-intensive. If used for too long or incorrectly, they can lead to packet loss and device reboot. At this stage, reboot will cause a complete outage unless there is a HA pair firewall to take over. If advanced debug commands are needed, please call Type allocation code (TAC).

### 6.8.3 Decryption policies

A new Decryption Log and new Application Command Center (ACC) widgets provide enhanced visibility into TLS traffic, which enables you to troubleshoot and monitor decryption issues and identify traffic that uses weak algorithms and protocols. Use the new ACC widgets to identify traffic for which decryption causes issues and then use the new Decryption Log to drill down into details and gain context about that traffic.

The new **ACSSL Activity** widgets show you details about both successful and unsuccessful SSL Decryption activity in your network. They identify traffic—applications and Server Name Identifications (SNIs)—that cause decryption issues and that use weak ciphers and algorithms. Use that knowledge to identify misconfigured Decryption policies and profiles and to make informed decisions about what traffic to allow and what traffic to block. You can view SSL/TLS traffic in the ACC in multiple ways:

- **Traffic Activity Widget**—Shows SSL/TLS activity compared to non-SSL/TLS activity by total number of sessions or bytes.
- **Successful TLS Version Activity Widget**—Shows successful TLS connections by TLS version and application or SNI. This widget helps you understand how much risk you are taking on by allowing weaker TLS protocol versions. Identifying applications and SNIs that use weak protocols enables you to evaluate each one and decide whether you need to allow access to it for business reasons. If you don't need the application for business purposes, you may want to block the traffic instead of allowing it. Click an application or an SNI to drill down and see detailed information.
- **Decryption Failure Reasons Widget**—Shows the reasons for decryption failures, such as certificate or protocol issues, by SNI. Use this information to detect problems caused by Decryption policy or profile misconfiguration or by traffic that uses weak protocols or algorithms. Click a failure reason to drill down and isolate the number of sessions per SNI or click an SNI to see the failures for that SNI.
- **SSL/TLS Traffic Widget**—Shows the amount of decrypted and non-decrypted traffic by sessions or bytes. Traffic that was not decrypted may be excepted from decryption by policy, policy misconfiguration, or by being on the Decryption Exclusion List (**Device Certificate Management** **SSL Decryption Exclusion**).
- **Successful Key Exchange Activity**—Shows successful key exchange activity per algorithm, by application or by SNI. Click a key exchange algorithm to see the activity for just that algorithm or click an application or SNI to view the key exchange activity for that application or SNI.

The new Decryption Log (**Monitor > Logs > Decryption**) provides comprehensive information about sessions that match a Decryption policy. You can view log information such as application, SNI, Decryption Policy Name, error index, TLS version, key exchange version, encryption algorithm, certificate key types, and many other characteristics by selecting which columns to display:

	RECEIVE TIME	APPLICATION	DESTINATION ADDRESS	RULE	POLICY NAME	ROOT STATUS	ERROR INDEX	ERROR	SOURCE ADDRESS	SUBJECT COMMON NAME	SERVER NAME IDENTIFICATION	CERTIFICATE END DATE	ISSUER COMMON NAME	ROOT COMMON NAME	SESSION ID	PROXY TYPE
🕒	02/07/11:44:54	web-browsing	51.143.106.177	web-browsing	web-decryption	trusted	None		172.23.11.11	settings-win.data.microsoft.com		2020/05/21 00:56:44	Microsoft Secure Server CA 2011	DigiCert SHA2 High Assurance Server CA	111377	Forward
🕒	02/07/11:41:24	dropbox-base	52.203.155.34	Web app moderate risk	web-decryption	trusted	None		172.23.11.11	*.dropbox.com	di-debug.dropbox.com	2020/11/05 12:00:00	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	111377	Forward
🕒	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:07	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:41:02	ssl	162.125.7.3	web-browsing	web-decryption	uninspected	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x00. Supported decrypt profile version bitmask: 0x00.	172.23.11.11		client.dropbox.com					
🕒	02/07/11:38:44	ssl	162.125.7.3	web-browsing	web-decryption	trusted	None		172.23.11.11	*.dropbox.com		2020/11/05 12:00:00	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	111377	Forward
🕒	02/07/11:38:44	ssl	162.125.7.3	web-browsing	web-decryption	trusted	None		172.23.11.11	*.dropbox.com		2020/11/05 12:00:00	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	111377	Forward

Click the magnifying glass icon (🔍) to see the Detailed Log View of a session:

### Detailed Log View

General		Source				Destination								
Session ID	111408	Source User	Source			Destination User	Destination							
Application	dropbox-base	172.23.11.11	Country	172.16.0.0-172.31.255.255			Destination	52.203.155.34						
Rule	Web app moderate risk	Port	50890			Country	United States							
Policy Name	web-decryption	Zone	inZone			Port	443							
Proxy Type	Forward	Interface	ethernet1/4			Zone	outZone							
Generated Time	2020/02/07 11:41:24	Certificate Details				Interface	ethernet1/1							
Receive Time	2020/02/07 11:41:24					Handshake Details								
PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME	
	2020/02/07 11:41:09	url	dropbox-base	alert	Web app moder... risk	ee9bb...		informa...	online-storag...	online-storag...		dl-deb...		
	2020/02/07 11:41:09	url	dropbox-base	alert	Web app moder... risk	ee9bb...		informa...	online-storag...	online-storag...		dl-deb...		

Close

After using the ACC to identify decryption issues, filter the Decryption Log to see detailed information about issues. [Common troubleshooting tasks](#) include:

- Filtering for weak cipher suites to identify SNIs and applications that use older, less secure protocols and algorithms. For example, the filter `(tls_version leq TLS1.1)` shows you all traffic that uses TLS versions lower than TLSv1.2. You can then make an informed decision about how you want to handle traffic that uses weaker TLS versions.

In the same way, you can filter for weak key exchange and encryption algorithms. For example, the filter `(tls_keyxchg eq RSA)` identifies all traffic that uses the RSA key exchange algorithm.

The filter `(tls_auth eq MD5)` identifies all traffic that uses the MD5 authentication algorithm.

The filter `(tls_enc eq 3DES_EDE_CBC)` identifies the traffic that uses that encryption algorithm.

- Filtering for expired certificates. The filter `(error eq 'Expired server certificate')` identifies traffic that generates an “Expired server certificate” error. You can check the results at [SSL Labs](#) and see the validity dates of the certificate.  
You can also filter for certificates that will expire soon. For example, to filter for certificates that expire after July 1st, 2020, use the filter `(notafter leq '2020/7/01 12:00:00')`.
- Filtering for revoked certificates (you must first enable [Certificate Revocation Checking](#) to do this).  
Use the filter `(error eq 'OCSP/CRL check: certificate revoked')`

There are many ways to filter the extensive information in the Decryption Logs to drill down into the details of any issue or potential issue.

#### 6.8.4 Authentication policies

Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, [Voice](#), [SMS](#), [Push](#), or [One-time Password \(OTP\) authentication](#). For the first factor, users authenticate through a Authentication Portal web form. For any additional factors, users authenticate through a [Multi-Factor Authentication](#) (MFA) login page.

After the user authenticates for all factors, the firewall evaluates [Security Policy](#) to determine whether to allow access to the service or application.

To reduce the frequency of authentication challenges that interrupt the user workflow, you can specify a timeout period during which a user authenticates only for initial access to services and applications, not for

subsequent access. Authentication policy integrates with Authentication Portal to record the timestamps used to evaluate the timeout and to enable user-based policies and reports.

Based on user information that the firewall collects during authentication, User-ID creates a new IP address-to-username mapping or updates the existing mapping for that user (if the mapping information has changed). The firewall generates User-ID logs to record the additions and updates. The firewall also generates an Authentication log for each request that matches an Authentication rule. If you favor centralized monitoring, you can configure reports based on User-ID or Authentication logs and forward the logs to Panorama or external services as you would for any other log types.

## 6.8.5 References

NAT Policy Match:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-troubleshooting/nat-policy-match.html#ida1834369-2df1-4714-810f-307b8f3a7f3e>

Enhances SSL Decryption Troubleshooting:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption>

Authentication policy:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/authentication-policy>

Troubleshoot Authentication issues:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/troubleshoot-authentication-issues.html#id168e72b8-9cca-45c3-8f33-b5b7eb83aa64>

## 6.9 Troubleshoot HA functions

### 6.9.1 Monitor

Troubleshooting tools provide enhanced visibility into TLS traffic so you can monitor your decryption deployment. The tools enable you to diagnose and resolve decryption issues quickly and easily, tighten weaknesses in your decryption deployment, and fix decryption issues to improve your security posture. For example, you can:

- Identify traffic that causes decryption failures by Service Name Identification (SNI) and application.
- Identify traffic that uses weak protocols and algorithms.
- Examine successful and unsuccessful decryption activity in the network.
- View detailed information about individual sessions.
- Profile decryption usage and patterns.

- Monitor detailed decryption statistics and information about adoption, failures, versions, algorithms, etc.

The following tools provide full visibility into the TLS handshake and can help you troubleshoot and monitor your decryption deployment:

- **ACC SSL Activity:** The five ACC widgets on this tab (introduced in PAN-OS 10.0) provide details about successful and unsuccessful decryption activity in your network, including decryption failures, TLS versions, key exchanges, and the amount and type of decrypted and undecrypted traffic.
- **Monitor Logs Decryption:** The Decryption log (introduced in PAN-OS 10.0) provides comprehensive information about individual sessions that match a decryption policy and about GlobalProtect sessions when you enable Decryption logging in the GlobalProtect portal or GlobalProtect gateway configuration. Select which columns to display to view information such as application, SNI, decryption policy name, error index, TLS version, key exchange version, encryption algorithm, certificate key types, and many other characteristics. Filter the information in columns to identify traffic that uses particular TLS versions and algorithms, particular errors, or any other characteristics you want to investigate. By default, Decryption policies log only unsuccessful TLS handshakes. Depending on the available log storage, you can configure Decryption policies to log successful TLS handshakes as well.
- **Local Decryption Exclusion Cache:** There are two constructs for sites that break decryption for technical reasons and therefore need to be excluded from decryption: the SSL Decryption Exclusion List and the Local Decryption Exclusion Cache. The SSL Decryption Exclusion List contains the sites that Palo Alto Networks has identified that break decryption technically. Content updates keep the list up to date, and you can add sites to the list manually. The Local Decryption Exclusion Cache automatically adds sites that local users encounter that break decryption for technical reasons and excludes them from decryption, providing that the Decryption Profile applied to the traffic allows unsupported modes. (If unsupported modes are blocked, then the traffic is blocked instead of added to the local cache.)
- **Custom Report Templates for Decryption:** You can create custom reports ([Monitor > Manage Custom Reports](#)) using four predefined templates that summarize decryption activity.

The general troubleshooting methodology is to use the ACC widgets to identify traffic that causes decryption issues and then use the Decryption Log and custom report templates to drill down into details. The tools allow you to gain context about that traffic, which enables you to diagnose issues much more accurately and easily than in the past. Understanding decryption issues and their causes enables you to select the appropriate way to fix each issue, such as:

- Modifying decryption policy rules (a policy rule defines traffic that the rule affects, the action taken on that traffic, log settings, and the Decryption Profile applied to the traffic)
- Modifying Decryption Profiles (profiles define acceptable protocols and algorithms for the traffic, as well as failure checks, unsupported mode checks for items such as unsupported ciphers and versions, certificate checks, etc.)

- Adding sites that break decryption for technical reasons to the SSL Decryption Exclusion List
- Evaluating security decisions about which sites your employees, customers, and partners really need to access and which sites you can block when sites use weak decryption protocols or algorithms

The goals should be to decrypt all the traffic you can decrypt (a decryption best practice) and to properly handle traffic that you don't decrypt.

When you upgrade to PAN-OS 10.0, the device takes 1 percent of the log space and allocates it to Decryption logs. Step 3 in Configure Decryption Logging shows you how to modify the log space allocation to provide more space for Decryption logs.

If you downgrade from PAN-OS 10.2 or later to PAN-OS 9.1 or earlier, the features introduced in PAN-OS 10.2 (Decryption Log, SSL Activity widgets in the ACC, and custom report decryption templates) are removed from the UI. References to Decryption logs are also removed from Log Forwarding profiles. In addition, the Local Decryption Exclusion Cache is only viewable using the CLI in PAN-OS 9.1 and earlier (PAN-OS 10.2 added the local cache to the UI).

### **6.9.2 Failover triggers**

When a failure occurs on the active Panorama and the passive Panorama begins managing the firewalls, the event is called a failover. A failover is triggered when a monitored metric on the active Panorama fails. This failure transitions the state on the primary Panorama from active-primary to passive-primary, and the secondary Panorama becomes active-secondary.

The conditions that trigger a failover are:

- The Panorama peers cannot communicate with each other, and the active peer does not respond to health and status polls; the metric used is HA heartbeat polling and Hello messages.

When the Panorama peers cannot communicate with each other, the active peer monitors whether the peers are still connected before a failover is triggered. This check helps in avoiding a failover and causing a split-brain scenario, where both Panorama peers are in an active state.

- One or more of the destinations (IP addresses) specified on the active peer cannot be reached; the metric used is HA path monitoring.

In addition to the failover triggers listed above, a failover also occurs when the administrator places the Panorama peer in a suspended state or when preemption occurs. Preemption is a preference for the primary Panorama to resume the active role after recovering from a failure (or user-initiated suspension). By default, preemption is enabled. When the primary Panorama recovers from a failure and becomes available, the secondary Panorama relinquishes control and returns to the passive state. When preemption occurs, the event is logged in the System log.

If you are logging to an Network file system (NFS) datastore, do not disable preemption because it allows the primary peer (that is mounted to the NFS) to resume the active role and write to the NFS datastore. For all other deployments, preemption is only required if you want to make sure that a specific Panorama is the preferred active peer.

# Appendix A: Sample Questions with Answers

## Domain 1

### *Domain 1.1.8*

1. Which component of the integrated Palo Alto Networks security solution limits network-attached workstation access to a corporate mainframe?
  - a. threat intelligence cloud
  - b. advanced endpoint protection
  - c. **next-generation firewall**
  - d. tunnel inspection
  
2. Which Palo Alto Networks product is designed primarily to provide threat context with deeper information about attacks?
  - a. Prisma Cloud
  - b. WildFire
  - c. **AutoFocus**
  - d. Threat Prevention
  
3. Which Palo Alto Networks product is designed primarily to provide normalization of threat intelligence feeds with the potential for automated response?
  - a. **MineMeld**
  - b. WildFire
  - c. AutoFocus
  - d. Threat Prevention
  
4. Which Palo Alto Networks product is designed primarily to prevent endpoints from successfully running malware programs?
  - a. GlobalProtect
  - b. Cortex XDR - Analytics
  - c. **Cortex XDR**
  - d. Prisma Cloud
  
5. The Palo Alto Networks Cortex Data Lake can accept logging data from which two products?  
(Choose two.)
  - a. **Cortex XDR**
  - b. **NGFWs**
  - c. Prisma SaaS
  - d. MineMeld
  - e. AutoFocus
  
6. Which Palo Alto Networks product is a cloud-based storage service designed to hold log information?

- a. Prisma Cloud
  - b. Cortex XDR
  - c. NGFW
  - d. **Cortex Data Lake**
7. Which product is an example of an application designed to analyze Cortex Data Lake information?
- a. **Cortex XDR – Analytics**
  - b. Prisma Cloud
  - c. Cortex XDR – Automated Response
  - d. AutoFocus
8. A Heatmap provides an adoption rate for which three features? (Choose three.)
- a. **WildFire**
  - b. Traps
  - c. **File Blocking**
  - d. **User-ID**
  - e. Authentication profiles
9. What are three Best Practice Assessment (BPA) tool class summaries? (Choose three.)
- a. **Technical**
  - b. **Operational**
  - c. **Management**
  - d. Risk
  - e. Contingency
10. Which two security features normally do not achieve an adoption rate of 100 percent? (Choose two.)
- a. **URL Filtering**
  - b. App-ID
  - c. Logging
  - d. **DNS Sinkhole**
11. Which type of file is used to generate the Heatmap report and the BPA report?
- a. **Technical Support**
  - b. Configuration
  - c. Statistics
  - d. XML
12. What are two components of the BPA tool? (Choose two.)
- a. **Adoption Heatmap**
  - b. **BPA**
  - c. XML
  - d. Security policy

### *Domain 1.2.12*

1. Virtual wire does not switch VLAN \_\_\_\_\_.
  - a. addresses
  - b. subnets
  - c. **tags**
  - d. wires
  
2. 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 \_\_\_\_\_.
  - a. service routes
  - b. static routes
  - c. virtual systems
  - d. **subinterface**

### *Domain 1.3.8*

1. With SSH Proxy, PAN-OS firewalls can be configured to detect \_\_\_\_\_. Select all that apply.
  - a. **SSH traffic**
  - b. **SSH port forwarding**
  - c. **Hidden applications inside a SSH tunnel**
  - d. **Breached security policies**
  
2. A Decryption policy rule allows administrators to:
  - a. Require certificates
  - b. **Inspect inside encrypted sessions**
  - c. Re-encrypt firewall settings
  - d. Decrypt VPN traffic
  
3. Select a use case for a Decryption profile to block and control various aspects of the decrypted traffic.
  - a. Terminate idle encrypted user-sessions after 300 seconds
  - b. Search for admin users after business hours
  - c. Retrieve a list of user groups from Microsoft Active Directory using TLS
  - d. **Terminate sessions using unsupported versions and unsupported algorithms**

### *Domain 1.4.8*

1. PAN-OS firewalls support which three directory services? (Choose three.)
  - a. **Microsoft Active Directory (AD)**
  - b. **Novell eDirectory**

- c. Sun ONE Directory Server
  - d. Apache directory
2. When you enable a user- or group-based policy, which network security issues could occur if an administrator enables User-ID on an external untrusted zone?
- a. You may disclose internal IP address spacing.
  - b. Traffic will be treated as intrazone traffic and by default will be allowed.
  - c. Virus/Phishing attacks
  - d. You may allow an attacker to gain unauthorized access to protected services and applications.**
3. User-ID maps users to which type of information?
- a. MAC addresses
  - b. IP addresses**
  - c. IP address and port number
  - d. port numbers
4. User-ID uses which protocol to map between user identities and groups?
- a. NetBIOS
  - b. LDAP**
  - c. syslog
  - d. HTTPS
5. Which format do you use when calling the API to inform the firewall of a new IP-address-to-username mapping?
- a. XML**
  - b. JSON
  - c. YAML
  - d. Base64
6. What must you configure on the firewall before it can read User-ID-to-IP-address mapping tables from external sources?
- a. Group Mapping Settings
  - b. Server Monitoring
  - c. Captive Portal
  - d. User-ID Agents**
7. For an external device to consume a local User-ID-to-IP-address mapping table, which data is used for authentication between the devices?
- a. the source device's Data Redistribution Collector Name and Pre-Shared Key**
  - b. the User-ID agent's Server Monitor Account information

- c. the Administrator's account information on the source device with the User-ID role set
  - d. certificates added to the User-ID agent configuration
8. Which product or service can read User-ID-to-IP-address mapping tables?
- a. Cortex XDR
  - b. Panorama Log Collector**
  - c. AutoFocus
  - d. Prisma Cloud

#### *Domain 1.5.5*

1. Which firewall configuration object is used to specify more than one external authentication source for a user's login attempt?
- a. Multiple Server Profiles configured to failover
  - b. Authentication Sequence**
  - c. Local User account set to failover
  - d. Account Sequence
2. Which object links the Captive Portal method with an Authentication profile when multi-factor authentication is configured?
- a. Multi-Factor Authentication server profile
  - b. Authentication policy rule
  - c. Authentication Sequence
  - d. Authentication Enforcement object**
3. Which four firewall server profiles can provide first factor authentication for multi-factor authentication configurations? (Choose four.)
- a. HTTP
  - b. Okta
  - c. PingID
  - d. Kerberos**
  - e. RADIUS**
  - f. SAML**
  - g. LDAP**
  - h. RSA SecurID Access
4. What are the two purposes of multi-factor authentication? (Choose two.)
- a. reduce the value of stolen passwords**
  - b. simplify password resets**
  - c. reduce and prevent password sharing**
  - d. ensure strong passwords

- e. provide single sign-on functionality
5. Which MFA factor is *not* supported by the next-generation firewall?
- a. voice
  - b. push
  - c. SMS
  - d. S/Key**
6. What is the meaning of setting the source user to known-user in an Authentication policy rule?
- a. The user identity is known (i.e., linked to an IP address), but the resource is sensitive enough to require additional authentication.**
  - b. The next-generation firewall will demand user authentication, and only then will the resource be available.
  - c. The source device is a known device that is used only by a single person.
  - d. The firewall attempts to match only users defined in the firewall's local user database.
7. What are the two Captive Portal modes? (Choose two.)
- a. proxy
  - b. transparent**
  - c. web form
  - d. certificate
  - e. redirect**
8. Which action is not required when multi-factor authentication and a SAML Identity Provider (IdP) are configured?
- a. Create an Authentication policy rule.
  - b. Configure NTLM settings.**
  - c. Create an Authentication object.
  - d. Create an Authentication Profile.
9. An Authentication policy rule has a HIP profile. Where are the users being authenticated coming from?
- a. internal devices, such as Linux workstations
  - b. external devices belonging to customers of the organization
  - c. internal servers running UNIX (e.g., Solaris, HPUX, AIX, etc.)
  - d. GlobalProtect connections through the internet**

### *Domain 1.6.2*

1. On a PA-7000 Series firewall, which management function runs on a separate, dedicated card?
- a. configuration management
  - b. logging**
  - c. reporting

- d. management web service
2. Do some next-generation firewall models use FPGA chips?
- a. no, never
  - b. yes, on the data plane, but only on higher-end models**
  - c. yes, on the management plane, but only on higher-end models
  - d. yes, on both the data plane and the management plane, but only on higher-end models
3. Which function resides on the management plane?
- a. App-ID matching
  - b. route lookup
  - c. policy match
  - d. logging**

## Domain 2

### *Domain 2.2.9*

1. Which action specifies that Security profiles are relevant in a policy rule?
- a. deny
  - b. drop
  - c. reset
  - d. allow**
2. Are files quarantined while WildFire checks if they are malware or legitimate?
- a. yes, always
  - b. no, never**
  - c. by default, yes, but you can change the settings
  - d. by default, no, but you can change the settings
3. Which feature of the Next-Generation Firewall allows you to block websites that are not business-appropriate?
- a. App-ID
  - b. File Blocking
  - c. Exploit Protection
  - d. URL Filtering**
4. Which credential phishing prevention action allows users to choose to submit credentials to a site anyway?
- a. alert
  - b. allow
  - c. block
  - d. continue**

5. Which user credential detection method works if multiple users share the same client IP address (e.g., because of dynamic address translation done by a device on the internal side of the firewall)?

- a. IP-to-user mapping
- b. group mapping
- c. **domain credential filter**
- d. IP-and-port-to-user mapping

6. Which type of user credential detection must be used by a firewall administrator who wants to enable credential phishing prevention that blocks an attempt by a user to enter the organization's user ID and password?

- a. IP-to-user mapping
- b. **domain credential filter**
- c. group mapping
- d. Citrix mapping

7. Which profile do you use for DLP based on file content?

- a. Anti-Spyware
- b. Vulnerability Protection
- c. URL Filtering
- d. WildFire Analysis
- e. **Data Filtering**

8. Which profile do you use to monitor DNS resolution lookups for sites associated with threat activity?

- a. Antivirus
- b. **Anti-Spyware**
- c. Vulnerability Protection
- d. File Blocking
- e. Data Filtering

9. Which profile do you use to analyze files for zero-day malware?

- a. Anti-Spyware
- b. URL Filtering
- c. File Blocking
- c. **WildFire Analysis**
- d. Data Filtering

10. Which profile do you use to examine browsing traffic for appropriate browsing policy enforcement?

- a. Antivirus
- b. Anti-Spyware
- c. Vulnerability Protection

- d. **URL Filtering**
- e. File Blocking
- f. WildFire Analysis
- g. Data Filtering

11. Which profile do you use to detect and block an executable file from being transferred through the firewall?

- a. Anti-Spyware
- b. Vulnerability Protection
- c. **File Blocking**
- d. WildFire Analysis
- e. Data Filtering

#### *Domain 2.3.2*

1. For which two reasons are denial-of-service protections applied by zone? (Choose two.)

- a. because denial-of-service protections are applied early in the processing, before much information is known about the connection but when the ingress interface already is known
- b. because denial-of-service protections are applied only when manually turned on to avoid quota overload (which would make denial of service easier)
- c. because denial-of-service protections can only depend on the zone, and never on port numbers or IP addresses
- d. because denial-of-service protections on a Layer 3 interface are different from the denial-of-service protections available on a Layer 2 interface and interfaces on virtual wires

2. SYN flood protection provides flood protection from which protocol?

- a. UDP
- b. **TCP**
- c. ICMP
- d. GRE

3. Port scan reconnaissance protection applies to which two protocols? (Choose two.)

- a. UDP
- b. **TCP**
- c. GRE
- d. ICMP
- e. IPX

4. In which two places do you configure flood protection? (Choose two.)

- a. **DoS Protection profile**
- b. QoS profile
- c. **Zone Protection profile**

- d. SYN Protection profile
  - e. XOFF profile
5. Which two firewall features should be used to provide tailored DoS protection to a specific address?  
(Choose two.)
- a. Zone Protection profiles
  - b. virtual routers
  - c. server profiles
  - d. DoS policy rules**
  - e. DoS Protection profiles**
- Domain 2.4.6*
1. Which step is performed first on a firewall with factory default settings, according to Palo Alto Networks best practices?
- a. Add licenses.
  - b. Update PAN-OS software.
  - c. Configure the management network port.**
  - d. Update dynamic update files.
2. You finished configuring the firewall's basic connectivity in the lab and are ready to put it in the data center. What must you do before you power down the firewall?
- a. Save the changes.
  - b. Commit the changes.**
  - c. Create a restore thumb drive in case the configuration is deleted.
  - d. Verify that the configuration is correct. You do not need to do anything else if it is correct; the configuration is updated automatically.
3. The firewall's MGT port can be configured as which type of interface?
- a. Layer 2
  - b. Layer 3**
  - c. virtual wire
  - d. serial
4. When will a firewall check for the presence of bootstrap volume?
- a. each time it cold boots
  - b. each time it boots from a factory default state**
  - c. when a firewall is started in maintenance mode
  - d. each time it warm boots
5. Where in the bootstrap volume directories is a required dynamic update file located?
- a. /config

- b. /license
  - c. /software
  - d. /content**
6. Can a firewall's PAN-OS software be updated by the bootstrap process?
- a. Yes, it can be updated by including a copy of the desired PAN-OS software in the /software folder of the bootstrap volume.**
  - b. Yes, it can be updated by including a copy of the desired PAN-OS software in the /content folder of the bootstrap volume.
  - c. No, it must be updated by an administrator after the firewall starts.
  - d. No, the firewall must be licensed before the software can be updated.

#### *Domain 2.5.6*

1. Which three configuration pieces must be addressed to configure multi-factor authentication for users accessing services through the firewall? (Choose three.)
- a. GlobalProtect Portal
  - b. Captive Portal**
  - c. Authentication Enforcement profile
  - d. Authentication profile
  - e. response pages
2. Which firewall configuration component is used to configure access to an external authentication service?
- a. local user database
  - b. server profiles**
  - c. VM Information source
  - d. admin roles
  - e. Authentication policy rules
3. Which two firewall functions are reserved only for administrators assigned the superuser dynamic role? (Choose two.)
- a. managing certificates
  - b. managing firewall admin accounts**
  - c. editing the management interface settings
  - d. creating virtual systems within a firewall**
  - e. accessing the configuration mode of the CLI

#### *Domain 2.6.5*

1. Which condition could be a symptom of a certificate chain-of-trust issue?
- a. The firewall no longer decrypts HTTPS traffic.
  - b. The firewall no longer decrypts HTTPS traffic from a specific site.

- c. The firewall still decrypts HTTPS traffic from all sites, but it re-encrypts it using the Forward Untrust certificate instead of the Forward Trust certificate.
  - d. **The firewall still decrypts HTTPS traffic from a specific site, but it re-encrypts it using the Forward Untrust certificate instead of the Forward Trust certificate.**
2. Which field is mandatory in the subject field of a certificate?
- a. Organization
  - b. Organizational Unit
  - c. **Common Name**
  - d. Locale
3. Which field in a certificate must include a value known to the firewall for the certificate to be considered valid by the firewall?
- a. **Issuer**
  - b. Subject
  - c. Key
  - d. Object
4. A Palo Alto Networks firewall can obtain a certificate for its internal use through which three methods? (Choose three.)
- a. **import a certificate file generated by an external CA**
  - b. reference an externally stored certificate by a URL configured in an SSL/TLS Service profile
  - c. **generate a certificate directly by manually entering certificate data**
  - d. **obtain a certificate from an SCEP server using an SCEP Profile**
  - e. import a certificate from an external CA by using an Authentication profile
5. Which two resources must be available to successfully run certificate validation tests on a certificate received from an external source? (Choose two.)
- a. **Root Certificate of the issuing CA**
  - b. public key for the received certificate
  - c. **OCSP connection address**
  - d. existing certificate profile that matches the received certificate's CA identity
6. How are updates made to the cache of root certificates that is used for certificate verification purposes and maintained by Palo Alto Networks?
- a. The administrator reviews certificate status and replaces certificates manually.
  - b. The firewall automatically updates the certificates as it updates the associated certificate revocation list.
  - c. **The administrator installs PAN-OS software and dynamic content updates.**
  - d. The firewall automatically installs new certificates using OCSP.

7. How does a firewall administrator who creates a certificate on the firewall mark it for use in an SSL Forward Proxy configuration?

- a. They add a certificate tag in the Decryption policy rule.
- b. They configure a trust certificate in the Decryption profile.
- c. **They set the Forward Trust Certificate property of the certificate itself.**
- d. They map the certificate to the URL in the SSL/TLS Service profile.

8. Administrators within the enterprise want to replace the default certificate that is used by the firewall to secure the management web interface traffic with a certificate that is generated by their existing certificate authority. Which certificate property must be set for their new certificate to function?

- a. Certificate CN must be set to a domain name that resolves to any traffic port address of the firewall.
- b. Certificate must be signed by the firewall root certificate.
- c. Certificate must have the Forward Trust Certificate property set.
- d. **CN must be set to the management port of the firewall.**

9. A Palo Alto Networks firewall can forward DHCP packets to servers connected to which two kinds of network? (Choose two.)

- a. virtual wire
- b. Layer 2
- c. **Layer 3**
- d. **aggregate**

10. How does a Palo Alto Networks firewall that is configured to forward DHCP packets to multiple server destinations choose which reply to forward to the sender?

- a. The first server listed in the Server Priority DHCP configuration is forwarded until it fails to respond, then the next one is chosen.
- b. **A request is sent to all servers on the list, and the first responder is forwarded.**
- c. All DHCP server responses are forwarded, and the receiving client chooses which response to accept.
- d. The server that is the fewest network hops from the requesting client is chosen. When more than one server has the same hop count, all packets from the servers are forwarded to the client.

#### *Domain 2.7.5*

1. How do two legacy virtual routers on a firewall forward traffic to each other?

- a. Virtual router traffic is sent to an external router that routes it back to the second virtual router.
- b. Both virtual routers pass traffic via a dedicated VLAN routing interface.
- c. Both virtual routers pass traffic via a configurable shared routing interface.
- d. **Virtual routers forward traffic directly to each other within the firewall using routing table lookups.**

2. A firewall's virtual router can connect to which three types of interfaces? (Choose three.)

- a. virtual wire

- b. **Layer 3 traffic**
  - c. HA1
  - d. **loopback**
  - e. **tunnel**
3. Without having to make network address configuration changes, you would use which type of network interface to insert a Palo Alto Networks firewall in front of a legacy port-based firewall to collect application information from incoming network traffic?
- a. VLAN
  - b. tunnel
  - c. tap
  - d. **virtual wire**
  - e. Layer 2
4. Which type of interface do you use to connect Layer 2 and Layer 3 interfaces?
- a. **VLAN**
  - b. tunnel
  - c. tap
  - d. virtual wire
  - e. Layer 3
5. Which three types of interface can the firewall's management web interface be bound to? (Choose three.)
- a. **VLAN**
  - b. **tunnel**
  - c. virtual wire
  - d. Layer 2
  - e. **Layer 3**
6. Which three types of interfaces connect to a virtual router? (Choose three.)
- a. **VLAN**
  - b. **tunnel**
  - c. tap
  - d. Layer 2
  - e. **Layer 3**
7. Which dynamic routing protocol is *not* supported by the Palo Alto Networks firewall?
- a. RIP
  - b. OSPF
  - c. OSPFv3

- d. IGRP
  - e. BGP
8. Which action is *not* compatible with aggregate interface configuration?
- a. **aggregating 18 Layer 3 interfaces**
  - b. aggregating four virtual wire interfaces
  - c. aggregating interfaces in an HA pair
  - d. aggregating two 10Gbps optical and two 10Gbps copper Ethernet ports

#### *Domain 2.8.9*

1. Which two source address translation types can use a single IP address to NAT multiple IP addresses?  
(Choose two.)

- a. static IP
  - b. **dynamic IP**
  - c. **dynamic IP and port**
  - d. translated address
  - e. address override
2. Which NAT type can be used to translate between IPv4 and IPv6?
- a. IPv4
  - b. **NAT64**
  - c. NPTv6
  - d. IPv6

3. How does a firewall process a packet that has more than one NAT policy rule that matches the packet?
- a. Each matching rule in the list is applied from the top down, with cumulative changes being processed at the end of the list.
  - b. **The first rule matching the packet is applied and processed, skipping the others.**
  - c. The firewall issues an error when committing NAT policy rules that can affect the same packet.
  - d. The last matching rule in the list is applied and processed.

#### *Domain 2.10.7*

1. Which protocol is supported for traffic decryption matching a Decryption policy rule?
- a. IPSec
  - b. SP3
  - c. **SSH**
  - d. NLSP
2. Where do you specify that a certificate is to be used for SSL Forward Proxy?
- a. **Certificate properties**

- b. Decryption profile
  - c. Decryption policy
  - d. Security policy
3. Which feature must be configured to exclude sensitive traffic from decryption?
- a. Security policy rule that includes the specific URL with an “allow” action
  - b. Decryption policy rule with the specific URL and “no decrypt” action**
  - c. Application Override policy that matches the application URL and port number
  - d. Decryption profile that includes the site’s URL

#### *Domain 2.11.8*

1. Which parameter is important for QoS policy match decisions?
- a. App-ID**
  - b. Content-ID
  - c. User-ID
  - d. ingress interface
2. What is the maximum number of QoS classes supported by the Next-Generation Firewall?
- a. 4
  - b. 8**
  - c. 16
  - d. 32
3. In a site-to-site VPN configuration, what is an alternative method to the use of pre-shared keys to authenticate each device during connection setup?
- a. certificates**
  - b. expected IP address of the partner’s interface
  - c. known hexadecimal string configured in both endpoints
  - d. matching proxy ID definitions configured in both endpoints
4. Which type of firewall interface can be associated with a tunnel interface?
- a. tap
  - b. virtual wire
  - c. Layer 2
  - d. Layer 3**
5. A firewall administrator is deploying 50 Palo Alto Networks firewalls to protect remote sites. Each firewall must have a site-to-site IPSec VPN tunnel to each of three campus locations. Which configuration function is the basis for automatic site-to-site IPSec tunnels set up from each remote location to the three campuses?
- a. import of a settings table into the remote firewall’s IPSec tunnel config
  - b. import of a settings table into the IPSec tunnel config of the three campuses**

- c. configuration of the GlobalProtect satellite settings of the campus and remote firewalls
- d. entry of campus IPSec tunnel settings for each remote firewall's IPSec profile

## Domain 3

### *Domain 3.1.7*

1. Which option is not a parameter that is used to identify applications in an Application Override policy?
  - a. protocol
  - b. port number
  - c. **first characters in the payload**
  - d. destination IP address
2. How does the firewall resolve conflicting App-ID assignments to the same traffic between an Application Override policy rule and the firewall's built-in App-ID?
  - a. The firewall's regular App-ID is assigned.
  - b. The Application Override's App-ID is assigned.**
  - c. The App-ID is set to duplicate definitions.
  - d. The App-ID is set to "not available."
3. Which firewall process is bypassed when an Application Override policy matches traffic and assigns an App-ID?
  - a. QoS
  - b. IPSec
  - c. Content-ID**
  - d. User-ID
4. Which firewall tool provides settings and tools to convert policies from port-based to App-ID?
  - a. Network Monitor display under App Scope
  - b. Policy Optimizer under Policies**
  - c. Application Hit Count under Policies
  - d. View Applications as Groups under Policies

5. An administrator creates a Security policy rule that allows office-on-demand traffic through the firewall. After the change is committed, the firewall issues the following warning:

```
"vsys1: Rule 'Allow Office apps' application dependency warning:  
Application 'office-on-demand' requires 'ms-office365-base' be allowed  
Application 'office-on-demand' requires 'sharepoint-online' be allowed  
Application 'office-on-demand' requires 'ssl' be allowed  
Application 'office-on-demand' requires 'web-browsing' be allowed"
```

Which action should the administrator take?

- a. create an application chain that includes the dependencies
  - b. add the listed applications to the same Security policy rule**
  - c. set the Service action of the rule to “dependent application default”
  - d. create a new Security policy rule for each listed application with an “allow” action higher in the rule list
6. Which security risk is elevated when port-based Security policy rules are used?
- a. The firewall’s resources will be negatively impacted by processing unwanted traffic.
  - b. Unwanted applications can get through the firewall, bringing their vulnerabilities with them.**
  - c. The network is more vulnerable to TCP DoS attacks.
  - d. The firewall is more vulnerable to UDP DoS attacks.
7. What is the Palo Alto Networks suggested process for converting port-based Security policy rules to use App-ID?
- a. Use the Expedition tool to analyze Traffic logs against Security policy to suggest policy changes.
  - b. Use the built-in firewall reports to identify applications found in the traffic and update policy based on desired traffic.
  - c. Use the Policy Optimizer feature of the firewall to identify applications and update policy rules.**
  - d. Use the firewall’s New Applications Seen feature to identify applications and update policy rules.
8. If App-ID is implemented in Security policy rules, should port numbers also be included?
- a. No, App-ID-based Security policy rules detect and allow or block any desired application using the included port number values in the App-ID database.
  - b. Yes, including the port numbers as a service-matching condition can eliminate some traffic before App-ID processing, thus conserving firewall resources.
  - c. Yes, including an application-default setting in the service-matching condition requires that applications use only known or typical port numbers.**
  - d. No, App-ID-based Security policy rules detect and allow or block any desired application using the edited port number values in the App-ID database.
9. An application using which protocol can receive an incomplete value in the Application field in the Traffic log?
- a. UDP
  - b. TCP**
  - c. ICMP
  - d. GRE
10. Session traffic being evaluated by a firewall is encrypted with SSL. If the firewall does not decrypt the traffic, how can the firewall make an App-ID determination?
- a. evaluate the HTTP headers
  - b. evaluate the SSL Hello exchange
  - c. evaluate certificate contents used for encryption**

- d. use information in the SSL Decryption Exclusion cache
11. While a firewall is scanning an active session, how does it respond when it detects a change of application?
- a. It closes the session, opens a new one, and evaluates all Security policy rules again.
  - b. It closes the session, opens a new one, and evaluates the original matching Security policy rule only.
  - c. **It updates the app in the existing session and evaluates all Security policy rules again.**
  - d. It updates the app in the existing session and continues to use the original action from the first Security policy rule match.

#### *Domain 3.2.10*

1. Which GlobalProtect configuration component contains the setting that specifies when the agent software starts on the client system?
- a. **Agent settings in the GlobalProtect Portal settings**
  - b. General settings in the GlobalProtect Portal settings
  - c. Agent settings of the GlobalProtect Gateway
  - d. General settings of the GlobalProtect Gateway
2. Which configuration or service is required for an iOS device using the GlobalProtect license to connect to a GlobalProtect Gateway?
- a. X-Auth configuration in the gateway settings
  - b. **GlobalProtect Gateway license**
  - c. firewall Authentication policy with an iOS setting
  - d. GlobalProtect client downloaded from the GlobalProtect Portal
3. A GlobalProtect Gateway is solely responsible for which function?
- a. **terminating SSL tunnels**
  - b. authenticating GlobalProtect users
  - c. creating on-demand certificates to encrypt SSL
  - d. managing and updating GlobalProtect client configurations
  - e. managing GlobalProtect Gateway configurations

#### *Domain 3.3.6*

1. Which two configuration conditions must be met for a firewall to NAT between IPv4 and IPv6? (Choose two.)
- a. Select NAT64 in the Session tab under Device > Setup > Session.
  - b. **Choose the NAT Type of NAT64 in the General tab of a NAT policy rule.**
  - c. **Add an IPv6 address to the Translated Packet tab.**
  - d. Add an IPv6 prefix in the NAT64 configuration in the NAT policy rule.

2. Which two configuration conditions must be met for a Palo Alto Networks firewall to send and receive IPv6 traffic? (Choose two.)

- a. Enable IPv6 check box in the virtual router configuration is checked.
- b. An Ethernet interface is configured for virtual wire.
- c. **An Ethernet interface is configured for Layer 3.**
- d. **Enable IPv6 Firewalling check box under Session Settings is turned on.**

#### *Domain 3.5.8*

1. For WildFire file type support, which file types are supported for analysis? Select all that apply.

- a. **Links contained in emails**
- b. **Adobe Flash files**
- c. **PDF files**
- d. **Java Archive (JAR) files**

2. A server on the DMZ with a private NIC address has network access provided by a NAT policy rule whose Bi-directional check box is selected in the Translated Packet settings for static IP source address translation. Which Security policy rule must be created to allow bidirectional traffic to and from the DMZ server?

- a. **a rule for each direction of travel using the pre-NAT server IP address**
- b. a rule with the post-NAT source IP address
- c. a rule for each direction of travel using the post-NAT server IP address
- d. a rule with the pre-NAT source IP address

3. An internal web browser sends a packet to a server. The browser's connection has the source IP address 192.168.5.3, port 31415. The destination is 209.222.23.245, port 80. The firewall translates the source to 75.22.21.54, port 27182. Which three of these source IP addresses would cause a NAT policy rule to apply to this traffic? (Choose three.)

- a. **192.168.5.0/24**
- b. 75.22.21.0/24
- c. **192.168.4.0/23**
- d. **192.168.0.0/16**
- e. 75.22.0.0/17
- f. 75.22.128.0/17

4. A NAT policy rule is created to change the destination address of any packets with a source of any address and a destination address of 10.10.10.10 (in the DMZ zone) to 192.168.3.45 (in the Trust zone). Which Security policy rule components are required for a packet that has this rule applied to match and allow this traffic?

- a. source address any, source zone any, destination address 192.168.3.45, destination zone Trust, action = allow
- b. **source address any, source zone any, destination address 10.10.10.10, destination zone Trust, action = allow**

- c. source address any, source zone any, destination address 192.168.3.45, destination zone DMZ, action = allow
  - d. source address any, source zone any, destination address 10.10.10.10, destination zone DMZ, action = allow
5. Which file type is not supported by WildFire?
- a. iOS
  - b. Android
  - c. Windows PE
  - d. Microsoft Excel
6. The firewall will skip the file upload to WildFire in which three cases? (Choose three.)
- a. **The file has been signed by a trusted signer.**
  - b. The file is being uploaded rather than downloaded.
  - c. The file is an attachment in an email.
  - d. **The file hash matches a previous submission.**
  - e. **The file is larger than 50MB.**

7. Which feature is *not* supported on the WF-500 appliance?

- a. **bare metal analysis**
- b. Microsoft Windows XP 32-bit analysis
- c. Microsoft Windows 7 64-bit analysis
- d. static analysis

## Domain 4

### *Domain 4.1.7*

1. The Security policy for all of a customer's remote offices is the same, but different offices have different firewall models. If the remote offices are managed by Panorama, how might the offices share device groups and templates?
- a. same device groups, same template stacks
  - b. same device groups, different template stacks**
  - c. different device groups, same template stacks
  - d. different device groups, different template stacks
2. A Panorama template stack contains two templates, and one configuration setting has a different value in each template. When Panorama pushes the template stack to the managed firewalls, which setting value will the firewalls receive?
- a. value from the top template of the stack**
  - b. value from the bottom template in the stack
  - c. value from the template designated as the parent

- d. value an administrator selects from the two available values
3. Which two firewall settings are stored in Panorama templates? (Choose two.)
- a. custom Application-ID signatures
  - b. Server Profile for an external LDAP server**
  - c. services definitions
  - d. DoS Protection profiles
  - e. data-plane interface configurations**

#### *Domain 4.3.12*

- 1. What is the format of the firewall configuration files?
  - a. YAML
  - b. JSON
  - c. XML**
  - d. CSV
- 2. Which method can be used to restore the previous configuration when a new configuration committed on a firewall has undesired consequences?
  - a. Use the Load configuration version to restore the previous configuration settings and follow with a commit.**
  - b. Use the Rollback commit link in the commit completion message.
  - c. Use the Import device state to restore the pre-commit configuration.
  - d. Use the Load named configuration snapshot to restore the previous configuration and follow with a commit.
- 3. Which CLI command do you use to move a configuration file from an external server to a firewall's local storage?
  - a. rdist
  - b. ssh
  - c. scp**
  - d. rcp
- 4. Where in Panorama do you enter Security policy rules to ensure that your new rules will take precedence over locally entered rules?
  - a. Security policy rules with a targeted firewall
  - b. default rules section of Security policy rules
  - c. pre-rules section of Security policy rules**
  - d. post-rules section of Security policy rules
- 5. In Panorama, how should you make changes to a Security policy rule for a specific firewall?
  - a. Log in to Panorama, clone the rule, modify the clone, and add a target firewall to the new rule.**

- b. Select the rule, click the override button, and enter the changes.
  - c. Create a new locally defined Security policy rule that is placed higher in the rule list than the rule to be overridden.
  - d. Log in to Panorama and modify the original rule.
6. Which three firewall settings are stored in Panorama device groups? (Choose three.)
- a. **custom Application-ID signatures**
  - b. **services definitions**
  - c. **DoS Protection profiles**
  - d. data-plane interface configurations
  - e. Zone Protection profiles

## Domain 5

### *Domain 5.1.9*

1. Dynamic tags can be assigned to which kind of data in a log event?
- a. source and destination address, source and destination zone name
  - b. source and destination address**
  - c. interface, zone name
  - d. DNS name, zone name
2. How can the firewall use dynamically tagged objects to block traffic?
- a. Add the object to an enforcement list of a Data Filtering object that then is attached to a Security policy rule.
  - b. Assign the object to a dynamic list, which then is included in the destination address matching condition of a Security policy rule.
  - c. Assign the object to a Dynamic Address Group object, which then is added to the destination address matching condition of a Security policy rule.**
  - d. Add the object to an application group and use it in Security policy rules.
3. A tag can be dynamically assigned to data in which four types of logs? (Choose four.)
- a. Traffic**
  - b. Threat**
  - c. URL Filtering**
  - d. HIP Match
  - e. Tunnel Inspection**
  - f. Configuration
  - g. System
4. Dynamic tagging activity is recorded in which log?
- a. System

- b. Configuration
  - c. **IP-Tag**
  - d. Data Filtering
5. A firewall can forward log events to which two types of log formats? (Choose two.)
- a. XES
  - b. **SNMP**
  - c. **HTTP**
  - d. databases using XML format
6. How does a firewall forward log events to an external destination?
- a. It sends them in batches at the frequency specified in the destination's Server Profile.
  - b. It queues them and sends them in batches at differing intervals, depending on the event severity.
  - c. It sends them as quickly as the required QoS policy rule governing log event traffic allows.
  - d. It sends them in real time as the firewall generates them.**
7. Which two firewall logs can be exported using the Scheduled Log Export function? (Choose two.)
- a. Configuration
  - b. System
  - c. **Traffic**
  - d. **URL**

#### *Domain 5.2.6*

1. Match the upgrade step description with the correct step number.

a. Upgrade PAN-OS software.	Step 3
b. Reboot the firewall.	Step 4
c. Update dynamic content.	Step 2
<b>d. Activate subscription licenses.</b>	<b>Step 1</b>

2. Match each component with the order in which the component should be upgraded to a new version of PAN-OS software.

a. HA active firewall	Step 4
<b>b. Panorama</b>	<b>Step 1</b>
c. Log Collector	Step 2
d. HA passive firewall	Step 3

3. How do you upgrade an active/passive HA firewall pair to PAN-OS 10.1 while maintaining internet access?

- a. Upgrade the active firewall first, then the passive one.
- b. Upgrade the passive firewall first, then the active one.**
- c. Run the upgrade on the active firewall. It will manage the process and upgrade the passive firewall.
- d. You must upgrade both members of the pair at the same time, which requires an upgrade window that allows downtime.

#### *Domain 5.3.10*

1. Which feature is an intended advantage of an active/active firewall pair versus an active/passive pair?

- a. increased throughput
- b. support of asynchronous routing**
- c. increased session count
- d. shared dynamic updates

2. Which location does a firewall use to forward HA-related events to an external monitoring technology?

- a. Device > Log Settings > System Log settings**
- b. Objects > Log Forwarding Profile > System Log Type
- c. Device > High Availability > General > Event Forwarding
- d. Dashboard > High Availability Widget > Notification

3. Which two Panorama objects can display current HA state information about a managed firewall? (Choose two.)

- a. firewall listings in Monitor > HA Status
- b. firewall-specific information in Managed Devices > Health**
- c. firewall listings in Managed Devices > Summary**
- d. firewall HA Status widget in Dashboard > Widgets
- e. firewall HA status in Panorama > High Availability

4. In which circumstance would you recommend an active/active firewall pair instead of an active/passive firewall pair?

- a. Active/active is the preferred solution when the firewall pair is behind a load balancer that randomizes routing, thus requiring both firewalls to be active.**
- b. Active/active usually is the preferred solution because it allows for more bandwidth while both firewalls are up.
- c. Active/active is the preferred solution when the PA-7000 Series is used. Use active/passive with the PA-5200 Series or smaller form factors.
- d. Active/active is the preferred solution when the PA-5200 Series or smaller form factors are used. Use active/passive with the PA-7000 Series.

5. Which two events can trigger an HA pair failover event? (Choose two.)

- a. An HA1 cable is disconnected from one of the firewalls.**

- b. A dynamic update fails to download and install.
  - c. **The firewall fails to successfully ping a path-monitored destination address.**
  - d. OSPF implemented on the firewall determines that an available route is now down.
  - e. RIP implemented on the firewall determines that an available route is now down.
6. Which two firewall features support floating IP addresses in an active/active HA pair? (Choose two.)
- a. data-plane traffic interfaces
  - b. **source NAT**
  - c. **VPN endpoints**
  - d. loopback interfaces
  - e. management port
7. How are firewall configurations in an active/passive HA pair synchronized if the firewalls are not under Panorama control?
- a. An administrator commits the changes to one, then commits them to the partner, at which time the changes are sent to the other.
  - b. An administrator pushes the configuration file to both firewalls, then commits them.
  - c. **An administrator commits changes to one, which automatically synchronizes with the other.**
  - d. An administrator schedules an automatic sync frequency in the firewall configurations.
8. In which two ways is an active/passive HA pair configured in virtual firewalls deployed in public clouds? (Choose two.)
- a. **The virtual firewalls are deployed in a cloud scale set with a cloud-supplied load balancer in front to detect and manage failover.**
  - b. **The virtual firewalls rely on a VM-Series plugin to map appropriate cloud functions to the firewall's HA settings.**
  - c. Virtual firewalls use PAN-OS HA configuration combined with appropriate cloud deployments of interfaces for HA use.
  - d. The virtual firewalls use an HA compatibility module for the appropriate cloud technology.

## Domain 6

### Domain 6.2.7

1. Where in the firewall web interface can you see whether sessions are going through a specific interface?
- a. Dashboard
  - b. Application Command Center (ACC)
  - c. Session Log node on the Monitor tab
  - d. Session Browser on the Monitor tab
2. Communication through a specific interface works most of the time but fails when traffic throughput is at its highest. Which policy would you consider implementing to identify the problem?

- a. Security
  - b. DoS Protection
  - c. QoS
  - d. Application Override
3. Which interface type allows you to control traffic with the least disruption to a network?
- a. tap
  - b. Layer 3
  - c. Layer 2
  - d. virtual wire

#### *Domain 6.3.6*

1. Why would SSL decryption that has been working suddenly stop?
- a. **The firewall's CA certificate expired.**
  - b. The firewall's IP address, which is encoded in the certificate, changed.
  - c. The firewall has been upgraded to a different model.
  - d. The firewall's decryption subscription expired.
2. A company uses a small SaaS application provider. This application is accessed through HTTPS but suddenly stops working through the firewall. However, when the application is accessed from home, users receive an error about the certificate. Which two situations would explain this behavior? (Choose two.)
- a. **The SaaS certificate had expired. The firewall's decryption policy is configured to block connections with expired certificates.**
  - b. The SaaS certificate had expired. The firewall's decryption policy is configured to use the untrusted CA with expired certificates.
  - c. **The SaaS certificate was replaced with one whose certificate authority is not known to the firewall. The firewall's decryption policy is configured to block connections with certificates whose CA is not trusted.**
  - d. The SaaS certificate was replaced with one whose certificate authority is not known to the firewall. The firewall's decryption policy is configured to use the untrusted certificate for certificates whose CA is not trusted.
  - e. The firewall's own CA certificate needs to be updated.
3. Which encryption algorithm is not supported by the firewall and causes the firewall to drop the connection?
- a. **DES**
  - b. 3DES
  - c. AES256-CBC
  - d. AES256-GCM

### *Domain 6.5.5*

1. Where do you find the dynamic routing configuration in the next-generation firewall's web interface?
  - a. Device > Network > Virtual Router
  - b. Network > Virtual Router**
  - c. Device > Network > Interfaces
  - d. Network > Interfaces
  
2. The organization has three redundant connections to the internet, and all three of them are available. What are two reasons why access to one set of IP addresses through the firewall consistently results in good performance while access to another set of IP addresses consistently results in poor performance? (Choose two.)
  - a. The organization uses equal-cost multi-path (ECMP) routing to the internet and selects which path to use based on the source IP address, and some IP addresses get routed through a slower ISP.**
  - b. The organization uses Policy Based Forwarding (PBF) and selects which route to use for the internet based on source IP address, and some IP addresses get routed through a slower ISP.**
  - c. The organization uses the Routing Information Protocol (RIP), and some IP addresses get routed through a slower ISP.
  - d. The organization uses Border Gateway Protocol (BGP), and some IP addresses get routed through a slower ISP.
  - e. The organization uses Open Shortest Path First (OSPF), and some IP addresses get routed through a slower ISP.
  
3. An organization has two links to the internet, one 100Mbps and the other 10Mbps. The firewall balances them using ECMP in the virtual router. Which load balancing ECMP setting does the organization need to use to optimize network resources?
  - a. Balanced Round Robin
  - b. Weighted Round Robin, with a weight of 10 for the fast connection and 100 for the slow one
  - c. IP Hash
  - d. Weighted Round Robin, with a weight of 100 for the fast connection and 10 for the slow one**
  
4. Which Security profile does not have a packet-capture option?
  - a. Antivirus
  - b. Anti-Spyware
  - c. Vulnerability Protection
  - d. URL Filtering**
  
5. On a PA-7080, which feature do you need to disable to use packet capture?
  - a. NAT
  - b. hardware offload**
  - c. hardware acceleration

- d. decryption
6. When must you use `tcpdump` to capture traffic on the Next-Generation Firewall?
- a. on tunnel interface traffic
  - b. on data-plane interfaces**
  - c. on packets on the management interface
  - d. on IPSec negotiation traffic
7. If users cannot access their Gmail accounts through the firewall, which log and filter do you use to troubleshoot the problem?
- a. Traffic, (app eq gmail)**
  - b. Traffic, (app in gmail)
  - c. Configuration, (app eq gmail)
  - d. Configuration, (app in gmail)
8. You cannot access the firewall web interface. From the firewall CLI, how do you check whether the web service is running?
- a. `ps -aux | grep appweb`
  - b. `ps -aux | match appweb`
  - c. `show system software status | grep appweb`
  - d. show system software status | match appweb**
9. Which firewall log displays information about connection failures to an external LDAP authentication server?
- a. Traffic
  - b. System**
  - c. User-ID
  - d. Authentication

#### *Domain 6.6.4*

1. Applying Zone Protections to all interfaces, both internal and external, for protective measures across the entire environment is an example of \_\_\_\_\_.
- a. Zero Trust approach**
  - b. Alarm rate
  - c. SYN cookies
  - d. Maximum CPS rate

## Appendix B: Sample Test

1. What is the last step of packet processing in the firewall?
  - a. check allowed ports
  - b. check Security profiles
  - c. check Security policy
  - d. forwarding lookup
2. Which interface type requires you to configure where the next hop is for various addresses?
  - a. tap
  - b. virtual wire
  - c. Layer 2
  - d. Layer 3
3. How do you enable the firewall to be managed through a data-plane interface?
  - a. You specify Web UI in the interface properties.
  - b. You specify Management in the interface properties.
  - c. You specify HTTPS in the Interface Management profile, and then specify in the interface properties to use that profile.
  - d. You specify Management in the Interface Management profile, and then specify in the interface properties to use that profile.
4. Some devices managed by Panorama have their external interface on ethernet1/1, some on ethernet1/2. However, the zone definitions for the external zone are identical. What is the recommended solution in this case?
  - a. Create two templates: one for the ethernet1/1 devices, one for the ethernet1/2 devices. Use the same external zone definitions in both. Apply those two templates to the appropriate devices.
  - b. Create three templates: one for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Use those templates to create two template stacks, one with the ethernet1/1 and external zone, another with the ethernet1/2 and external zone. Apply those two template stacks to the appropriate devices.
  - c. Create three templates: one for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).

- d. Create three template stacks: one for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).
5. In a Panorama managed environment, which two options show the correct order of policy evaluation? (Choose two.)
- a. device group pre-rules, shared pre-rules, local firewall rules, intrazone-default, interzone-default
  - b. device group pre-rules, local firewall rules, shared post-rules, device group post-rules, intrazone-default, interzone-default
  - c. device group pre-rules, local firewall rules, device group post-rules, shared post-rules, intrazone-default, interzone-default
  - d. device group pre-rules, local firewall rules, intrazone-default, interzone-default, device group post-rules, shared post-rules
  - e. shared pre-rules, device group pre-rules, local firewall rules, intrazone-default, interzone-default
6. When you deploy the Palo Alto Networks NGFW on NSX, how many virtual network interfaces does a VM-Series firewall need?
- a. two: one for traffic input and output and one for management traffic
  - b. four: two for traffic input and output and two for management traffic (for high availability)
  - c. three: one for traffic input, one for traffic output, and one for management traffic
  - d. six: two for traffic input, two for traffic output, and two for management traffic (for high availability)
7. Which source of user information is *not* supported by the NGFW?
- a. RACF
  - b. LDAP
  - c. Active Directory
  - d. SAML
8. What is the main mechanism of packet-based vulnerability attacks?
- a. malformed packets that trigger software bugs when they are received
  - b. excess packets that fill up buffers, thus preventing legitimate traffic from being processed
  - c. packets that get responses that leak information about the system
  - d. packets that either fill up buffers or get responses that leak information
9. Which method is *not* a PAN-OS software decryption method?
- a. SSH Proxy

- b. SSL Proxy
  - c. SSL Forward Proxy
  - d. SSL Inbound Inspection
10. Which type of identification does an Application Override policy override?
- a. App-ID
  - b. User-ID
  - c. Content-ID
  - d. Service
11. Which two types of protocols can cause an insufficient data value in the Application field in the Traffic log? (Choose two.)
- a. UDP
  - b. TCP
  - c. ICMP
  - d. GRE
  - e. IGP
12. Which three profile types are used to prevent malware executables from entering the network? (Choose three.)
- a. Anti-Spyware
  - b. WildFire Analysis
  - c. File Blocking
  - d. Vulnerability Protection
  - e. Zone Protection
13. Which user credential detection method does *not* require access to an external directory?
- a. group mapping
  - b. domain credential filter
  - c. LDAP
  - d. Certificate

14. Which object type has a property to specify whether it can transfer files?
  - a. Application
  - b. Service
  - c. User
  - d. User group
15. When destination NAT rules are configured, the associated Security rule is matched using which parameters?
  - a. pre-NAT source zone and post-NAT destination zone
  - b. post-NAT source zone and pre-NAT destination zone
  - c. pre-NAT source zone and post-NAT destination IP address
  - d. post-NAT source zone and post-NAT destination zone
16. What is the initial IP address for the management interface?
  - a. 10.0.0.1
  - b. 172.16.0.1
  - c. 192.168.1.1
  - d. 192.168.255.254
17. In a new firewall, which port provides web interface access by default?
  - a. data port #1
  - b. any data port
  - c. management port
  - d. console port
18. Which application requires you to import private keys?
  - a. Captive Portal
  - b. Forward Trust
  - c. SSL Inbound Inspection
  - d. SSL Exclude Certificate
19. Under which conditions can two Layer 3 interfaces have the same IP address?
  - a. They must be connected to a common VLAN object interface.
  - b. They must be connected to the same Ethernet network through a switch. This configuration can be used only for high availability.

- c. They must be connected to different virtual routers.
  - d. They must be subinterfaces of the same physical interface.
  - e. This feature is not supported.
20. Which two protocols are supported for site-to-site VPNs? (Choose two.)
- a. Authentication Header (AH)
  - b. Secure Socket Layer (SSL)
  - c. Encapsulating Security Payload (ESP)
  - d. Transport Layer Security (TLS)
  - e. Secure Shell (SSH)
21. GlobalProtect Portal is responsible for which two functions? (Choose two.)
- a. terminating SSL tunnels
  - b. authenticating GlobalProtect users
  - c. creating on-demand certificates to encrypt SSL
  - d. managing and updating GlobalProtect client configurations
  - e. managing GlobalProtect Gateway configurations
22. What is the preferred SYN flood defense action type?
- a. Random Drop
  - b. Random Early Drop
  - c. SYN Proxy
  - d. SYN Cookies
23. What would be a valid reason to allow non-SYN TCP packets at the start of a connection?
- a. Such packets could happen legitimately in the case of asymmetric routing.
  - b. Such packets could happen legitimately if there is load balancing across firewalls.
  - c. Such packets could happen legitimately because of either asymmetric routing or load balancing across firewalls.
  - d. Such packets could happen because of router bugs.
24. Where do you configure protection from malformed IP and TCP headers?
- a. DoS Profile
  - b. QoS Profile
  - c. Zone Protection profile

- d. Application Profile
25. Which parameter is *not* a valid criterion for the original packet in address translation?
- a. source zone
  - b. application
  - c. service
  - d. destination address
26. Which parameter in a Security policy rule do you use to apply a rule to traffic coming in from a specific interface?
- a. source zone
  - b. source address
  - c. user
  - d. source interface
27. Where do you specify that certain URL categories are not to be decrypted?
- a. certificate properties
  - b. Decryption profile
  - c. Decryption policy
  - d. Security policy
28. Where do you specify how the firewall should treat invalid certificates?
- a. certificate properties
  - b. Decryption Profile
  - c. Decryption policy
  - d. Security policy
29. Which two public cloud environments support pay-as-you-go (PAYG) firewall licensing? (Choose two.)
- a. Microsoft Azure
  - b. Microsoft Hyper-V
  - c. Amazon AWS
  - d. VMware NSX
  - e. VMware ESXi

30. Which log type gets redirected in Device > Log Settings?
- Config
  - Traffic
  - Threat
  - WildFire Submission
31. Which tab of the firewall web interface gives you a consolidated picture of the security situation and the top-level threats?
- Dashboard
  - ACC
  - Monitor
  - Devices
32. A company's custom application uses SMTP (email) to transfer directory information, which needs to be filtered in a different manner from normal SMTP. How do you configure this filtering?
- You cannot do it with the NGFW. You need to manually configure a proxy.
  - Create specific rules for the sources and destinations that run this application.
  - Create a custom signature and specify the SMTP fields that are different from normal SMTP use and patterns to identify when it is the custom application.
  - Create an Application Override policy and specify the sources and destinations that run this application.
33. Which kind of update requires a disruption in connectivity?
- downloading the PAN-DB seed file
  - dynamic content
  - PAN-OS software
  - WildFire subscription antivirus signatures
34. Which dedicated high availability port is used for which plane?
- HA1 for the data plane, HA2 for the management plane
  - HA1 for the management plane, HA2 for the data plane
  - MGT for the management plane, HA2 as a backup
  - MGT for the management plane, HA2 for the data plane

35. Which two protocols can AutoFocus use to retrieve log information from an NGFW? (Choose two.)
- a. syslog
  - b. Log transfer protocol, a Palo Alto Networks proprietary protocol
  - c. HTTP
  - d. HTTPS
  - e. SNMP
36. Palo Alto Networks publishes new applications at which approximate interval?
- a. every 30 minutes
  - b. hourly
  - c. daily
  - d. weekly
37. Which type of device can receive the GlobalProtect data files content update?
- a. Log Collector
  - b. firewall
  - c. WildFire
  - d. Antivirus
38. In which log will you see evidence that an administrator cannot log in to the firewall?
- a. Traffic
  - b. System
  - c. Configuration
  - d. Authentication
39. How do you reboot the firewall from the command line?
- a. restart system
  - b. reboot
  - c. request restart system
  - d. request reboot

40. Where in the user interface do you configure how many packets to capture when the extended-capture option is selected in an Anti-Spyware profile or Vulnerability profile?
- Device tab, as part of the Setup node
  - Security profiles because the desired number of captured packets can vary between profiles
  - as a default in the Device tab, as part of the Capture node. Then, exceptions can be configured in the Security profiles.
  - Capturing options for each defined capture file
41. You are preparing a bootstrap template for use with a VM-Series firewall hosted in a public cloud. You do not need to include the Content-ID files because the firewall will download the latest version when it is booted. How do you configure the bootstrap's content?
- Create a content directory with an empty file named "download latest" and leave it empty.
  - Delete the Content-ID files.
  - Rename Content-ID files to content-null.
  - Add an empty file to Content-ID files named no-download.
42. Which format do you use for an AWS CloudFormation Template?
- XML
  - CSV
  - JSON
  - JSON or XML
43. In which order are Security policy rules from Panorama processed relative to local firewall policy rules?
- Local firewall policy rules are processed only during loss of Panorama connectivity.
  - All Panorama rules are processed first.
  - All local firewall policy rules are processed first.
  - Some Panorama rules are processed before the firewall's local rules, and some are processed after the local rules.
44. Which statement is true about Security profiles?
- They are evaluated from top down, with the first match processing the traffic.
  - They are applied to all inbound traffic when they are enabled.
  - They enable a specific type of threat scanning (e.g., Virus, Spyware).
  - They can specify actions based on the username.

45. Which Captive Portal authentication method can be handled by the browser without affecting the user experience?
- web-challenge
  - browser-challenge
  - web-form
  - browser-form
46. The firewall of a defense contractor is not connected to the internet. However, it is connected to the classified SIPRNet. The contractor is concerned about getting malware files through that network. Can this defense contractor use the WildFire service for protection?
- No, because there is no network path to the WildFire cloud.
  - No, because all SIPRNet files are encrypted.
  - Yes, but only for PE-type file analysis.
  - Yes, they can use a WF-500 appliance.
47. How does the NGFW handle excess packets when there are QoS constraints?
- It buffers them until there is bandwidth to send them.
  - It drops a percentage of them randomly.
  - It replaces them with packets that tell the computer on the other side to slow down.
  - It sends a portion instead of the whole packet.
48. Which function does the management plane perform?
- signature matching
  - VPN encryption
  - policy matching
  - User-ID group lookups
49. Which User-ID IP-address-to-username mapping method can be visible to users?
- Captive Portal
  - monitoring Active Directory event logs
  - monitoring print server event logs
  - monitoring a Cisco WLAN controller

50. Which feature of the NGFW enables you to identify attempts to tunnel SSH over other ports?

- a. App-ID
- b. Content-ID
- c. User-ID
- d. SSH Forward Proxy

51. What is the correct order of operations?

- a. Check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security policy, check Security profiles, re-encrypt traffic.
- b. Check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security profiles, check Security policy, re-encrypt traffic.
- c. Decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security policy, re-encrypt traffic.
- d. Decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security profiles, check Security policy, re-encrypt traffic.

## Appendix C: Answers to the Sample Test

1. What is the last step of packet processing in the firewall?
  - a. check allowed ports
  - b. check Security Profiles**
  - c. check Security policy
  - d. forwarding lookup
2. Which interface type requires you to configure where the next hop is for various addresses?
  - a. tap
  - b. virtual wire
  - c. Layer 2
  - d. Layer 3**
3. How do you enable the firewall to be managed through a data-plane interface?
  - a. You specify Web UI in the interface properties.
  - b. You specify Management in the interface properties.
  - c. You specify HTTPS in the Interface Management Profile, and then specify in the interface properties to use that profile.**
  - d. You specify Management in the Interface Management Profile, and then specify in the interface properties to use that profile.
4. Some devices managed by Panorama have their external interface on ethernet1/1, some on ethernet1/2. However, the zone definitions for the external zone are identical. What is the recommended solution in this case?
  - a. Create two templates: one for the ethernet1/1 devices, one for the ethernet1/2 devices. Use the same external zone definitions in both. Apply those two templates to the appropriate devices.**
  - b. Create three templates: one for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Use those templates to create two template stacks, one with the ethernet1/1 and external zone, another with the ethernet1/2 and external zone. Apply those two template stacks to the appropriate devices.
  - c. Create three templates: one for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).
  - d. Create three template stacks: one for the ethernet1/1 devices, one for the ethernet1/2 devices, and one with the external zone definitions. Apply the external zone template to all devices, and the ethernet1/1 and ethernet1/2 as appropriate (you can apply up to five templates per device).

5. In a Panorama managed environment, which two options show the correct order of policy evaluation? (Choose two.)
  - a. device group pre-rules, shared pre-rules, local firewall rules, intrazone-default, interzone-default
  - b. device group pre-rules, local firewall rules, shared post-rules, device group post-rules, intrazone-default, interzone-default
  - c. **device group pre-rules, local firewall rules, device group post-rules, shared post-rules, intrazone-default, interzone-default**
  - d. device group pre-rules, local firewall rules, intrazone-default, interzone-default, device group post-rules, shared post-rules
  - e. **shared pre-rules, device group pre-rules, local firewall rules, intrazone-default, interzone-default**
6. When you deploy the Palo Alto Networks NGFW on NSX, how many virtual network interfaces does a VM-Series firewall need?
  - a. two, one for traffic input and output and one for management traffic
  - b. four, two for traffic input and output and two for management traffic (for High Availability)
  - c. **three, one for traffic input, one for traffic output, and one for management traffic**
  - d. six, two for traffic input, two for traffic output, and two for management traffic (for High Availability)
7. Which source of user information is *not* supported by the NGFW?
  - a. **RACF**
  - b. LDAP
  - c. Active Directory
  - d. SAML
8. What is the main mechanism of packet-based vulnerability attacks?
  - a. **malformed packets that trigger software bugs when they are received**
  - b. excess packets that fill up buffers, thus preventing legitimate traffic from being processed
  - c. packets that get responses that leak information about the system
  - d. packets that either fill up buffers or get responses that leak information
9. Which method is *not* a PAN-OS software decryption method?
  - a. SSH Proxy
  - b. **SSL Proxy**
  - c. SSL Forward Proxy
  - d. SSL Inbound Inspection

10. What type of identification does an Application Override policy override?
  - a. **App-ID**
  - b. User-ID
  - c. Content-ID
  - d. Service
11. Which two types of protocols can cause an insufficient data value in the Application field in the Traffic log? (Choose two.)
  - a. **UDP**
  - b. **TCP**
  - c. ICMP
  - d. GRE
  - e. IGP
12. Which three profile types are used to prevent malware executables from entering the network? (Choose three.)
  - a. **Antivirus**
  - b. Anti-Spyware
  - c. **WildFire Analysis**
  - d. **File Blocking**
  - e. Vulnerability Protection
13. Which user credential detection method does *not* require access to an external directory?
  - a. group mapping
  - b. domain credential filter
  - c. LDAP
  - d. **Certificate**

14. Which object type has a property to specify whether it can transfer files?
- a. **Application**
  - b. Service
  - c. User
  - d. User group
15. When destination NAT rules are configured, the associated Security rule is matched using which parameters?
- a. **pre-NAT source zone and post-NAT destination zone**
  - b. post-NAT source zone and pre-NAT destination zone
  - c. pre-NAT source zone and post-NAT destination IP address
  - d. post-NAT source zone and post-NAT destination zone
16. What is the initial IP address for the management interface?
- a. 10.0.0.1
  - b. 172.16.0.1
  - c. **192.168.1.1**
  - d. 192.168.255.254
17. In a new firewall, which port provides web interface access by default?
- a. data port #1
  - b. any data port
  - c. **management port**
  - d. console port
18. Which application requires you to import private keys?
- a. Captive Portal
  - b. Forward Trust
  - c. **SSL Inbound Inspection**
  - d. SSL Exclude Certificate
19. Under which conditions can two Layer 3 interfaces have the same IP address?
- a. They must be connected to a common VLAN object interface.
  - b. They must be connected to the same Ethernet network through a switch. This configuration can be used only for High Availability.

- c. They must be connected to different virtual routers.
  - d. They must be subinterfaces of the same physical interface.
  - e. **This feature is not supported.**
20. Which two protocols are supported for site-to-site VPNs? (Choose two.)
- a. **Authentication Header (AH)**
  - b. Secure Socket Layer (SSL)
  - c. **Encapsulating Security Payload (ESP)**
  - d. Transport Layer Security (TLS)
  - e. Secure Shell (SSH)
21. GlobalProtect Portal is responsible for which two functions? (Choose two.)
- a. terminating SSL tunnels
  - b. **authenticating GlobalProtect users**
  - c. creating on-demand certificates to encrypt SSL
  - d. **managing and updating GlobalProtect client configurations**
  - e. managing GlobalProtect Gateway configurations
22. What is the preferred SYN flood defense action type?
- a. Random Drop
  - b. Random Early Drop
  - c. SYN Proxy
  - d. **SYN Cookies**
23. What would be a valid reason to allow non-SYN TCP packets at the start of a connection?
- a. Such packets could happen legitimately in the case of asymmetric routing.
  - b. **Such packets could happen legitimately if there is load balancing across firewalls.**
  - c. Such packets could happen legitimately because of either asymmetric routing or load balancing across firewalls.
  - d. Such packets could happen because of router bugs.
24. Where do you configure protection from malformed IP and TCP headers?
- a. DoS Profile
  - b. QoS Profile
  - c. **Zone Protection profile**

- d. Application Profile
25. Which parameter is *not* a valid criterion for the original packet in address translation?
- a. source zone
  - b. application**
  - c. service
  - d. destination address
26. Which parameter in a Security policy rule do you use to apply a rule to traffic coming in from a specific interface?
- a. source zone**
  - b. source address
  - c. user
  - d. source interface
27. Where do you specify that certain URL categories are not to be decrypted?
- a. certificate properties
  - b. Decryption Profile
  - c. decryption policy**
  - d. Security policy
28. Where do you specify how the firewall should treat invalid certificates?
- a. certificate properties
  - b. Decryption Profile**
  - c. decryption policy
  - d. Security policy
29. Which two public cloud environments support pay-as-you-go (PAYG) firewall licensing? (Choose two.)
- a. Microsoft Azure**
  - b. Microsoft Hyper-V
  - c. Amazon AWS**
  - d. VMware NSX
  - e. VMware ESXi

30. Which log type gets redirected in **Device > Log Settings**?
- Config**
  - Traffic
  - Threat
  - WildFire Submission
31. Which tab of the firewall web interface gives you a consolidated picture of the security situation and the top-level threats?
- Dashboard
  - ACC**
  - Monitor
  - Devices
32. A customer's custom application uses SMTP (email) to transfer directory information, which needs to be filtered in a different manner from normal SMTP. How do you configure this filtering?
- You cannot do it with the NGFW. You need to manually configure a proxy.
  - Create specific rules for the sources and destinations that run this application.
  - Create a custom signature and specify the SMTP fields that are different from normal SMTP use and patterns to identify when it is the custom application.**
  - Create an Application Override policy and specify the sources and destinations that run this application.
33. Which kind of update requires a disruption in connectivity?
- downloading the PAN-DB seed file
  - dynamic content
  - PAN-OS software**
  - WildFire subscription antivirus signatures
34. Which dedicated High Availability port is used for which plane?
- HA1 for the data plane, HA2 for the management plane
  - HA1 for the management plane, HA2 for the data plane**
  - MGT for the management plane; HA2 as a backup
  - MGT for the management plane, HA2 for the data plane

35. Which two protocols can AutoFocus use to retrieve log information from an NGFW? (Choose two.)
- a. syslog
  - b. Log transfer protocol, a Palo Alto Networks proprietary protocol
  - c. **HTTP**
  - d. **HTTPS**
  - e. SNMP
36. Palo Alto Networks publishes new applications at which approximate interval?
- a. every 30 minutes
  - b. hourly
  - c. daily
  - d. weekly**
37. Which type of device can receive the GlobalProtect data files content update?
- a. Log Collector
  - b. firewall**
  - c. WildFire
  - d. Antivirus
38. In which log will you see evidence that an administrator cannot log in to the firewall?
- a. Traffic
  - b. System**
  - c. Configuration
  - d. Authentication
39. How do you reboot the firewall from the command line?
- a. restart system
  - b. reboot
  - c. request restart system**
  - d. request reboot
40. Where in the user interface do you configure how many packets to capture when the extended-capture option is selected in an Anti-Spyware Profile or Vulnerability Profile?
- a. Device tab, as part of the Setup node**
  - b. Security Profiles, because the desired number of captured packets can vary between profiles

- c. as a default in the Device tab, as part of the Capture node. Then, exceptions can be configured in the Security Profiles
  - d. Configure Capturing options for each defined capture file
41. You are preparing a bootstrap template for use with a VM-Series firewall hosted in a public cloud. You do not need to include the Content-ID files because the firewall will download the latest version when it is booted anyway. How do you configure the bootstrap's content directory?
- a. **Create a content directory with an empty file named “download latest” and leave it empty.**
  - b. delete Content-ID files
  - c. rename Content-ID files to content-null
  - d. add an empty file to Content-ID files named no-download
42. Which format do you use for an AWS CloudFormation Template?
- a. XML
  - b. CSV
  - c. **JSON**
  - d. JSON or XML
43. In which order are Security policy rules from Panorama processed relative to local firewall policy rules?
- a. Local firewall policy rules are processed only during loss of Panorama connectivity.
  - b. All Panorama rules are processed first.
  - c. All local firewall policy rules are processed first.
  - d. **Some Panorama rules are processed before the firewall’s local rules, and some are processed after the local rules.**
44. Which statement is true about Security Profiles?
- a. They are evaluated from top down, with the first match processing the traffic.
  - b. They are applied to all inbound traffic when they are enabled.
  - c. **They enable a specific type of threat scanning (e.g., Virus, Spyware).**
  - d. They can specify actions based on the username.
45. Which Captive Portal authentication method can be handled by the browser without affecting the user experience?
- a. web-challenge
  - b. **browser-challenge**

- c. web-form
  - d. browser-form
46. The firewall of a defense contractor is not connected to the internet. However, it is connected to the classified SIPRNet. The contractor is concerned about getting malware files through that network. Can this defense contractor use the WildFire service for protection?
- a. **No, because there is no network path to the WildFire cloud.**
  - b. No, because all SIPRNet files are encrypted.
  - c. Yes, but only for PE-type file analysis.
  - d. Yes, it can use a WF-500 appliance.
47. How does the NGFW handle excess packets when there are QoS constraints?
- a. It buffers them until there is bandwidth to send them.
  - b. **It drops a percentage of them randomly.**
  - c. It replaces them with packets that tell the computer on the other side to slow down.
  - d. It sends a portion instead of the whole packet.
48. Which function is performed by the management plane?
- a. signature matching
  - b. VPN encryption
  - c. policy matching
  - d. **User-ID group lookups**
49. Which User-ID IP address-to-username mapping method can require user interaction?
- a. **Captive Portal**
  - b. monitoring Active Directory event logs
  - c. monitoring print server event logs
  - d. monitoring a Cisco WLAN controller
50. Which feature of the NGFW enables you to identify attempts to tunnel SSH over other ports?
- a. **App-ID**
  - b. Content-ID
  - c. User-ID
  - d. SSH Forward Proxy
51. What is the correct order of operations?

- a. check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security policy, check Security Profiles, re-encrypt traffic
- b. check allowed ports, decrypt (if traffic is encrypted and the policy specifies to decrypt it), check Security Profiles, check Security policy, re-encrypt traffic
- c. decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security policy, re-encrypt traffic
- d. decrypt (if traffic is encrypted and the policy specifies to decrypt it), check allowed ports, check Security Profiles, check Security policy, re-encrypt traffic

## Appendix D: Glossary

**Advanced Encryption Standard (AES):** A symmetric block cipher based on the Rijndael cipher.

**AES:** See Advanced Encryption Standard (AES).

**API:** See application programming interface (API).

**application programming interface (API):** A set of routines, protocols, and tools for building software applications and integrations.

**attack vector:** A path or tool that an attacker uses to target a network.

**BES:** See bulk electric system (BES).

**boot sector:** Contains machine code that is loaded into an endpoint's memory by firmware during the startup process, before the operating system is loaded.

**boot sector virus:** Targets the boot sector or master boot record (MBR) of an endpoint's storage drive or other removable storage media. See also *boot sector* and *master boot record (MBR)*.

**bot:** Individual endpoints that are infected with advanced malware that enables an attacker to take control of the compromised endpoint. Also known as a zombie. See also *botnet*.

**botnet:** A network of bots (often tens of thousands or more) working together under the control of attackers using numerous command and control (C2) servers. See also *bot*.

**bring your own apps (BYOA):** Closely related to BYOD, BYOA is a policy trend in which organizations permit end users to download, install, and use their own personal apps on mobile devices, primarily smartphones and tablets, for work-related purposes. See also *bring your own device (BYOD)*.

**bring your own device (BYOD):** A policy trend in which organizations permit end users to use their own personal devices, primarily smartphones and tablets, for work-related purposes. BYOD relieves organizations from the cost of providing equipment to employees but creates a management challenge due to the vast number and type of devices that must be supported. See also *bring your own apps (BYOA)*.

**bulk electric system (BES):** The large interconnected electrical system, consisting of generation and transmission facilities (among others), that comprises the "power grid."

**BYOA:** See bring your own apps (BYOA).

**BYOD:** See bring your own device (BYOD).

**child process:** In multitasking operating systems, a sub-process created by a parent process that is currently running on the system.

**CIP:** See Critical Infrastructure Protection (CIP).

**consumerization:** A computing trend that describes the process that occurs as end users increasingly find personal technology and apps that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use, than enterprise IT solutions.

**covered entity:** Defined by HIPAA as a healthcare provider that electronically transmits PHI (such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies), a health plan (such as a health insurance company, health maintenance organization, company health plan, or government program including Medicare, Medicaid, military and veterans' healthcare), or a healthcare clearinghouse. See also *Health Insurance Portability and Accountability Act (HIPAA)* and *protected health information (PHI)*.

**Critical Infrastructure Protection (CIP):** Cybersecurity standards defined by NERC to protect the physical and cyber assets necessary to operate the bulk electric system (BES). See also *bulk electric system (BES)* and *North American Electric Reliability Corporation (NERC)*.

**data encapsulation:** A process in which protocol information from the OSI layer immediately above is wrapped in the data section of the OSI layer immediately below. See also *open systems interconnection (OSI) reference model*.

**DDOS:** See distributed denial-of-service (DDOS).

**distributed denial-of-service (DDOS):** A type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make their network and systems (such as an e-commerce website or other web application) unavailable or unusable.

**EAP:** See extensible authentication protocol (EAP).

**EAP-TLS:** See extensible authentication protocol Transport Layer Security (EAP-TLS).

**EHR:** See electronic health record (EHR).

**electronic health record (EHR):** As defined by HealthIT.gov, an EHR “goes beyond the data collected in the provider’s office and include[s] a more comprehensive patient history. EHR data can be created, managed, and consulted by authorized providers and staff from across more than one healthcare organization.”

**electronic medical record (EMR):** As defined by HealthIT.gov, an EMR “contains the standard medical and clinical data gathered in one provider’s office.”

**EMR:** See electronic medical record (EMR).

**endpoint:** A computing device such as a desktop or laptop computer, handheld scanner, point-of-sale (POS) terminal, printer, satellite radio, security or videoconferencing camera, self-service kiosk, server, smart meter, smart TV, smartphone, tablet, or Voice over Internet Protocol (VoIP) phone. Although endpoints can include servers and network equipment, the term is generally used to describe end user devices.

**Enterprise 2.0:** A term introduced by Andrew McAfee and defined as “the use of emergent social software platforms within companies, or between companies and their partners or customers.” See also *Web 2.0*.

**exclusive or (XOR):** A Boolean operator in which the output is true only when the inputs are different (for example, TRUE and TRUE equals FALSE, but TRUE and FALSE equals TRUE).

**exploit:** A small piece of software code, part of a malformed data file, or a sequence (string) of commands, that leverages a vulnerability in a system or software, causing unintended or unanticipated behavior in the system or software.

**extensible authentication protocol (EAP):** A widely used authentication framework that includes approximately 40 different authentication methods.

**extensible authentication protocol Transport Layer Security (EAP-TLS):** An Internet Engineering Task Force (IETF) open standard that uses the Transport Layer Security (TLS) protocol in Wi-Fi networks and PPP connections. See also *point-to-point protocol (PPP)* and *Transport Layer Security (TLS)*.

**extensible markup language (XML):** A programming language specification that defines a set of rules for encoding documents in a human- and machine-readable format.

**false negative:** In anti-malware, malware that is incorrectly identified as a legitimate file or application. In intrusion detection, a threat that is incorrectly identified as legitimate traffic. See also *false positive*.

**false positive:** In anti-malware, a legitimate file or application that is incorrectly identified as malware. In intrusion detection, legitimate traffic that is incorrectly identified as a threat. See also *false negative*.

**favicon (“favorite icon”):** A small file containing one or more small icons associated with a particular website or webpage.

**Federal Information Security Management Act (FISMA):** See *Federal Information Security Modernization Act (FISMA)*.

**Federal Information Security Modernization Act (FISMA):** A U.S. law that implements a comprehensive framework to protect information systems used in U.S. federal government agencies. Known as the Federal Information Security Management Act prior to 2014. Financial Services Modernization Act of 1999: See *Gramm-Leach-Bliley Act (GLBA)*.

**FISMA:** See Federal Information Security Modernization Act (FISMA).

**floppy disk:** A removable magnetic storage medium commonly used from the mid-1970s until approximately 2007, when they were largely replaced by removable USB storage devices.

**generic routing encapsulation (GRE):** A tunneling protocol developed by Cisco Systems® that can encapsulate various network layer protocols inside virtual point-to-point links.

**GLBA:** See Gramm-Leach-Bliley Act (GLBA).

**Gramm-Leach-Bliley Act (GLBA):** A U.S. law that requires financial institutions to implement privacy and information security policies to safeguard the non-public personal information of clients and consumers. Also known as the Financial Services Modernization Act of 1999.

**GRE:** See generic routing encapsulation (GRE).

**hacker:** Originally used to refer to anyone with highly specialized computing skills, without connoting good or bad purposes. However, common misuse of the term has redefined a hacker as someone that circumvents computer security with malicious intent, such as a cybercriminal, cyberterrorist, or hacktivist.

**hash signature:** A cryptographic representation of an entire file or program’s source code.

**Health Insurance Portability and Accountability Act (HIPAA):** A U.S. law that defines data privacy and security requirements to protect individuals' medical records and other personal health information. See also *covered entity* and *protected health information (PHI)*.

**heap spraying:** A technique used to facilitate arbitrary code execution by injecting a certain sequence of bytes into the memory of a target process.

**HIPAA:** See Health Insurance Portability and Accountability Act (HIPAA).

**indicator of compromise (IOC):** A network or operating system (OS) artifact that provides a high level of confidence that a computer security incident has occurred.

**initialization vector (IV):** A random number used only once in a session, in conjunction with an encryption key, to protect data confidentiality. Also known as a nonce.

**IOC:** See indicator of compromise (IOC).

**IV:** See initialization vector (IV).

**jailbreaking:** Hacking an Apple® iOS device to gain root-level access to the device. This is sometimes done by end users to allow them to download and install mobile apps without paying for them, from sources, other than the App Store®, that are not sanctioned and/or controlled by Apple®. Jailbreaking bypasses the security features of the device by replacing the firmware's operating system with a similar, albeit counterfeit version, which makes it vulnerable to malware and exploits. See also *rooting*.

**least privilege:** A network security principle in which only the permission or access rights necessary to perform an authorized task are granted.

**malware:** Malicious software or code that typically damages, takes control of, or collects information from an infected endpoint. Malware broadly includes viruses, worms, Trojan horses (including Remote Access Trojans, or RATs), anti-AV, logic bombs, backdoors, rootkits, bootkits, spyware, and (to a lesser extent) adware.

**master boot record (MBR):** Contains information about how the logical partitions (or file systems) are organized on the storage media, and an executable boot loader that starts up the installed operating system.

**MBR:** See master boot record (MBR).

**metamorphism:** A programming technique used to alter malware code with every iteration, to avoid detection by signature-based anti-malware software. Although the malware payload changes with each iteration – for example, by using a different code structure or sequence, or inserting garbage code to change the file size – the fundamental behavior of the malware payload remains unchanged.

Metamorphism uses more advanced techniques than polymorphism. See also *polymorphism*.

**Microsoft Challenge-handshake authentication protocol (MS-CHAP):** A protocol used to authenticate Microsoft Windows-based workstation, using a challenge-response mechanism to authenticate PPTP connections without sending passwords.

**MS-CHAP:** See Microsoft Challenge-handshake authentication protocol (MS-CHAP).

**mutex:** A program object that allows multiple program threads to share the same resource, such as file access, but not simultaneously.

**NERC:** See North American Electric Reliability Corporation (NERC).

**Network and Information Security (NIS) Directive:** A European Union (EU) directive that imposes network and information security requirements – to be enacted by national laws across the EU within two years of adoption in 2016 – for banks, energy companies, healthcare providers and digital service providers, among others.

**NIS:** See Network and Information Security (NIS) Directive.

**nonce:** See initialization vector (IV).

**North American Electric Reliability Corporation (NERC):** A not-for-profit international regulatory authority responsible for assuring the reliability of the bulk electric system (BES) in the continental U.S., Canada, and the northern portion of Baja California, Mexico. See also *bulk electric system (BES)* and *Critical Infrastructure Protection (CIP)*.

**obfuscation:** A programming technique used to render code unreadable. It can be implemented using a simple substitution cipher, such as an *exclusive or* (XOR) operation, or more sophisticated encryption algorithms, such as the *Advanced Encryption Standard* (AES). See also *Advanced Encryption Standard (AES)*, *exclusive or (XOR)*, and *packer*.

**one-way (hash) function:** A mathematical function that creates a unique representation (a hash value) of a larger set of data in a manner that is easy to compute in one direction (input to output), but not in the

reverse direction (output to input). The hash function cannot recover the original text from the hash value. However, an attacker could attempt to guess what the original text was and see if it produces a matching hash value.

**open systems interconnection (OSI) reference model:** Defines standard protocols for communication and interoperability using a layered approach in which data is passed from the highest layer (application) downward through each layer to the lowest layer (physical), then transmitted across the network to its destination, then passed upward from the lowest layer to the highest layer. See also *data encapsulation*.

**OSI model:** See open systems interconnection (OSI) reference model.

**packer:** A software tool that can be used to obfuscate code by compressing a malware program for delivery, then decompressing it in memory at run time. See also *obfuscation*.

**packet capture (PCAP):** A traffic intercept of data packets that can be used for analysis.

**PAP:** See password authentication protocol (PAP).

**password authentication protocol (PAP):** An authentication protocol used by PPP to validate users with an unencrypted password. See also *point-to-point protocol (PPP)*.

**Payment Card Industry Data Security Standards (PCI DSS):** A proprietary information security standard mandated and administered by the PCI Security Standards Council (SSC), and applicable to any organization that transmits, processes, or stores payment card (such as debit and credit cards) information. See also *PCI Security Standards Council (SSC)*.

**PCAP:** See packet capture (PCAP).

**PCI:** See Payment Card Industry Data Security Standards (PCI DSS).

**PCI DSS:** See Payment Card Industry Data Security Standards (PCI DSS).

**PCI Security Standards Council (SSC):** Comprised of Visa, MasterCard, American Express, Discover, and JCB, the SSC maintains, evolves, and promotes PCI DSS. See also *Payment Card Industry Data Security Standards (PCI DSS)*.

**Personal Information Protection and Electronic Documents Act (PIPEDA):** A Canadian privacy law that defines individual rights with respect to the privacy of their personal information, and governs how private sector organizations collect, use, and disclose personal information during business.

**Personally Identifiable Information:** Defined by the U.S. National Institute of Standards and Technology (NIST) as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity... and (2) any other information that is linked or linkable to an individual....”

**PHI:** See protected health information (PHI).

**PIPEDA:** See Personal Information Protection and Electronic Documents Act (PIPEDA).

**PKI:** See public key infrastructure (PKI).

**point-to-point protocol (PPP):** A Layer 2 (data link) protocol layer used to establish a direct connection between two nodes.

**polymorphism:** A programming technique used to alter a part of malware code with every iteration, to avoid detection by signature-based anti-malware software. For example, an encryption key or decryption routine may change with every iteration, but the malware payload remains unchanged. See also *metamorphism*.

**PPP:** See point-to-point protocol (PPP).

**pre-shared key (PSK):** A shared secret, used in symmetric key cryptography which has been exchanged between two parties communicating over an encrypted channel.

**promiscuous mode:** Refers to Ethernet hardware used in computer networking, typically a network interface card (NIC), that receives all traffic on a network segment, even if the traffic is not addressed to the hardware.

**protected health information (PHI):** Defined by HIPAA as information about an individual’s health status, provision of healthcare, or payment for healthcare that includes identifiers such as names, geographic identifiers (smaller than a state), dates, phone and fax numbers, email addresses, Social Security numbers, medical record numbers, or photographs, among others. See also *Health Insurance Portability and Accountability Act (HIPAA)*.

**public key infrastructure (PKI):** A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption.

**QoS:** See Quality of Service (QoS).

**Quality of Service (QoS):** The overall performance of specific applications or services on a network including error rate, bit rate, throughput, transmission delay, availability, jitter, etc. QoS policies can be configured on certain network and security devices to prioritize certain traffic, such as voice or video, over other, less performance-intensive traffic, such as file transfers.

**RADIUS:** See Remote Authentication Dial-In User Service (RADIUS).

**rainbow table:** A pre-computed table used to find the original value of a cryptographic hash function.

**Remote Authentication Dial-In User Service (RADIUS):** A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize access to a system or service.

**remote procedure call (RPC):** An inter-process communication (IPC) protocol that enables an application to be run on a different computer or network, rather than the local computer on which it is installed.

**representational state transfer (REST):** An architectural programming style that typically runs over HTTP, and is commonly used for mobile apps, social networking websites, and mashup tools.

**REST:** See representational state transfer (REST).

**rooting:** The Google Android equivalent of jailbreaking. See jailbreaking.

**RPC:** See remote procedure call (RPC). **SaaS:** See Software as a Service (SaaS).

**salt:** Randomly generated data that is used as an additional input to a one-way hash function that hashes a password or passphrase. The same original text hashed with different salts results in different hash values.

**Sarbanes-Oxley (SOX) Act:** A U.S. law that increases financial governance and accountability in publicly traded companies.

**script kiddie:** Someone with limited hacking and/or programming skills that uses malicious programs (malware) written by others to attack a computer or network.

**Secure Sockets Layer (SSL):** A cryptographic protocol for managing authentication and encrypted communication between a client and server to protect the confidentiality and integrity of data exchanged in the session.

**service set identifier (SSID):** A case sensitive, 32-character alphanumeric identifier that uniquely identifies a Wi-Fi network.

**Software as a Service (SaaS):** A cloud computing service model, defined by the U.S. National Institute of Standards and Technology (NIST), in which “the capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.”

**SOX:** See Sarbanes-Oxley (SOX) Act.

**spear phishing:** A highly targeted phishing attack that uses specific information about the target to make the phishing attempt appear legitimate.

**SSID:** See service set identifier (SSID).

**SSL:** See Secure Sockets Layer (SSL).

**STIX:** See structured threat information expression (STIX).

**structured threat information expression (STIX):** An XML format for conveying data about cybersecurity threats in a standardized format. See also extensible markup language (XML).

**threat vector:** See attack vector.

**TLS:** See Transport Layer Security (TLS).

**Tor (“The Onion Router”):** Software that enables anonymous communication over the internet.

**Transport Layer Security (TLS):** The successor to SSL (although it is still commonly referred to as SSL). See also Secure Sockets Layer (SSL).

**uniform resource locator (URL):** A unique reference (or address) to an internet resource, such as a webpage.

**URL:** See uniform resource locator (URL).

**vulnerability:** A bug or flaw that exists in a system or software and creates a security risk.

**Web 2.0:** A term popularized by Tim O'Reilly and Dale Dougherty, unofficially referring to a new era of the World Wide Web, which is characterized by dynamic or user-generated content, interaction, and collaboration, and the growth of social media. See also Enterprise 2.0.

**XML:** See extensible markup language (XML).

**XOR:** See exclusive or (XOR).

**zero-day threat:** The window of vulnerability that exists from the time a new (unknown) threat is released until security vendors release a signature file or security patch for the threat.

**zombie:** See bot.

# Continuing Your Learning Journey with Palo Alto Networks

Training from Palo Alto Networks and our Authorized Training Partners delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications give you the Palo Alto Networks product portfolio knowledge necessary to prevent successful cyberattacks and to safely enable applications.

## Digital Learning

For those of you who want to keep up to date on our technology, a learning library of *free* digital learning is available. These on-demand, self-paced digital learning classes are a helpful way to reinforce the key information for those who have been to the formal hands-on classes. They also serve as a useful overview and introduction to working with our technology for those unable to travel to a hands-on, instructor-led class.

Simply register in our Learning Center and you will be given access to our digital learning portfolio. These online classes cover foundational material and contain narrated slides, knowledge checks, and, where applicable, demos for you to access.

New courses are being added often, so check back to see new curriculum available.

## Instructor-Led Training

Looking for a hands-on, instructor-led course in your area?

Palo Alto Networks Authorized Training Partners (ATPs) are located globally and offer a breadth of solutions from onsite training to public, open environment classes. About 42 authorized training centers are delivering online courses in 14 languages and at convenient times for most major markets worldwide. For class schedule, location, and training offerings, see:

<https://www.paloaltonetworks.com/services/education/atc-locations>

## Learning Through the Community

You also can learn from peers and other experts in the field. Check out our community site <https://live.paloaltonetworks.com>, where you can:

- Discover reference material
- Learn best practices
- Learn what is trending