

#####
#####

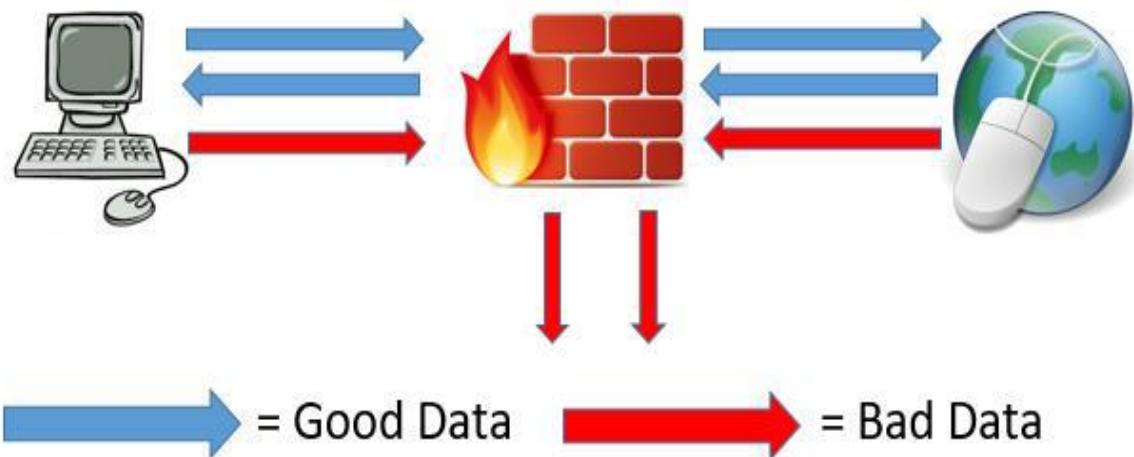
Day 01

!

1. What is Firewall?
 2. State Full Inspection
 3. Palo Alto Firewall History
 4. PAN OS and PAN H/W and VM Series
 5. SP3
 6. Packet Flow
 7. Initial Access
-
-

What is Firewall?

A firewall is security devices used to stop or mitigate unauthorized access. The only traffic allowed on the network is defined via firewall policies. Firewall is placed between a trusted network and an untrusted network. Firewall grants or rejects access to traffic flows between untrusted & trusted zone. A firewall inspect incoming and outgoing network related traffic.





Check Point
SOFTWARE TECHNOLOGIES LTD.

State Full Inspection:

In State full Inspection firewall create the state table (conn table) on the basis of source IP, source port, destination IP, destination port, protocol number and ingress zone. When firewall receive subsequent request and reply packet for a flow then It will perform the lookup and session table if session information is available in that case it will bypass the session setup stage and it will process the packet in fast path.

The screenshot shows the Palo Alto Networks Firewall interface under the 'Monitor' tab. On the left, there's a navigation sidebar with various monitoring and threat detection modules like Logs, Traffic, Threat, and Session Browser. The 'Session Browser' module is highlighted with a red box. The main pane displays a table titled 'Click Here' with the following data:

Start Time	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule	Ingress I/F	Egress I/F	Bytes	Virtual System
09/30 18:08:27	Trusted Zone	Untrusted Zone	10.1.1.11	10.9.15.66	56816	443	6	ssl	Internet	ethernet1/2	ethernet1/1	479603	vsys1
10/02 15:27:38	Trusted Zone	Untrusted Zone	10.1.1.11	2.90.116.68	52824	32863	17	bit torrent	Internet	ethernet1/2	ethernet1/1	186	vsys1
10/02 15:12:41	Trusted Zone	Untrusted Zone	10.1.1.11	82.221.103.2...	52824	6881	17	bit torrent	Internet	ethernet1/2	ethernet1/1	159	vsys1
10/02 14:50:09	Trusted Zone	Trusted Zone	10.1.1.11	10.1.1.1	54300	22	6	ssh	Same Security Traffic	ethernet1/2	ethernet1/2	138700	vsys1
10/02 15:10:51	Trusted Zone	Untrusted Zone	10.1.1.11	62.150.174.1...	52824	28930	17	bit torrent	Internet	ethernet1/2	ethernet1/1	1829	vsys1
10/02 15:05:35	Trusted Zone	Untrusted Zone	10.1.1.11	89.216.166.2...	52824	18464	17	bit torrent	Internet	ethernet1/2	ethernet1/1	372	vsys1
10/02 15:27:46	Trusted Zone	Untrusted Zone	10.1.1.11	60.54.120.235	55067	1500	6	undecided	Internet	ethernet1/2	ethernet1/1	62	vsys1
10/02 15:12:45	Trusted Zone	Untrusted Zone	10.1.1.11	95.111.65.180	52824	62529	17	bit torrent	Internet	ethernet1/2	ethernet1/1	159	vsys1
10/02 15:17:54	Trusted Zone	Untrusted Zone	10.1.1.11	86.127.46.5	52824	20015	17	bit torrent	Internet	ethernet1/2	ethernet1/1	159	vsys1
10/02 15:16:52	Trusted	Untrusted	10.1.1.11	41.225.226.1...	52824	63785	17	bit torrent	Internet	ethernet1/2	ethernet1/1	186	vsys1

> show session all

> show session id <id number>

```

admin@PA-5060> show session id 2359361

Session          2359361

    c2s flow:
        source:      192.168.42.132 [Trust]
        dst:         8.8.8.8
        proto:       17
        sport:       1078
        dport:       53
        state:       ACTIVE
        type:        FLOW
        src user:   unknown
        dst user:   unknown

    s2c flow:
        source:      8.8.8.8 [Untrust]
        dst:         172.24.12.42
        proto:       17
        sport:       53
        dport:       47075
        state:       ACTIVE
        type:        FLOW
        src user:   unknown
        dst user:   unknown

        start time           : Sun Mar 17 09:18:29 2013
        timeout              : 30 sec
        time to live         : 2 sec
        total byte count(c2s) : 5474
        total byte count(s2c) : 9290
        layer7 packet count(c2s) : 59
        layer7 packet count(s2c) : 59
        vsys                 : vsys1
        application          : dns
        rule                 : Test-Rule
        session to be logged at end : True
        session in session ager   : True

```

PAN OS and PAN H/W and VM Series:

1. Physical devices:

PA-220, PA-800, PA-3200, PA-5200 – Next Gen hardware.

PA-7050 and PA-7080 are Chassis architecture

2. Virtual devices:

VM-700, VM-500, VM-300, VM-100, VM-50, VM-50 lite

Supported environment:

ESXi: All

KVM/Openstack: All

Hyper-V: All

VMWare NSX: VM100-500

AWS: VM100-700

Azure: VM100-700

!

IPsec throughput, all models: Varies according to model (originally was 250mbps, per the training, however documentation states otherwise. Please see the hardware spec sheet at the top of this post for specifics)

!

Virtual Systems

Ability to have separate virtual firewalls in a single physical chassis

Each system has its own zones, policies, administrators.

Supported on the 3k/5k/7k models

Hardware Platforms

- PA-200, PA-500, PA-2000 Series (EoS), PA-3000 Series, PA-4000 Series (EoS), PA-5000 Series, PA-7050, PA-7080
- Nearly every feature is supported on every platform
- Compare capacities at:
<https://www.paloaltonetworks.com/products/product-selection.html>



Virtual Platforms

- Ideal for protecting virtualized data centers and “East-West” traffic
- VMware, KVM, Citrix SDX, and Amazon AWS

	VM-1000-HV	VM-300	VM-200	VM-100
Firewall Throughput (App-ID)	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Threat Prevention Throughput	600 Mbps	600 Mbps	600 Mbps	600 Mbps
Connections per Second	8,000	8,000	8,000	8,000
Max Sessions	250,000	250,000	100,00	50,000

!

PAN OS:

Palo Alto Operating System is known as PAN-OS. PAN-OS based on Linux kernel. Palo Alto coded on top of free BSD similar to Juniper firewall. Latest PAN-OS version is 10.x.

!

SP3 (Single Pass Software and Parallel Processing Hardware):

The Palo Alto Networks firewall allows you to specify security policies based on a more accurate identification of each application seeking access to your network. Unlike traditional firewalls that identify applications only by protocol and port number, the firewall uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port, and to identify potentially malicious applications that use nonstandard ports.

The strength of the Palo Alto Networks firewall is its Single Pass Parallel Processing™ (SP3) engine. Each of the current protection features in the device (Anti-Virus, Spyware, Data Filtering and vulnerability protection) utilize the same stream-based signature format. As a result, the SP3 engine can search for all of these risks simultaneously.

The advantage of providing a stream-based engine is that the traffic is scanned as it crosses the box with a minimal amount of buffering. This speed allows you to turn on advanced features like scanning for viruses and malware without slowing down the firewall’s performance.

Palo Alto Networks offers processors dedicated to specific security functions that work in parallel.

On the higher end hardware models, the Data Plane contains three types of FPGA processors that are connected by high-speed 1 Gbps busses:

- Signature Match Processor: Performs vulnerability and virus detection
- Security Processors: Multicore processors that handle security tasks such as SSL decryption
- Network Processor: Responsible for routing, NAT, and network layer communication

On the higher-end hardware models, the control plane has its own dual core processor, RAM, and hard drive. This processor is responsible for tasks such as management UI, logging, and route updates.

Single-Pass Architecture

Per-Packet Operations:

Traffic Classification with App-ID

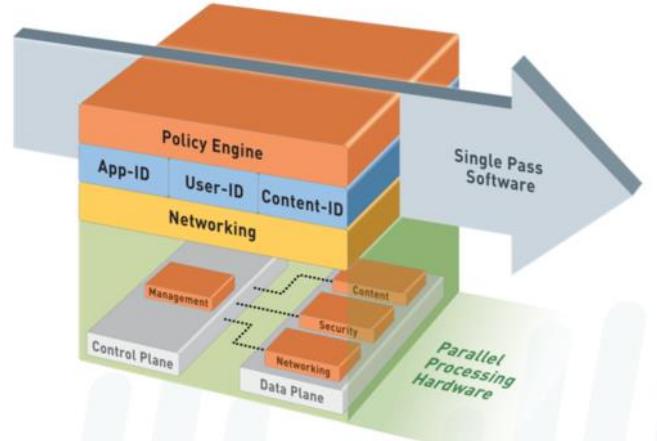
User/group mapping

Content Scan (threats, URL, confidential data)

Palo Alto Networks Single Pass Architecture

Single Pass

- Operations per packet
 - Traffic classification with App-ID
 - User/group mapping
 - Content scanning – threats, URLs, confidential data
- One policy



Parallel Processing

- Function-specific parallel processing hardware engines
- Separate data/control planes

Parallel Processing

Function specific parallel processing hardware engine

Separate data/control plane

PAN is a single-pass Parallel Processing system.

Data plane:

Signature Matching: IPS, virus, spyware, CC#, SSN

Security Processing: App-ID, User-ID, URL Match, Policy Match, App Decoding, SSL/IPsec, decompression

Network Processing: Flow Control, Route Lookup, MAC lookup, QoS, NAT

Control Plane:

Management: Configuration, Management UI, Logging, Reporting

Zero Trust Security Model

No trust provided by default

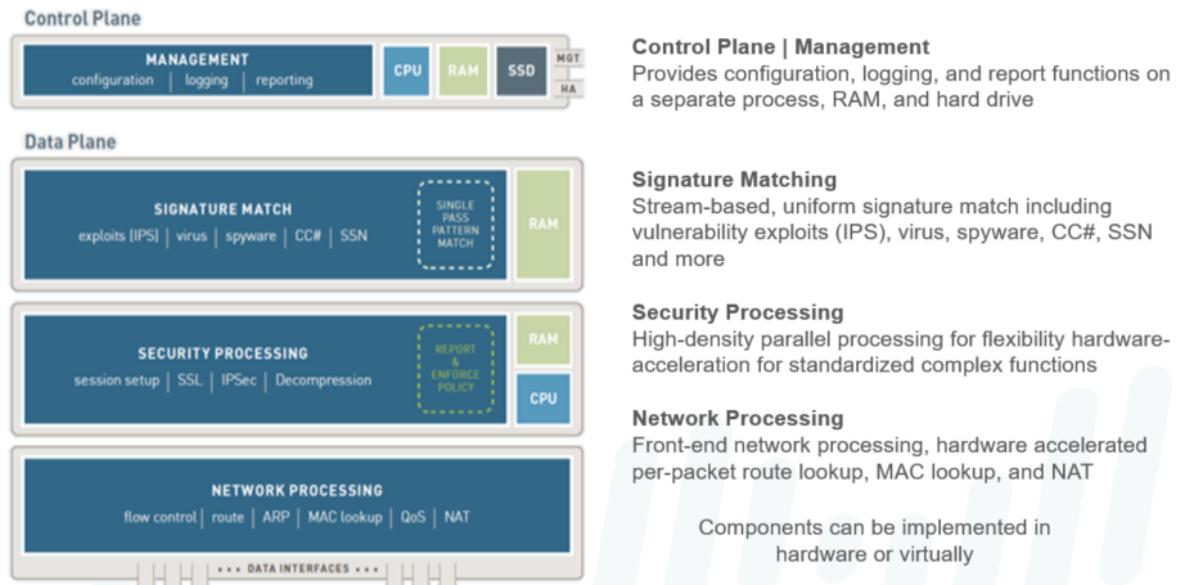
Never Trust, always verify

Need to establish trust boundaries

NGFW offer several options to help approach the zero-trust model:

App-ID, User-ID, URL filtering, Vulnerability filtering, anti-spyware, anti-virus, Traps, file blocking, DOS protection, Zone Protection, Wildfire

Palo Alto Networks Firewall Architecture



Packet Flow:

SECTION 1: OVERVIEW

SECTION 2: INGRESS STAGE

2.1 PACKET PARSING

2.2 TUNNEL DECAPSULATION

2.3 IP DEFRAAGMENTATION

SECTION 3: FIREWALL SESSION LOOKUP

3.1. ZONE PROTECTION CHECKS

3.2. TCP STATE CHECK

3.3. FORWARDING SETUP

3.4. NAT POLICY LOOKUP

3.5. USER- ID

3.6. SECURITY POLICY LOOKUP

3.7. DOS PROTECTION POLICY LOOKUP

3.8. SESSION ALLOCATION

SECTION 4: FIREWALL SESSION FAST PATH

SECURITY PROCESSING

CAPTIVE PORTAL

SECTION 5: APPLICATION IDENTIFICATION (APP - ID)

SECTION 6: CONTENT INSPECTION

SECTION 7: FORWARDING/EGRESS

SECTION 8: SUMMARY

Ingress State:

The ingress stage receives packets from the network interface, parses those packets,

And then determines whether a given packet is subject to further inspection. If the

Packet is subject to further inspection, the firewall continues with a session lookup and

The packet enters the security processing stage. Otherwise, the firewall forwards the

Packet to the egress stage. Section 3 summarizes cases when the firewall forwards

Packets without inspection, depending on the packet type and the operational mode of

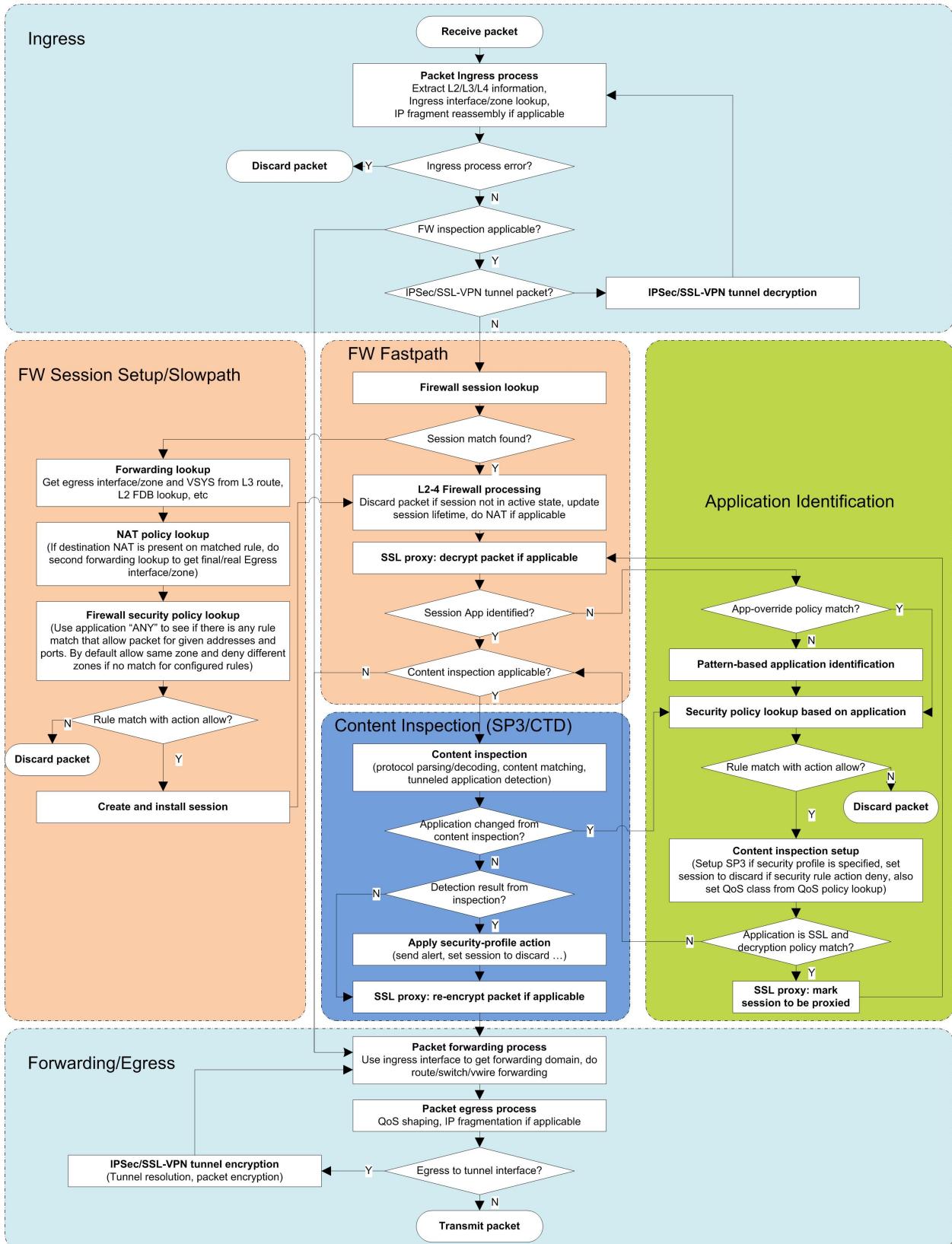
The interface.

Note: During packet processing, the firewall may discard a packet because of a protocol

Violation. In certain cases, due to firewall attack prevention features, it discards packets

Without configurable options. Section 2.1 enumerates such cases when the firewall

Discards packets at this stage.



Packet parsing starts with the Ethernet (Layer-2) header of the packet received from The wire.

The ingress port, 802.1q tag, and destination MAC address are used as keys to lookup The ingress logical interface. If the interface is not found, the packet is discarded. The Hardware interface counter "receive error" and global counter "flow_rcv_dot1q_tag_err" are incremented.

Next, the IP header is parsed (Layer-3).

IPv4: The firewall will discard the packet for any one of the following reasons:

!

- Mismatch of Ethernet type and IP version
- Truncated IP header
- IP protocol number 0
- TTL zero
- Land attack
- Ping of death
- Martian IP address
- IP checksum errors

IPv6: The firewall will discard the packet for any one of the following reasons:

- Mismatch of Ethernet type and IP version
- Truncated IPv6 header
- Truncated IP packet (IP payload buffer length less than IP payload field)
- Jumbo Gram extension (RFC 2675)
- Truncated extension header

Next, the Layer-4 (TCP/UDP) header is parsed, if applicable.

TCP: The firewall will discard the packet for any one of the following reasons:

- TCP header is truncated,
- Data-offset field is less than 5
- Checksum error
- Port is zero

- Invalid combination of TCP flags

!

UDP:

The firewall will discard the packet for any one of the following reasons:

- UDP header truncated
- UDP payload truncated (not IP fragment and UDP buffer length less than UDP length field)
- Checksum error

!

2.2 Tunnel Decapsulation

The firewall performs decapsulation/decryption at the parsing stage. After parsing

The packet, if the firewall determines that it matches a tunnel, i.e. IPsec, SSL-VPN

With SSL transport, then it performs the following sequence:

1. The firewall decapsulates the packet first and discards it if errors exist.
2. The tunnel interface associated with the tunnel is assigned to the packet as

Its new ingress interface and then the packet is fed back through the parsing

Process, starting with the packet header defined by the tunnel type. Currently,

The supported tunnel types are IP layer tunneling, thus packet parsing (for a

Tunneled packet) starts with the IP header.

!

2.3 IP Defragmentation

The firewall parses IP fragments, reassembles using the defragmentation process, and

Then feeds the packet back to the parser starting with the IP header. At this stage, a

Fragment may be discarded due to tear-drop attack (overlapping fragments),

Fragmentation errors, or if the firewall hits system limits on buffered fragments (hits

The max packet threshold).

Section 3: Firewall Session Lookup

A packet is subject to firewall processing depending on the packet type and the

Interface mode. The following table summarizes the packet processing behavior for a

Given interface operation mode and packet type:

Packet Type	Interface operational modes			
	Layer-3	Layer-2	Virtual-Wire	Tap
IPv4 unicast	inspect & forward	inspect & forward	inspect & forward	inspect & drop
IPv4 Multicast (224.0.0.1-239.255.255.255)	inspect & forward	forward only (flood)	forward, but inspect only if multicast firewalling is on	inspect & drop
IP broadcast (255.255.255.255)	drop	forward only (flood)	forward, but inspect only if multicast firewalling is on	drop
IP local broadcast	drop	forward only (flood)	forward, but inspect only if multicast firewalling is on	drop
IPv6	inspect and forward if enabled	forward, but inspect only if IPv6 firewalling is on (default)	forward, but inspect only if IPv6 firewalling is on (default)	drop, but inspect only if IPv6 firewalling is on (default)
Non-IP	process if applicable, not forward	forward only	forward only	drop

If the packet is subject to firewall inspection, it performs a flow lookup on the packet. A

Firewall session consists of two unidirectional flows, each uniquely identified. In

PAN-OS's implementation, the firewall identifies the flow using a 6-tuple key.

- Source and destination addresses: IP addresses from the IP packet.
- Source and destination ports: Port numbers from TCP/UDP protocol headers.

For non-TCP/UDP, different protocol fields are used (e.g. for ICMP the ICMP

Identifier and sequence numbers are used, for IPsec terminating on device the

Security Parameter Index (SPI) is used, and for unknown, a constant reserved

Value is used to skip Layer-4 match).

- Protocol: The IP protocol number from the IP header is used to derive the flow Key.

- Security zone: This field is derived from the ingress interface at which a packet Arrives.

The firewall stores active flows in the flow lookup table. When a packet is determined to

Be eligible for firewall inspection, the firewall extracts the 6-tuple flow key from the

Packet and then performs a flow lookup to match the packet with an existing flow. Each

Flow has a client and server component, where the client is the sender of the first

Packet of the session from firewall's perspective, and the server is the receiver of this

First packet.

Note: The distinction of client and server is from the firewall's point of view and may or may not be the same from the end hosts' point of view.

Based on the above definition of client and server, there will be a client-to-server (C2S) and server-to-client (S2C) flow, where all client-to-server packets should contain the same key as that of the C2S flow, and so on for the S2C flow.

3.1 Firewall Session Setup

The firewall performs the following steps to set up a firewall session:

3.2. Zone Protection Checks

After the packet arrives on a firewall interface, the ingress interface information is used to determine the ingress zone. If any zone protection profiles exist for that zone, the packet is subject to evaluation based on the profile configuration.

3.3. TCP State Check

If the first packet in a session is a TCP packet and it does not have the SYN bit set, the firewall discards it (default).

If SYN flood settings are configured in the zone protection profile and action is set to SYN Cookies, then TCP SYN cookie is triggered if the number of SYN matches the activate threshold. SYN cookie implementation functions as follows:

- The seed to encode the cookie is generated via random number generator

Each time the data plane boots up.

- If an ACK packet received from the client does not match cookie encoding,

It treats the packet as non-SYN packet.

- A session that passes SYN cookie's process is subject to TCP sequence

Number translation because the firewall acted as a proxy for TCP 3-way handshake.

If the SYN Flood protection action is set to Random Early Drop (RED) instead, which is the default, then the firewall simply drops any SYN messages that are received

After hitting the threshold. SYN Cookies is preferred when you want to permit more legitimate traffic to pass through while being able to distinguish SYN flood packets and drop those instead. RED, on the other hand, will drop SYN packets randomly and

can impact legitimate traffic equally.

Note: You can configure the firewall to allow the first TCP packet, even if it does not have SYN bit set. Altering the default behavior and allowing non-SYN TCP packets through poses a security risk by opening up the Firewall to malicious packets not part of a valid TCP connection sequence. Although this is not a recommended setting, it might be required for scenarios with asymmetric flows.

You should configure the firewall to reject TCP non-SYN when SYN cookies are enabled.

3.4. Forwarding Setup

This stage determines the packet-forwarding path. Packet forwarding depends on the configuration of the interface. The following table summarizes the packet-forwarding behavior:

Interface Mode	Forwarding action
Tap	Egress interface/zone is the same as the ingress interface/zone from a policy perspective. The firewall discards the packet.
Virtual Wire	Egress interface is the peer interface configured in the virtual wire
Layer-2	Egress interface for the destination MAC is retrieved from the MAC table. If the information is not present, the frame is flooded to all interfaces in the associated VLAN broadcast domain, except for the ingress interface.
Layer-3	The firewall uses the route lookup table to determine the next hop, or discards the packet if there is no match.

3.5. NAT Policy Lookup

This is applicable only in Layer-3 or Virtual Wire mode. At this stage, the ingress and egress zone information is available. The firewall evaluates NAT rules for the original packet.

- For destination NAT, the firewall performs a second route lookup for the translated address to determine the egress interface/zone.
- For source NAT, the firewall evaluates the NAT rule for source IP allocation. If the allocation check fails, the firewall discards the packet.

3.6. User-ID

The firewall uses the IP address of the packet to query the User-IP mapping table (maintained per VSYS). The corresponding user information is fetched. The firewall next takes this user information to query the user-group mapping table and fetches the group mapping associated with this user (it returns all groups the user belongs to).

There is a chance that user information is not available at this point. In that case, if captive portal policy is setup, the firewall will attempt to find out the user information via captive portal authentication (discussed in Section 4).

3.7. Security Policy Lookup

At this stage, the ingress and egress zone information is available. The firewall uses application ANY to perform the lookup and check for a rule match. In case of a rule match, if the policy action is set to 'deny', the firewall drops the packet. The firewall denies the traffic if there is no security rule match. The firewall permits intra-zone traffic by default. You can modify this default behavior for intra-zone and inter-zone traffic from the security policies rulebase.

Note: The firewall applies security rules to the contents of the original packet, even if there are NAT rules configured.

3.8. DoS Protection Policy Lookup

Next, the firewall checks the DoS (Denial of Service) protection policy for traffic thresholds based on the DoS protection profile.

If the DoS protection policy action is set to "Protect", the firewall checks the specified thresholds and if there is a match (DoS attack detected), it discards the packet.

If the policy action is either allow or deny, the action takes precedence regardless of threshold limits set in the DoS profile.

3.9.Session Allocation

The firewall allocates a new session entry from the free pool after all of the above steps are successfully completed. Session allocation failure may occur at this point due to resource constraints:

- VSYS session maximum reached, or
- The firewall allocates all available sessions.

After the session allocation is successful:

- The firewall fills session content with flow keys extracted from the packet and the forwarding/policy results.
- Session state changes from INIT (pre-allocation) to OPENING (post-allocation).
- If the application has not been identified, the session timeout values are set to default value of the transport protocol. You can configure these global timeout values from the Firewall's device settings. Application specific timeout values override the global settings, and will be the effective timeout values for the session once application is identified.

After setup, session installation takes place:

- Firewall queries the flow lookup table to see if a match exists for the flow keys matching the session. If a flow lookup match is found (session with same tuple already exists), then this session instance is discarded as session already exists, else
- Session is added to the flow lookup table for both C2S and S2C flows and firewall changes the session's state from OPENING to ACTIVE.

The firewall then sends the packet into Session Fast Path phase for security

Section 4: Firewall Session Fast Path

A packet that matches an existing session will enter the fast path. This stage starts with Layer-2 to Layer-4 firewall processing:

- If the session is in discard state, then the firewall discards the packet. The firewall can mark a session as being in the discard state due to a policy action change to deny, or threat detection.
- If the session is active, refresh session timeout.
- If the packet is a TCP FIN/RST, the session TCP half closed timer is started if this is the first FIN packet received (half closed session) or the TCP Time Wait timer is started if this is the second FIN packet or RST packet. The session is closed as soon as either of these timers expire.
- If NAT is applicable, translate the L3/L4 header as applicable.

If an application uses TCP as the transport, the firewall processes it by the TCP reassembly module before it sends the data stream into the security-processing module. The TCP reassembly module will also perform window check, buffer out-of-order data while skipping TCP retransmission. The firewall drops the packets if there is a reassembly error or if it receives too many out-of-order fragments, resulting in the reassembly buffers filling up.

4.1. Security Processing

A packet matching an existing session is subject to further processing (application identification and/or content inspection) if packet has TCP/UDP data (payload), or it is a non-TCP/UDP packet.

If the firewall does not detect the session application, it performs an App-ID lookup. If App-ID lookup is non-conclusive, the content inspection module runs known protocol decoder checks and heuristics to help identify the application.

If the firewall detects the application, the session is subject to content inspection if any of the following apply:

- Application Layer Gateway (ALG) is involved.
- Application is tunneled application.
- Security rule has security profile associated.

The Application Identification (App-ID) and Content Inspection stages are discussed in detail in later sections (Section 5 and 6).

4.2. Captive Portal

If the user information was not available for the source IP address extracted from the packet, and the packet is destined to TCP/80, the firewall performs a captive portal rule lookup to see if the packet is subject to captive portal authentication. If captive portal is applicable, the packet is redirected to the captive portal daemon.

Note: Since captive portal is applicable to http traffic and also supports a URL category based policy lookup, this can be kicked in only after the TCP handshake is completed and the http host headers are available in the session exchange.

Section 5: Application Identification (App-ID)

The firewall first performs an application-override policy lookup to see if there is a rule match. If there is, the application is known and content inspection is skipped for this session.

If there is no application-override rule, then application signatures are used to identify the application. The firewall uses protocol decoding in the content inspection stage to determine if an application changes from one application to another.

After the firewall identifies the session application, access control, content inspection, traffic management and logging will be setup as configured.

- Security policy lookup: The identified application as well as IP/port/protocol/zone/user/URL category in the session is used as key to find rule match.
- If the security policy has logging enabled at session start, the firewall generates a traffic log, each time the App-ID changes throughout the life of the session.
- If security policy action is set to allow and it has associated profile and/or application is subject to content inspection, then it passes all content through Content-ID.
- If security policy action is set to allow, the firewall performs a QoS policy lookup and assigns a QoS class based on the matching policy.
- If security policy action is set to allow and the application is SSL or SSH, perform a decryption policy lookup and set up proxy contexts if there is a matching decryption rule.

Section 6: Content Inspection

The firewall performs content inspection, if applicable, where protocol decoders' decode the flow and the firewall parses and identifies known tunneling applications (those that routinely carry other applications like web-browsing).

If the identified application changes due to this, the firewall consults the security policies once again to determine if the session should be permitted to continue.

If the application does not change, the firewall inspects the content as per all the security profiles attached to the original matching rule. If it results in threat detection, then the corresponding security profile action is taken.

The firewall forwards the packet to the forwarding stage if one of the conditions hold true:

- If inspection results in a 'detection' and security profile action is set to allow, or
- Content inspection returns no 'detection'.

The firewall then re-encrypts the packet before entering the forwarding stage, if applicable (SSL forward proxy decryption and SSH decryption).

Section 7: Forwarding/Egress

The firewall identifies a forwarding domain for the packet, based on the forwarding setup (discussed earlier).

The firewall performs QoS shaping as applicable in the egress process. Also, based on the MTU of the egress interface and the fragment bit settings on the packet, the firewall carries out fragmentation if needed.

If the egress interface is a tunnel interface, then IPSec/SSL-VPN tunnel encryption is performed and packet forwarding is reevaluated.

Finally the packet is transmitted out of the physical egress interface.

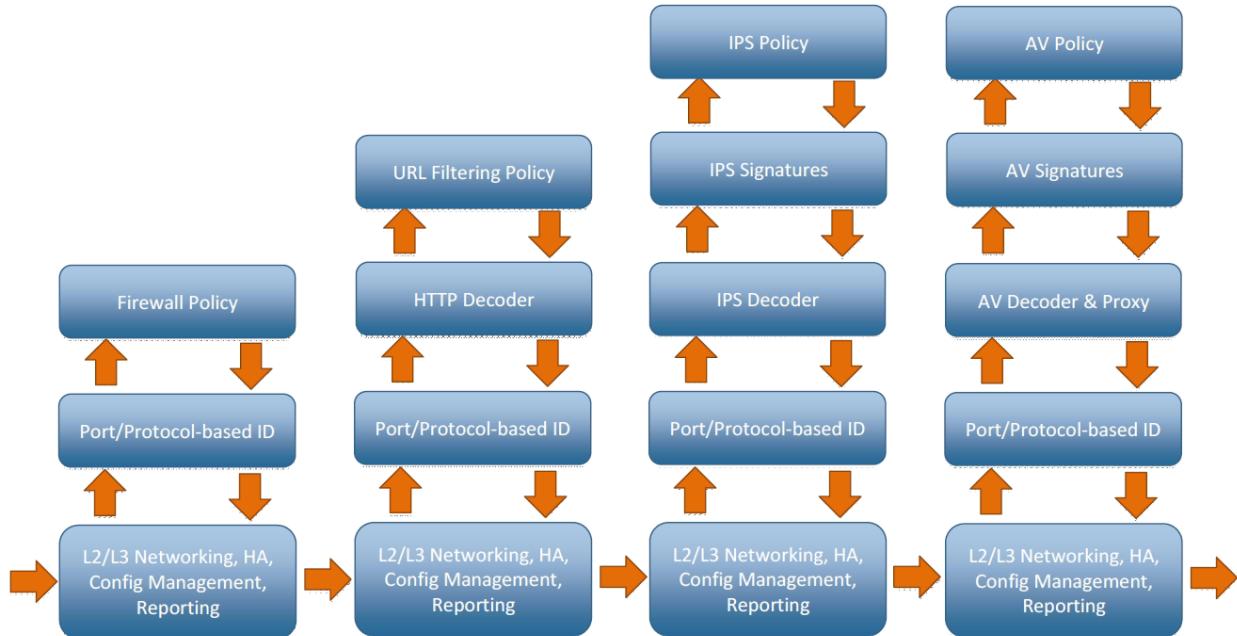
Section 8: Summary

Palo Alto Networks next-generation firewalls use a unique Single Pass Parallel Processing (SP3) Architecture—which enables high-throughput, low-latency network security, all while incorporating unprecedented features and technology. Palo Alto Networks solves the performance problems that plague today's security infrastructure. With the SP3 architecture, which combines two complementary components—Single Pass software, Parallel Processing hardware. The result is an excellent mix of raw throughput, transaction processing, and network security that today's high performance networks require.

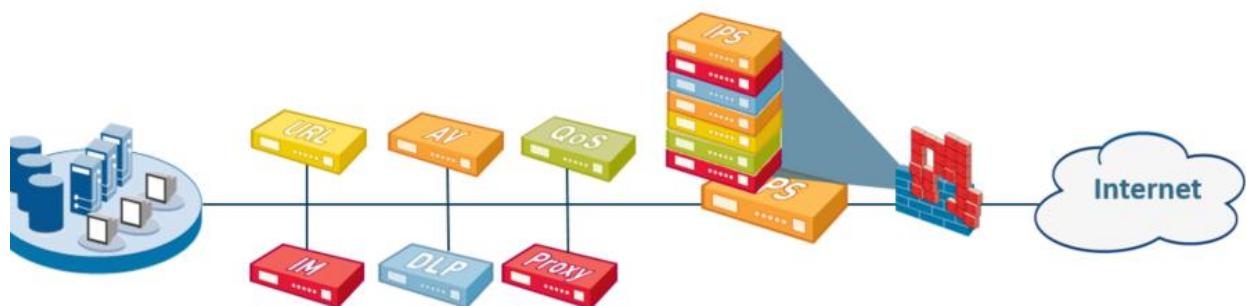
Multipass Architecture:

However, if you looked within the UTM devices, you would find that each functionality was being handled by a different software stack in a serial manner. So each security feature introduced its own latency to the network traffic. For example, the firewall would process traffic with a significant reduction in speed if you turned on antivirus detection.

An additional cost of UTM devices is that the features are typically managed independently. This management complexity adds significant time to any configurational response.



Development of Unified Threat Management



In the past, service providers and network engineers usually preferred to have single devices provide individual functions within the network. For example, one device would do URL filtering, another device

would do antivirus scanning, and another device would provide QoS. This approach assumed that using the “best-of-breed” for each device provided the highest quality service.

This approach had many problems. Each device added its own latency to the network traffic. Also, it was difficult to get a comprehensive overview of traffic and threats on a network from so many disparate devices.

This problem led vendors to provide Unified Threat Management (UTM) devices that performed all the necessary functions to protect a network in a single device.

Initial Access:

Palo Alto Networks firewalls are built with a dedicated out-of-band management interface, labeled MGT. This interface only passes management traffic for the device and cannot be configured as a standard traffic interface. Administrators use this interface for direct connectivity to the management plane of the firewall. By default, this interface has an IP address of 192.168.1.1.

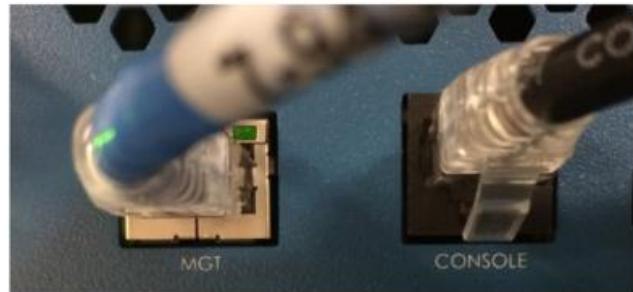
Initial configuration of the firewall can be accomplished by connecting to the MGT interface address or through a console session on the firewall. The console interface is an RJ-45 connection for all devices.

The default username of “admin” has a default password of “admin”. A warning message appears in the Web UI and the CLI until the default password is changed. This admin account cannot be deleted or disabled.

The serial port has default values of 9600-8-N-1.

Initial Access to the System

- Initial configurations must be performed over either:
 - Dedicated out-of-band management Ethernet interface (MGT)
 - Serial console connection
- Default values:
 - User name: admin
 - Password: admin
 - MGT IP address: 192.168.1.1/24



Configuring the MGT Interface Using the CLI:

```
#set deviceconfig system ip-address 10.30.11.1 netmask 255.255.255.0 default-gateway 10.30.11.254  
dns-setting servers primary 172.16.20.230  
  
#commit
```

The MGT interface can also be set up within the WebUI. By default, Palo Alto Networks firewalls are configured with an IP address of 192.168.1.1 on the MGT interface.

To assign an Ethernet interface:

1. Address your laptop Ethernet port with an address in the 192.168.1.0/24 subnet.
2. Connect to the MGT interface to your PC with an Ethernet cable.
3. Launch a web-browser connection to https://192.168.1.1.
4. Log in using the default user name and password.
5. Select **Device > Setup > Management**.
6. Click the gear icon on the Management Interface Settings panel.
7. From this location, set the networking information for the MGT interface of the firewall.

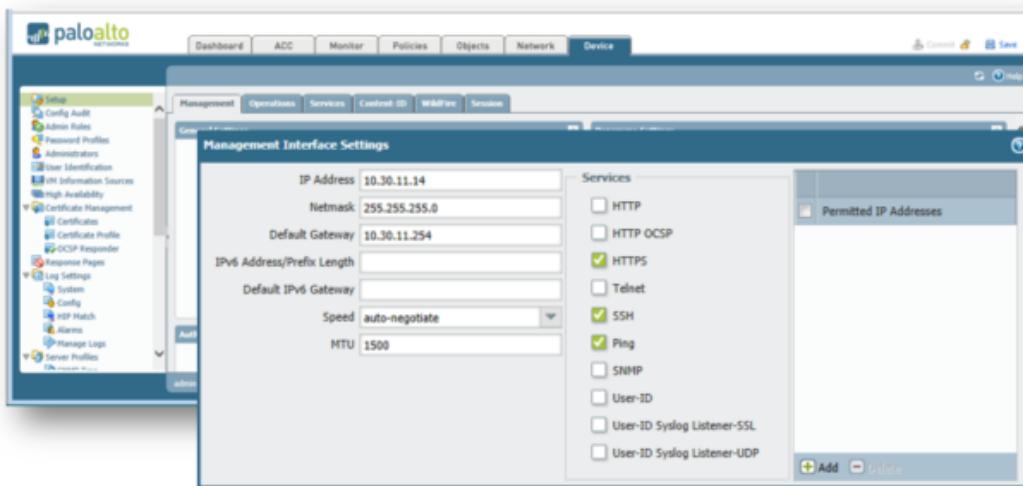
The WebUI is supported on Internet Explorer 7+, Firefox 3.6+, Safari 5+, and Chrome 11+.

By default, HTTP, SNMP, and Telnet are disabled on the MGT interface, but HTTPS, SSH, and Ping are enabled by default. These settings can be configured as appropriate for the environment. For additional security, the Permitted IP Addresses field restricts administrative access to specific IP addresses.

When you experience intermittent WebUI connectivity issues, change the Speed attribute from auto-negotiate to match the settings of the network. This change can alleviate the problem.

Configuring the MGT Interface Using the WebUI

Device > Setup > Management > Management Interface Settings



Configure the Hostname and Domain

Device > Setup > Management > General Settings

General Settings

Hostname	Student-11
Domain	dev.pan
Login Banner	*** This is the Palo Alto Networks - Student Firewall *** *** Authorized access ONLY!!! *** 205 6.1b Config 03/30/15 4 DevLab
SSL/TLS Service Profile	None
Time Zone	America/Los_Angeles
Locale	en
Date	2015/07/14
Time	10:40:50

DNS and NTP Configuration:

Device

Setup 2

Management Operations Services 3 Interfaces Telemetry Content-ID WildFire Session HSM

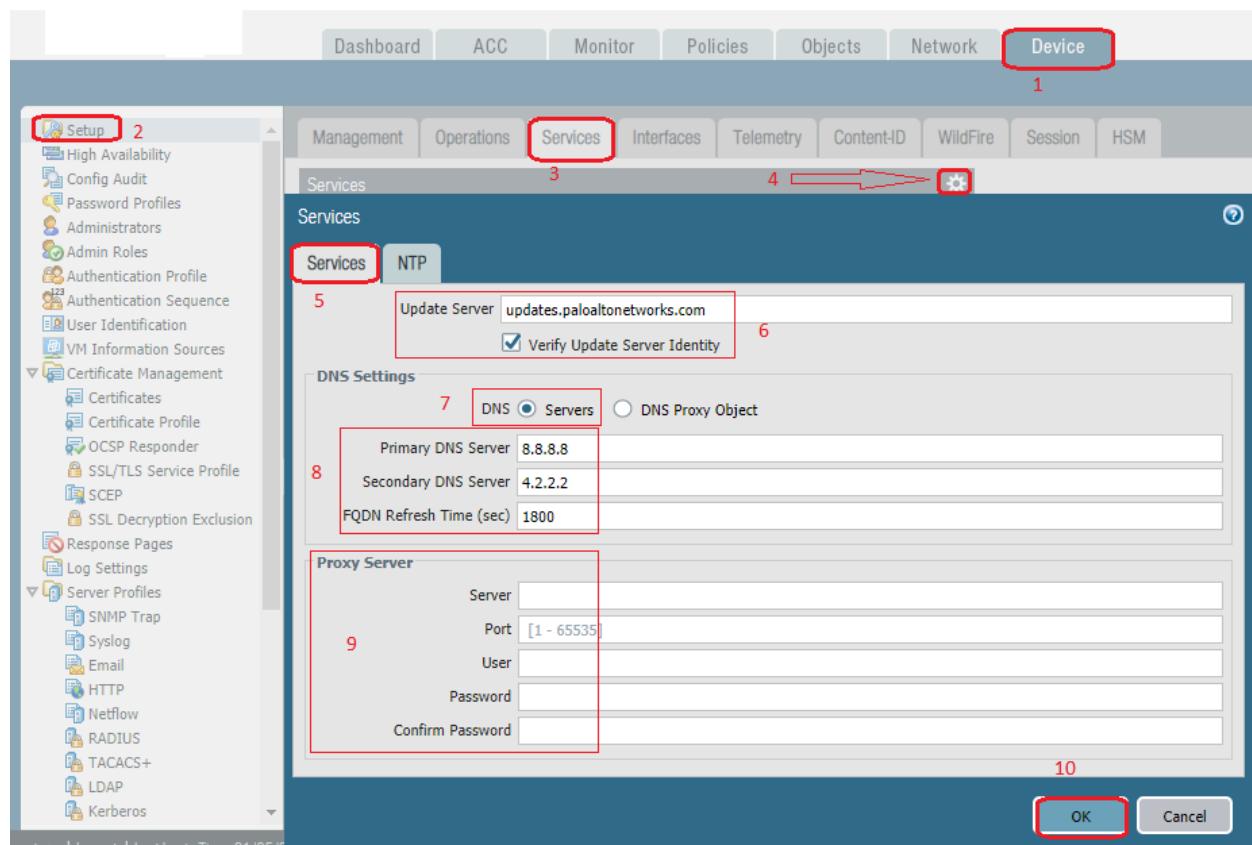
Services 4

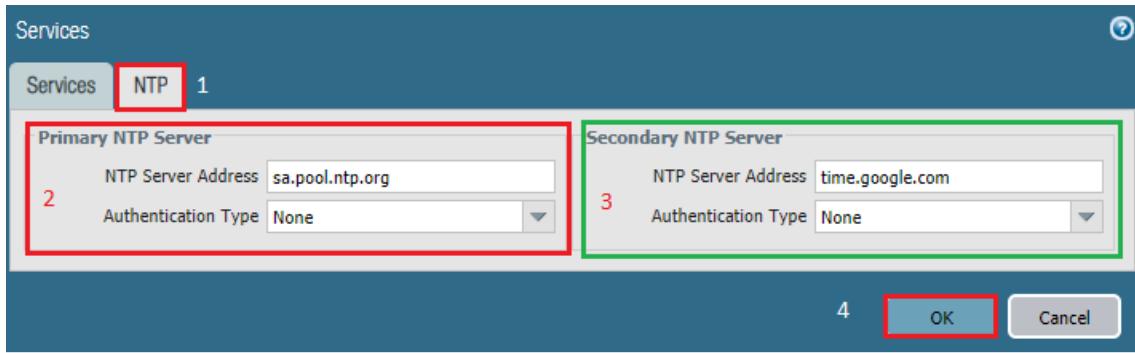
Services NTP 5 Update Server updates.paloaltonetworks.com 6 Verify Update Server Identity

DNS Settings 7 DNS Servers 8 Primary DNS Server 8.8.8.8 Secondary DNS Server 4.2.2.2 FQDN Refresh Time (sec) 1800

Proxy Server 9 Server Port [1 - 65535] User Password Confirm Password 10

OK Cancel





```
admin@PA-VM> show ntp
```

```
NTP state:
NTP synched to time1.google.com
NTP server: sa.pool.ntp.org
status: available
reachable: yes
authentication-type: none
NTP server: time1.google.com
status: synched
reachable: yes
authentication-type: none
```

```
admin@PA-VM> show clock more
```

```
dataplane time: Mon Jan 06 00:23:38 PST 2020
```

----- END -----

Day 03

!

Configuration Management (Candidate config and Running config)

Palo Alto Support Portal and Palo Alto update Server.

->(www.support.paloaltonetworks.com and updates.paloaltonetworks.com)

Licensing

Dynamic Updates

Software updates

Power Operations

-> request restart system

-> request shutdown system

-> request restart dataplane

Reset to factory configuration

-> request system private-data-reset

Administrative Controls (WebUI, CLI, RestAPI)

Frequently used CLI Commands

Candidate config and Running config:

When you change a configuration setting and click OK, the current or “candidate” configuration is updated; not the active or “running” configuration. When you click Commit at the top of the page, the candidate configuration is applied to the running configuration, which activates all configuration changes since the last commit.

Changes to the configuration of the firewall are logged within the Configuration Log, which is accessed through the Monitor Tab > Logs > Configuration. The configuration log contains details that include the date and time of the configuration change, the Administrator who made the change, the host IP address of the Administrator’s system, and the command and its result. For specific information and searches, you can set filters to find specific information within this log.

Config Types

Candidate Configuration

- What is shown in the UI becomes Running Config upon successful Commit



Running Configuration

- Active on the firewall



Licensing and Registration of Palo Alto Firewall in Support Portal:

When you purchase a VM-Series firewall, you receive a set of authorization codes by email. Typically the email includes authorization code(s) to license the VM-Series model that was purchased (VM-100, VM-200, VM300, VM-1000-HV), support entitlement that provides access to software/content updates (for example, PAN-SVC-PREM-VM-100 SKU auth-code), and any additional subscriptions such as, Threat Prevention, URL Filtering, GlobalProtect, or WildFire.

To use the authorization code(s), register the code to the Support account on the Palo Alto Networks Support portal. If you have an existing Support account, access the VM-Series Authentication Code link on the Support portal to manage the VM-Series firewall licenses and download the software.

If you do not have an existing Support account, use the capacity auth-code to register and create an account on the Support portal. After the new account is verified and the registration is complete, you can log in and download the software package that is needed to install the VM-Series firewall.

To activate the license on your VM-Series firewall, you must have deployed the VM-Series firewall already and completed initial configuration. The firewall must be configured with an IP address, netmask, default gateway, and DNS server IP address.

Until you activate the license on the VM-Series firewall, the firewall does not have a serial number, the MAC address of the dataplane interfaces are not unique, and only a minimal number of sessions are supported. The MAC addresses are not unique until the firewall is licensed, so to prevent issues caused by overlapping MAC addresses, make sure that you do not have multiple, unlicensed VM-Series firewalls.

When you activate the license, the licensing server uses the UUID and the CPU ID of the virtual machine to generate a unique serial number for the VM-Series firewall. The capacity auth-code is used in conjunction with the serial number to validate your entitlement.

Activate VM-Series Firewall



1. Register with Palo Alto Networks

- a. A set of authorization codes will be emailed
- b. Login to <https://support.paloaltonetworks.com>
If you haven't already, register for a Support account with your capacity auth-code and purchase or sales order number
- c. Click the **Assets > Add VM-Series Authentication Code** link to manage your VM-Series firewall licenses and download the software

2. Activate Licenses

- Select **Device > Licenses** and select the **Activate** feature using authentication code link.

3. Manage Content Updates

4. Install Software Updates

Licensing

Device > Licenses

GlobalProtect Gateway Date Issued: August 28, 2014 Date Expires: August 17, 2019 Description: GlobalProtect Gateway License	PA-VM Date Issued: August 28, 2014 Date Expires: Never Description: Standard VM-100
PAN-OS URL Filtering Date Issued: August 28, 2014 Date Expires: August 17, 2019 Description: Palo Alto Networks URL Filtering License Active: Yes Download Status: Download Now	Threat Prevention Date Issued: August 28, 2014 Date Expires: August 17, 2019 Description: Antivirus, anti-spamware, vulnerability protection
Wildfire License Date Issued: August 28, 2014 Date Expires: August 17, 2019 Description: WildFire signature feed, integrated WildFire logs, WildFire API	License Management Retrieve license keys from license server Activate feature using authorization code Manually upload license key

Device > Support

Support
Phone: 866-898-9087 Email: support@paloaltonetworks.com Expiry Date: August 17, 2019 Level: Premium Description: 24x7 phone support; advanced replacement hardware service Activate support using authorization code

Activate Firewall



1. Register with Palo Alto Networks

- a. Obtain the serial number from the WebUI dashboard
- b. Log in to <https://support.paloaltonetworks.com>
(If you haven't already, register for a Support account with your serial number)
- c. Click Assets
- d. Enter the assigned serial number and click Register Device

2. Activate Licenses

3. Manage Content Updates

- Updates include the latest application and threat signatures and URL filtering database

4. Install Software Updates

The Palo Alto Networks firewall features are licensed individually. You can activate just the functionality that is required for implementation. Only the features that are currently licensed are displayed in the Device > Licenses section of the WebUI. Several types of feature licenses are available: threat prevention, WildFire, URL filtering databases, virtual systems, decryption port mirroring, GlobalProtect, and multiple gateways and host checks require a license.

In addition to the feature licenses, the firewall must also have a valid support license. The support license entitles access to the Support portal where trouble tickets can be submitted to the Technical

Assistance Center (TAC). Additionally, the support license enables you to receive product and security alerts from Palo Alto Networks based on the serial number of your firewall.

Also, you can purchase a Palo Alto Networks firewall with a “software license” option. This option is necessary in countries that have a high tax on hardware but a low tax on software. Before the license key is installed using the console or SSH, the PAN-OS is in maintenance mode. This on-demand license option allows the customer to purchase the hardware and software as two separate items.

On-demand or usage-based licensing is available in Amazon Web Services (AWS) that allows you to obtain the Amazon Machine Image (AMI) for the VM-Series firewall from the AWS Marketplace and deploy the firewall for use in a virtual private cloud (VPC). This option allows you to consolidate your billing of AWS resources and the usage fees—at an hourly or a yearly rate—for the VM-Series firewall.

Also, a self-service license is available that allows you to deactivate the active licenses on a firewall to make them available for another firewall.

Dynamic Updates:

Dynamic Updates

Device > Dynamic Updates

Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently
▼ Antivirus	Last checked: 2015/04/08 20:29:15 CEST	Schedule: Every Saturday at 00:00 [Download and Install]					
1512-2350	panos-all-antivirus-1512-2350.candidate	Full		99 MB	2015/04/08 00:21:18 CEST	✓	
1510-2345	panos-all-antivirus-1510-2345.candidate	Full		100 MB	2015/04/01 00:21:50 CEST	✓ previously	
▼ Applications and Threats	Last checked: 2015/04/06 20:30:37 CEST	Schedule: Every Saturday at 01:02 [Download and Install]					
494-2664	panos2-all-content-494-2664	Apps, Threats	Full	26 MB	2015/04/04 01:00:37 CEST	✓	
492-2638	panos2-all-content-492-2638	Apps, Threats	Full	26 MB	2015/03/29 05:05:33 CEST	✓ previously	
493-2656	panos2-all-content-493-2656	Apps, Threats	Full	26 MB	2015/03/21 03:15:41 CEST	✓	
▼ GlobalProtect Data File	Schedule: Every Saturday at 03:00 [Download and Install]						
1413625901					2014/10/18 09:31:43	✓	
▼ URL Filtering	Schedule: None						
4369						✓	
4364						✓ previously	
▼ Wildfire	Last checked: 2015/04/06 20:33:32 CEST	Schedule: None					
61214-70111	panos-all-wildfire-61214-70111.candidate	Full		12 MB	2015/03/17 23:07:51 CEST	✓ previously	
63115-72018	panos-all-wildfire-63115-72018.candidate	Full		12 MB	2015/04/06 20:24:50 CEST	✓	
62623-71536	panos-all-wildfire-62623-71536.candidate	Full		12 MB	2015/03/19 06:34	✓	

To install from a file, upload content first

Schedule and check for new content

Check Now Upload Install From File

Palo Alto Networks posts updates with new or revised application definitions, information on new security threats (such as, antivirus signatures, URL filtering criteria), and updates to GlobalProtect data.

You can also view the latest updates, read the release notes for each update, and then select an update to download and install.

To download application and threat updates, you must have a threat prevention license.

Updates are issued on the following schedule:

- Antivirus: daily
- Applications and threats: weekly
- Bright Cloud URL filtering: daily

On the Dynamic Updates page, you may see two entries listed in the Application and Threats, Antivirus, or URL Filtering area, one for the currently installed version and one for the latest version available on the update server. If the latest version is already installed, only a single entry is listed.

Power Operations:

The firewall can be gracefully shut down or rebooted from the WebUI. Either action deletes the candidate configuration in memory, so be sure to save or commit to preserve changes.

-> **request restart system**

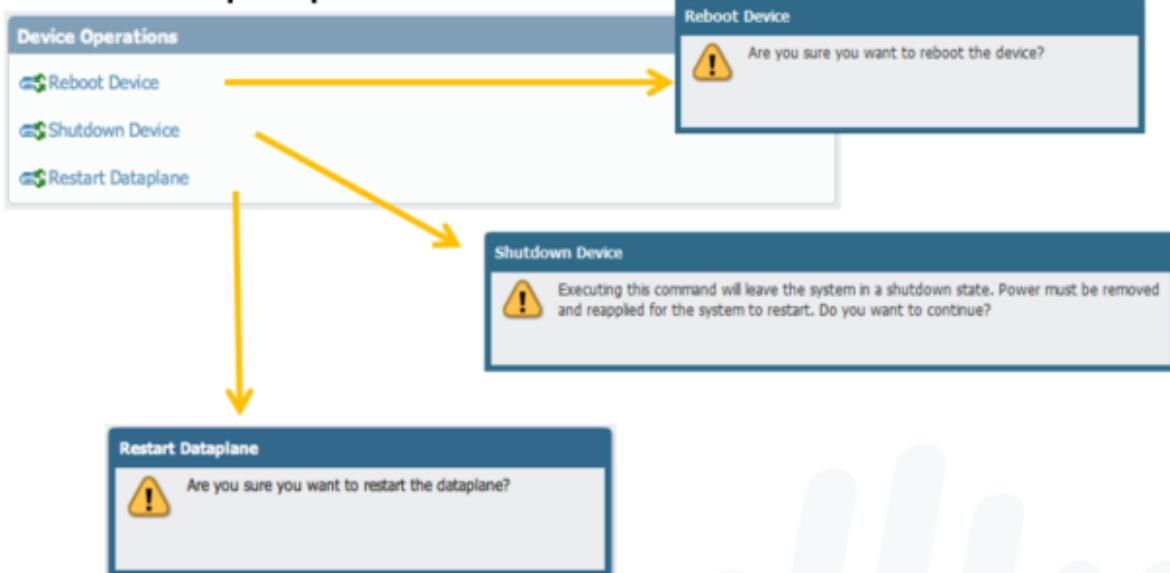
-> **request shutdown system**

-> **request restart dataplane**

If the firewall is shut down by these commands, it must be powered up manually by unplugging and reconnecting the power cords on the firewall.

Power Operations

Device > Setup > Operations



Reset to factory configuration

-> **request system private-data-reset**

To reset the system to factory default, you must enter maintenance mode. To enter maintenance mode, reboot the box, and as the system is booting up, type the word “maint” into the CLI through the console port. After some time, you can choose an option to have the system reset to default, including the default admin password.

After the system is reset to default, the MGT port IP address must be configured through the serial port CLI. Use the “set deviceconfig system ip-address <IP> netmask <mask> default-gateway <IP>” command.

This is a critical process following a product evaluation, that will ensure that no information remains on the evaluation device for later use.

Reset to Factory Configuration

- With Admin User password
 - Erases all logs
 - Resets all settings—including IP addressing, which causes loss of connectivity
 - Saves a default configuration after the MGT IP address is changed
- > **request system private-data-reset**
- Without Admin User password
 - From the console port
 - Type **maint** during bootup
 - Choose Reset to Factory Default
 - Or load another configuration into running memory



Administrative Controls (WebUI, CLI, RestAPI):

Administrators have multiple options when configuring a Palo Alto Networks firewall.

The most common way to manage the device is through the WebUI. Administrators can configure and monitor the firewall over HTTP/HTTPS from a web browser. This graphical interface provides detailed administrative and reporting tools in an intuitive web format.

The PAN-OS CLI provides the ability to access the firewall, view status and configuration information, and modify the configuration. Access to the PAN-OS CLI is provided through SSH, Telnet, or direct console access.

Palo Alto Networks also provides a REST-based interface to access device configuration, operational status, reports, and packet captures from the firewall. There is an API browser available on the firewall at <https://<firewall>/api>, where <firewall> is the host name or IP address of the firewall. This link provides help on the parameters that are required for each type of API call.

Administrative Controls

WebUI



REST-API

```
<response status="success" code="19">
  <result>
    <msg>
      <line>Commit job enqueued with jobid 17</line>
    </msg>
    <job>17</job>
  </result>
</response>
```

CLI over SSH, Telnet, or console session

Administrative Controls

- WebUI
- Panorama
- CLI
- XML API

Initial Access to System

- MGT is out of band, connected to the management plane; default IP it is [\[192.168.1.1/24\]](https://192.168.1.1/24)(<https://192.168.1.1/24>) for physical. VM is DHCP.
- Console port (RJ45) 9600,8,N,1
- Admin/Admin default login (nag screen until changed)
- MGT can be set for DHCP (although Static is highly recommended)

Initial config

- Factory Reset instructions:
 - ‘Request system private-data-reset’ if you have CLI access
 - If no CLI access, reboot into MAINT mode ([see PAN documentation for further information](#))
- Hostname limited to 31 characters

- Configure new IP if needed, hostname, domain name (if wanted), and Gateway
- MGT does updates for updates, DNS, NTP, unless done on a data port.
- Add Service route(s) if any are needed.
- HTTPS, SSH and Ping are enabled by default on the MGT Interface
- Minimum MGT Config are IP Address, Netmask and Default Gateway
- MGT port is used by default to access external management services, such as:
 - PAN Update Servers
 - NTP
 - DNS

- Inband port can be set up to for service routes to perform these services which ports to retrieve them from if MGT port is not able to.

Configuration Management

- Running config: active config running on the FW – running-config.xml
- Candidate config: sandbox configuration; when a commit is done, candidate replaces the running config.
- Previous configurations are saved. These can be reverted, exported, saved out, and imported.
- Admin-Level commit will commit all changes made by anyone (if commit all changes is selected)
- Config changes are logged under the admin logged in for change tracking
- Commit locks stop other admins from committing changes
- Config locks stop other admins from making any candidate config changes
- Admin Locks can only be removed by the admin that put the lock in place, or by a super admin.
- Candidate Configuration is stored on control plane memory
- Running configuration is written to both control and dataplane memory

Licensing and Software Updates

- Registration with PAN is first step – support page and register new device. Generally this will send an activation code to your email.
- Retrieve License from PAN License server
- VM's can be downloaded from the software page after registration
- Activate support license needed before activating other optional licenses (URL/threat/Wildfire, etc)
- (if licensed) Set the dynamic updates for update/install on specific intervals
- Update the Dynamic updates before upgrading the PanOS code. If no subscription, download and install manually.

- Update the PanOS software. Steps to upgrade will likely be needed if upgrading between major versions (7.0 ->8.0 for example)

Account Administration

- Administrators can be created with specific access, using Admin Roles.
- External auth servers supported are LDAP, Kerberos, RADIUS, TACACS+, SAML, along with 2FA are supported.
- For non-local admins, create an admin role profile, server profile, authentication profile. authentication sequence is optional.
- 2 types of admin role profiles:
 - predefined dynamic profiles
 - super user, superuser(read-only), device administrator, DA (read-only), VS Admin, VS Admin (read-only).
 - administrator defined role based profiles
 - These can be granularity specified for specifically what they have access to, and functions they can change, update or view.
 - Predefined local admin accounts are:
 - super user, superuser(read-only), device administrator, DA (read-only)
 - local admin accounts can be set for minimum passwords, password aging and password complexity. Not enabled by default.
- Creating non-local admins by creating an authentication profile.
 - Multiple servers can be used. LDAP, then RADIUS would be an example.
 - Create Server profile, then (optional) auth sequence, then authentication profile.
 - Allow list can be used for those that will be allowed to use certain auth profiles.

Viewing and Filtering Logs

- Clicking any link in the Monitor > Traffic (or other entries) will filter the logs to only show entries with those
- Filters can be saved and loaded for quick access

Frequently used CLI Commands:

> show interface management

Show management Interface details

> show system info

Display system's management IP, Serial number, and code version

> show system disk-space

Show percent usage of disk partitions.

> show system software status

Show running processes.

> show system resources

Show processes running in management plane.

> show running resource-monitor

Show resource utilization in the data plane.

> request license info

Show the licenses installed on the device.

> show jobs processed

Show when commits are completed.

> show session info

Display session usage, rate etc. information.

> show session id <session-id>

Display information about a specific session.

> show running security-policy

Show the running security policy.

> request restart system

Restart the device.

> request shutdown system

Shutdown the device.

>request system private-data-reset

Default Factory reset command

> show admins

Show administrators who are currently logged.

> show admins all

Show administrators who can access the web interface or command line interface CLI.

> ping host <destination-ip-address>

Ping from management interface

> ping source <ip-address-on-dataplane> host <destination-ip-address>

Ping from a dataplane interface to a destination IP address

> show running nat-policy

Shows current NAT policy table.

> show running ippool

Shows NAT pool utilization.

> show running global-ippool

Shows NAT pool utilization.

> show routing route

Shows routing table.

> show running security-policy

Shows current policy set.

> show vpn flow

Shows encap/decap counters

> show vpn gateway

Shows list of IKE gateway configurations.

> show vpn ike-sa

Shows IKE Phase 1 SA

> show vpn ipsec-sa

Shows IPSEC Phase 2 SA.

> show vpn tunnel

List of auto-key IPsec tunnel configurations.

> show high-availability state

Shows the HA state of the device.

> show high-availability all

Shows settings configured on device & peer.

> show high-availability state-synchronization

Shows if the devices are synchronized.

> request high-availability state suspend

Suspends active device and makes passive device active.

> request high-availability state functional

Changes the state from suspend to passive.

> request license info

Shows the license installed on the device.

!

Commands

Description

set zone Outside

Create zone with name Outside.

set network virtual-router VR-1

Create Virtual Router named VR-1

set network interface ethernet ethernet1/1 layer3 ip 192.168.100.100/24

Assign IP address and subnet mask to interface ethernet 1/1 and set as Layer 3

set deviceconfig system type static

Set the interface type to static

set deviceconfig system type dhcp-client

Set the interface type to DHCP

set deviceconfig system dns-setting servers

Set Primary and Secondary DNS

set mgt-config users admin password

Set Administrator password

```
# set deviceconfig system ip-address  
Assign IP address to Management interface.
```

> find command

Display entire command in current mode.

> find command keyword show

Locate all commands have specified keyword.

1. Palo Alto Hardware Tshoot

Case 01: Chassis related tshoot

```
show system state filter chassis.leds      (For Leds status)
```

```
show system environmental (FAN, Temperature, Power supply )
```

```
show system disk-space
```

```
show system statistics session
```

```
show system software status  (Daemons details)
```

```
show system services
```

Case 02: Interface Flapping

```
show interface ethernet1/21           (Detailed Info)
```

```
show interface ethernet1/21 | match link    (Link Status)
```

```
show interface ethernet1/21 | match address  (Mac address)
```

```
show interface ae1.60
```

```
show interface ae1.60 | match IP
```

GUI -> Monitor -> System -> See details by setting up the filter (eventid eq link-change) and (object eq 'ethernet1/21')

Or

```
show log system query equal "( eventid eq link-change ) and ( object eq 'ethernet1/21' )" 
```

```
show log system query equal "( eventid eq link-change ) and ( object eq 'ethernet1/21' )"   
direction equal backward
```

show log system (display all system log)

show log traffic app ssl (Display traffic log for ssl traffic)

show log traffic query equal "(addr.src in 11.50.151.228) and (addr.dst in 17.188.145.51)"

show log traffic from equal 11.50.136.218 to equal 199.19.250.205 dport equal 80

Show log traffic src in 11.50.136.218 DST in 199.19.250.205 dport equal 80

2. L2 Tshoot

Layer 2 MAC leaning, VLAN missmatched, Layer 2 loop, Aggregated interface and LACP

show mac all (Shows the mac details for vlan, interfaces)

Case 01: VLAN missmatched

show arp ae1.60 for arp table

show arp management

show arp ethernet1/1

show mac all for mac table

show interface ae1.60 | match received (interface counter)

Show interface ae1.60 | match error (error counter increased due to incorrect
tcp/udp checksum, cpd, unexpeted vlan traffic on trunk interface)

Case 02: Aggregate interface issue

show lacp aggregate-ethernet ae1 (check the details)

```
***** How to tshoot silent packet drop on Palo Alto
*****
```

Source IP = 172.16.3.100 , Dest IP = 42.42.100.3

1. Check the session on session table

```
show session all filter filter source 172.16.3.100 destination 42.42.100.3
```

2. Enable the debugging on data plane for this traffic

```
debug dataplane packet-diag set filter match source 172.16.3.100 destination 42.42.100.3
(This is set the debug)
```

```
debug dataplane packet-diag set filter on
```

3. show the debugging log

```
show counter global filter packet-filter yes delta yes security drop      (here we can see
the debug counters and session drop reason :: "No destination zone from forwardir)
```

4. check the routing for the source and destination

```
test routing fib-lookup ip 42.42.100.3 virtual-router default      ( NO route found)
```

5. Add the route and check the session

```
set network virtual-router default routing-table ip static-route 42.42.100.3/32 nexthop
192.168.1.1
```

```
test routing fib-lookup ip 42.42.100.3 virtual-router default
```

```
show session all filter filter source 172.16.3.100 destination 42.42.100.3
```

!

```
*****
```

Layer 03 Tshoot

```
*****  
*****
```

IP/Subnet config issue, missing or inactive route, inter virtual router communication error,
Dynamic routing protocol issues (OSPF, BGP).

show routing interface (it will show all interfaces which will participate on Routing)

show routing interface | match ae1.960

!

show arp all (This is shows the ARP is resolving or not for an IP/nextHop IP)

show arp all | match 30.191.60.39

!

test routing fib-lookup virtual-router Extranet-VR ip "26.122.64.10" (for getting the next hop)

!

show routing route destination 10.1.1.0/24 (Used to see the all next hops for the 10.1.1.0/24)

show routing fib virtual-router Extranet-VR | match 10.1.1.0/24 (It will give the active nexthop or preferred next hop).

!

Case 01 :: Static Route issues

!

1. A route can be down 1. Local interface to reach NextHop is down. 2. NextHop can not be resolved locally via ARP.

!

We use the following command to test an active route exit for a destination.

#show routing route destination 10.1.1.0/24

#show arp all

#test routing fib-lookup ip 10.1.1.100 virtual-router Extranet-VR

!

2. If a static route remain inactive make sure to

!

Use correct nexthop type (IP address)

Use the correct Virtual router (If dealing with multiple VR)

Use the correct routing table (Unicast/Multicast)

!

3. Also check the routing table exceed limits

```
#show routing fib virtual-router default afi ipv4
```

```
#show routing resource
```

!

show interface all (Use to see the IP address/Zone of an interface)

```
ping count 3 source 165.197.216.4 host 165.197.216.1
```

```
traceroute source 165.197.216.4 host 165.197.216.1
```

!

Case 02 :: Missing Route

!

```
ping count 3 source 10.1.1.250 host 10.1.1.221 (Not pinging)
```

```
show routing route destination 10.1.1.0/24 (look for next hop)
```

```
show arp all (For next hop) (No arp for next hop) Fix the route for the route
```

```
ping count 3 source 10.1.1.250 host 10.1.1.221
```

!

@@@@@@@

```
debug dataplane packet-diag set filter on
```

```
debug dataplane packet-diag set filter match source 192.168.140.60 destination  
192.168.122.60
```

```
debug dataplane packet-diag set capture stage drop file DP.pcap
```

```
debug dataplane packet-diag set capture stage firewall file FW.pcap
```

```
debug dataplane packet-diag set capture stage receive file RX.pcap
```

```
debug dataplane packet-diag set capture stage transmit file TX.pcap
```

```
debug dataplane packet-diag set capture on
```

```
!
```

```
> show counter global filter delta yes packet-filter yes
```

```
!
```

```
> debug dataplane packet-diag show setting
```

```
!
```

```
Packet capture is disabled
```

```
> debug dataplane packet-diag set capture off
```

```
debug dataplane packet-diag set filter off
```

```
debug dataplane packet-diag set clear all
```

```
!
```

```
@@@@@@@tcpdump filter "host 10.16.0.106 and not port 22"
```

```
tcpdump filter "host 10.16.0.106 and not port 443"
```

```
!
```

```
view-pcap mgmt-pcap mgmt.pcap
```

```
!
```

```
Filter By Port
```

```
> tcpdump filter "port 80"
```

```
Filter By Source IP
```

```
> tcpdump filter "src x.x.x.x"
```

```
Filter By Destination IP
```

```
> tcpdump filter "dst x.x.x.x"
```

```
Filter By Host (src & dst) IP
```

```
> tcpdump filter "host x.x.x.x"
```

```
Filter By Host (src & dst) IP, excluding SSH traffic
```

```
> tcpdump filter "host x.x.x.x and not port 22"  
!!! Exporting the log by scp.  
> scp export mgmt-pcap from mgmt.pcap to 192.168.137.1  
!!! Exporting the log by tftp.  
> tftp export mgmt-pcap from mgmt.pcap to 192.168.137.1  
!
```

@@@@@@@
Verify Sessions

```
>show session all filter source ip1 destination ip2
```

Clear debug logs & filters

```
>debug dataplane packet-diag clear all
```

```
>debug dataplane packet-diag clear log log
```

Investigate Counters

```
>debug dataplane packet-diag set filter match source ip1 destination ip2
```

```
>debug dataplane packet-diag set filter match source ip2 destination ip1
```

```
>debug dataplane packet-diag set filter on
```

```
> show counter global filter delta yes packet-filter yes severity drop
```

---- Type the command above many time ----

Full debug Mode

```
>debug dataplane packet-diag set filter match source ip1 destination ip2
```

```
>debug dataplane packet-diag set filter match source ip2 destination ip1
```

```
>debug dataplane packet-diag set filter on
```

```
>debug dataplane packet-diag set log feature flow basic
```

```
>debug dataplane packet-diag set log feature appid basic  
>debug dataplane packet-diag set log feature tcp all  
> debug dataplane packet-diag set log on  
---- Wait for the problem to surface ----  
> debug dataplane packet-diag set log off  
> debug dataplane packet-diag aggregate-logs  
> less mp-log pan_packet_diag.log
```

```
admin@firewall> debug dataplane packet-diag set filter match ?
```

+ destination Destination IP address

+ destination-netmask Destination netmask <<< new option for network

+ destination-port Destination port

+ ingress-interface Ingress traffic interface name

+ ipv6-only IPv6 packet only

+ lacp LACP packet

+ non-ip Non-IP packet

+ protocol IP protocol value

+ source Source IP address

+ source-netmask Source netmask <<< new option for network

+ source-port Source port

| Pipe through a command

!

Use the following command to configure the firewall to bypass asymmetric routing globally.

```
# set deviceconfig setting tcp asymmetric-path bypass
```

The changes can be reverted back with the following:

```
# delete deviceconfig setting tcp asymmetric-path
```

Use the following command to check the current action on asymmetric traffic:

```
> show running tcp state | match asymmetric  
session with asymmetric path      : drop packet  
!
```

IPsec VPN Tshoot ::

!

Phase 01

1. PSK, Phase 01, Phase 02 Parameter mismatch
2. Wrong IKE Egress Interface

Phase 02

3. Wrong tunnel interface and zone
4. Proxy ID mismatch
- !
5. NAT Traversal
6. Routing :: Incorrect route
- !

If IPsec not comming up:: 1. Check the session table, If session not exist which means its a routing or Security policy issue. If session is exist then check tunnel interface is used or not.

```
>show session id 1111
```

!

Phase 1 Mismatch can we identify by running below command:

```
> show vpn ike-sa  
!  
-> system log :: filter: ( subtype eq vpn )  
!
```

IKE Log ::

> tail follow yes mp-log ikemgr.log

!

Phase 02 Tshoot ::

!

1. Check tunel interface and zone

2. check security policy

3. Check Phase 02 Policies (IPsec Crypto Profile) and Proxy ID.

Default Proxy ID :: local 0.0.0.0/0, remote 0.0.0.0/0, Protocol any.

!

Check the System Logs:: -> system log :: filter: (subtype eq vpn)

!

NAT Traversal :: NAT-T is mandatory if vpn gateway behind the NAT Device.

-> IPsec packets dont have a layer 4 header by default.

-> NAT-T will add an extra UDP header to the IPsec packet to allow PAT.

-> With-Out NAT-T, The IPsec tunnel can estabilise but ESP packet are lost in the transit.

-> in case of any NAT device, enable NAT-T on both side.

!

Routing Issues :: For IPsec forwarding decision start with a route, make sure you have a route pointing to the tunnel interface.

!

-> system log :: filter: (subtype eq vpn)

-> show log system subtype equal vpn direction equal backward

!

-> test vpn IPsec-sa tunnel <name>

-> show vpn IPsec-sa

-> show vpn ike-sa

- > show vpn flow
- > show vpn flow tunnel-id 1
- > show session all filter protocol 50
- > show session all filter destination <peerIP> destination-port 500
- > less mp-log ikemgr.log

Packet capture

- > debug ike pcap on/off/delete
- > debug ike global on debug
- > scp export debug-pcap
- > view-pcap <options> debug-pcap ikemgr.pcap

!

IKE Log ::

> tail follow yes mp-log ikemgr.log

!

Description of Issues:

Wrong IP: The IP address used for the remote gateway is either wrong or there is no IP connectivity between the two public interfaces.

No matching P1 or P2 Proposal: The peers cannot find matches for the 5 parameters of the IKE Phase 1 or Phase 2 proposals.

Mismatched Peer ID: Value entered for Peer ID's do not match.

PFS Group mismatch: Both sides have PFS enabled but with different DH groups.

Mismatched Proxy ID: The values for local and remote proxy ID are not correct. Most commonly happens when interoperating with policy based VPNs.

Error Messages:

P1 – Timeout: IKE phase-1 negotiation failed as initiator, main mode. Due to timeout.

No suitable proposal (P1): IKE phase-1 negotiation failed. no suitable proposal found in peer's SA payload.

Peer identifier does not match: peer identifier does not match remote Remote2.

No proposal chosen: IKE protocol notification message received.

No suitable proposal (P2): IKE phase-2 negotiation failed when processing SA payload.

P2 – Timeout: IKE phase-2 negotiation is failed as initiator, quick mode. Due to timeout.

PFS group mismatch: pfs group mismatched: my:2 peer:5.

Cannot find matching tunnel: IKE phase-2 negotiation failed when processing proxy ID.

----- **END** -----

Day 04

Security Zones

Interface Types

Tap Mode

Decryption Mirror

Virtual Wire

Layer 2

Layer 3

HA

Aggregate

Virtual Router (Static Routing)

IP Addressing

DHCP (Client, Server, Relay)

Virtual Router (Static Routing)

Dual ISP

Path Monitoring

PBF

ECMP (when both interface part of same Zone and when part of diffirent zone)

Security Zones and interfaces:

Zone creation and zone management are vital roles performed to secure the network. Therefore, one of the first tasks performed is to create and define your zones. This activity includes naming your zone, specifying the zone type, and then assigning an interface to that zone. In fact, before you can pass traffic throughout the firewall via its interfaces, that interface must be assigned to a zone.

Zone Name: The name you choose to use to designate your zone of users is up to you. However, the zone name is case-sensitive. For example, “DMZ” and “dmz” are not the same zone. They are two different zones.

Zone Type: The four main zone types of the Palo Alto Networks firewall are Tap, Virtual Wire, Layer 2, and Layer 3.

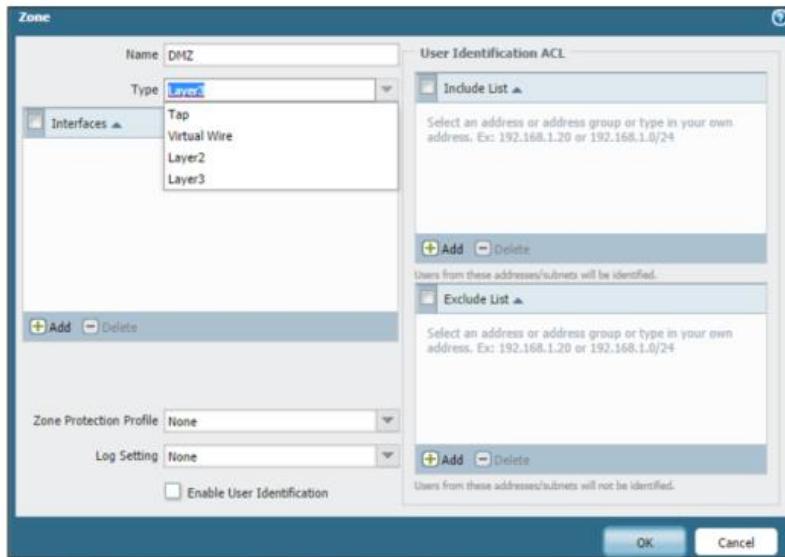
There is a fifth zone type called External, which is a special zone. It allows traffic to pass between virtual systems when multiple virtual systems are configured on the same firewall. The External zone type is visible in the pull-down menu only when supported by a firewall with the multi-vsyst feature enabled.

Interface: Each interface can be assigned only to a single zone.

Security Zones

- Specify Zone Name
- Select Zone Type
- Assign Interface

Network > Zones > Add



Security zones are used to group like-devices, user groups, locations or specific-use systems.

In-band interfaces are traffic-passing ports, ex: ethernet1/1, 1/2, etc

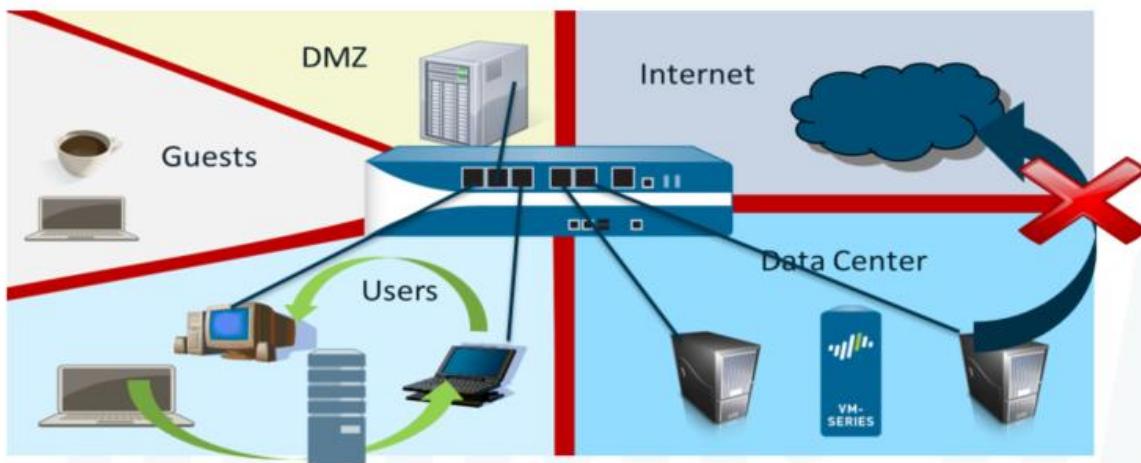
Each interface (or subinterface) can only be assigned to one zone

A zone can have multiple physical or logical interfaces

!

Security Zones and Policies

- Security policies use zones to regulate and log traffic
 - Intra-zone traffic is *allowed* by default
 - Inter-zone traffic is *denied* by default



Traffic inside zones is allowed by default. Example: Trust to trust is permitted by default

Traffic outside zones is denied by default. Example: Untrust to DMZ is NOT permitted by default

Palo Alto Networks firewalls use the concept of security zones to secure and manage your networks. These zones are a logical grouping based on a particular type of traffic on your network. The physical location of a zone and its traffic is irrelevant. In fact, zones may reside at different locations throughout your enterprise network.

Zone names have no predefined meaning or policy associations. They may help designate specific users, a group, a location, a function, or an entity.

Systems with similar security needs are grouped into zones. For example, the traffic going out of a DMZ server is very different than the traffic on a server inside the corporate data center. We would expect to see traffic initiated from the Internet making connections into the DMZ but we would never want to see this same kind of traffic going into the data center.

This depiction of zones shows five distinct security zones: DMZ, Guests, Users, Internet, and Data Center.

By default, PAN-OS zone rules allow intra-zone traffic to pass because it resides within the same zone. However, inter-zone traffic (that traffic that is traversing to another zone) is denied by

default. More information about these zone rule types is provided in the next module, “Security and NAT Policies.”

Security Zone Interfaces

- An interface is configured to only one zone
- A security zone can have multiple interfaces

Interface	Zone	Address
E 1/10	Internet	161.23.4.254
E 1/11	DMZ	172.16.1.254
E 1/12	--	--
E 1/12.10	Users	192.168.10.254
E 1/12.20	Users	192.168.20.254
E 1/12.30	VoIP	192.168.30.254
Tunnel.4	Remote-LAN	10.5.1.254

A logical interface, including VLAN-tagged subinterfaces, must be a member of only one zone. However, a zone can have multiple interfaces.

Zone types support specific zones:

Tap zone: tap interfaces

Tunnel zone: no interface

Layer 2 Zone: Layer 2 interface

Virtual Wire: VWire interfaces

Layer 3 Zone: L3, Aggregate, VLAN, Loopback and Tunnel interfaces

!

Creating a zone is done by naming the zone, selecting the type of zone (from the list above). Interfaces can be added at this time, or later by editing the interface.

Interface Types

- Ethernet
 - Tap
 - HA
 - Virtual Wire
 - Layer 2
 - Layer 3
 - Aggregate
- VLAN
- Loopback
- Tunnel
- Decrypt Mirror

Network > Interfaces

Interface	Interface Type	Management Profile
ethernet1/1	Layer3	Allow all
ethernet1/2	Layer3	
ethernet1/3	Layer2	
ethernet1/4	Tap	

Ethernet Interface Configuration

Network > Interfaces > Ethernet

Interface Type:

- Tap
- HA
- Virtual Wire
- Layer 2
- Layer 3
- Decrypt Mirror
- Aggregate

Virtual Wire

Layer 2

Layer 3

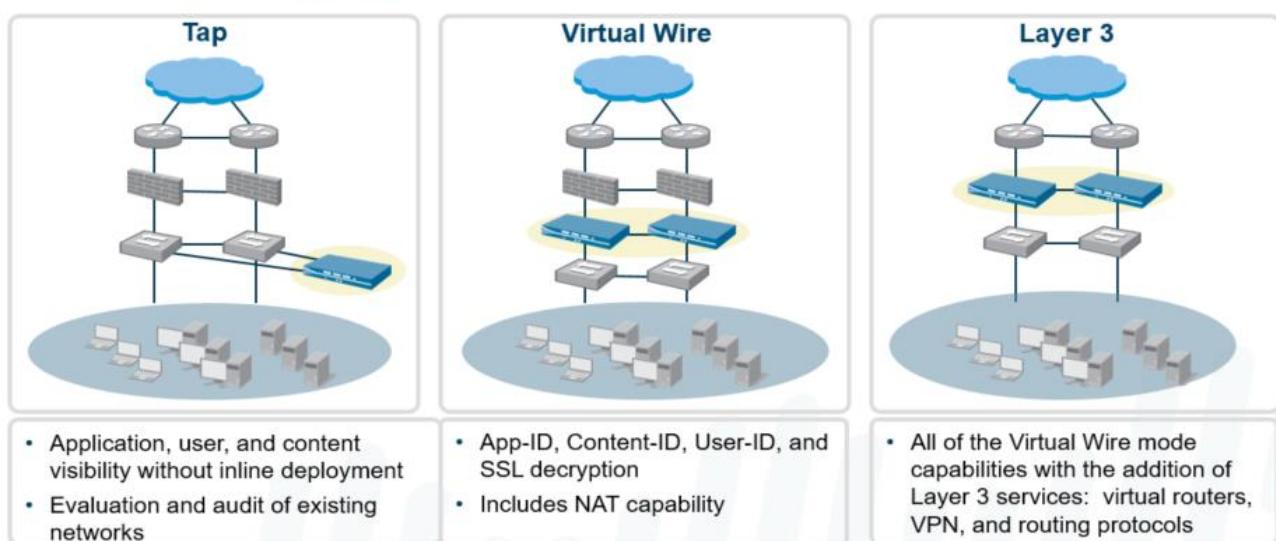
The Palo Alto Networks firewall can replace an existing firewall when installed between an Internet-facing device and a switch or router that connects to the internal network. The firewall supports a wide range of deployment options and interface types that can be used simultaneously on different physical interfaces.

This module addresses the interface types that are most commonly implemented in new firewall deployments. Other interface types will be addressed as appropriate in later modules.

Interface types are slightly different for the PA-7000 Series.

The Ethernet interface types – Tap, Virtual Wire, HA, Layer 2, and Layer 3 – all use a common configuration interface. Select Network > Interfaces > Ethernet and then click the name of the interface to be configured to access this screen. The Config tab changes based on the configuration options available for the interface type that is selected.

Flexible Deployment Options For Ethernet Interfaces



Numerous methods can be used to integrate Palo Alto Networks firewalls into your environment. Many implementations evolve over time, and they transition between some or all of these possible configurations.

Let's review some of the few Ethernet interfaces that can be utilized and employed based upon your deployment method:

- **Tap:** Using Tap interfaces, the firewall can be connected to a core switch's span port to identify applications running on the network. This option requires no changes to the existing network design. In this mode the firewall cannot block any traffic.
- **Virtual Wire:** Using Virtual Wire interfaces, the firewall can be inserted into an existing topology without requiring any reallocation of network addresses or redesign on the network topology. In this mode, all of the protection and decryption features of the device can be used. NAT functionality is provided in this mode.

- Layer 2: Using Layer 2 interfaces, all of the protection and decryption features of the firewall can be used for trunk (VLAN) interfaces. Layer 3 support, for VLAN switching, can be employed with VLAN interfaces.
- Layer 3: Using Layer 3 interfaces, the firewall can take the place of any current enterprise firewall deployment.

A unique advantage of the firewall is the ability to mix and match these interface types on a single device. The same firewall can be deployed in Tap mode for one portion of the network and be in Virtual Wire mode for another

TAP Interfaces:

Interface for receiving data from a mirror port on a switch. Generally used to gather data on the network in preparation for building security policies prior to cutover.

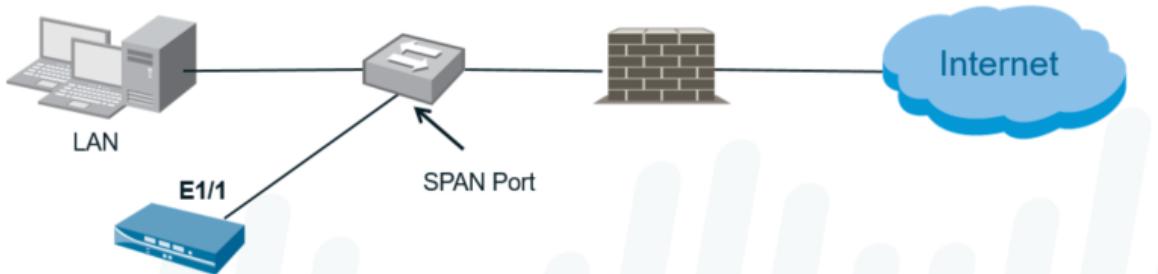
TAP cannot do anything with the traffic, be it control or shaping.

TAP must be assigned to a TAP security zone.

An Any/Any/Allow rule set with source/dest zones to the TAP zone the interface is in is needed to start this data gathering, or the data is dropped by the FW in the default deny rule.

Ethernet Tap Mode

- Tap mode deployment allows the capability to passively monitor traffic flows across a network by way of a switch SPAN or mirror port
- Firewall cannot perform traffic shaping or blocking
- Must be assigned to a security zone for ACC and reporting capabilities



Tap mode deployment allows the ability to passively monitor traffic flows across a network by way of a switch SPAN or mirror port.

- Useful for evaluating and auditing an existing network.
- No network or design changes are needed.

By using Tap interfaces, the device can be connected to a core switch's SPAN or mirror port to identify applications running on the network. This option does not require changes to the existing network design. In this mode, the device cannot block traffic or filter based on URL.

If the SPAN port passes encrypted traffic, the Tap interfaces support only SSL inbound decryption. An internal server certificate must be installed on the firewall and a decryption policy must be defined for the traffic to be decrypted. Decryption is discussed in detail later in this course.

Configuring Tap Interfaces

Network > Interfaces > Ethernet

The screenshot shows the FortiGate management interface under the 'Network > Interfaces > Ethernet' section. The left sidebar has 'Interfaces' selected. The main window shows a table of interfaces:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router
ethernet1/1	Layer3		green	none	none
ethernet1/2	Layer3	allow-ping	green	172.16.12.1/24	Student-VR-
ethernet1/3	Layer3	allow-all	green	192.168.12.1/24	Student-VR-
ethernet1/4			red	none	none
ethernet1/6			red	none	none

A modal dialog box titled 'Ethernet Interface' is open for 'ethernet1/6'. It shows the following configuration:

- Interface Name: ethernet1/6
- Interface Type: Tap
- Allow Profile: None
- Comment:
- Config tab is selected.
- Assign Interface To: Security Zone: WW-Zone

Two callout boxes highlight specific settings: 'Interface Type' points to the 'Tap' setting in the modal, and 'Security Zone' points to the 'WW-Zone' selection in the 'Assign Interface To' dropdown.

Even though Tap interfaces do not pass traffic like the other interfaces, a zone assignment still is required. Policies are required for logging, and policies require zones to work. To allow logging, policies are configured with the source and destination zones set to the zone that contains the Tap interface.

Virtual Wires Interfaces:

When using Virtual Wire interfaces, the device can be inserted into an existing topology without requiring any reallocation of network addresses or redesign on the network topology. In this mode, all of the protection and decryption features of the device can be used. If

necessary, a virtual wire can block or allow traffic based on the virtual LAN (VLAN) tag values. NAT functionality is provided in this mode.

A Virtual Wire is defined in two steps: creating the Virtual Wire object and configuring the Virtual Wire interfaces that the object connects. These steps can be done in any order.

A Virtual Wire interface binds two physical interfaces together. A Virtual Wire is also referred to as a “Bump in the Wire” or “Transparent In-Line”. No MAC or IP address assigned to the interface.

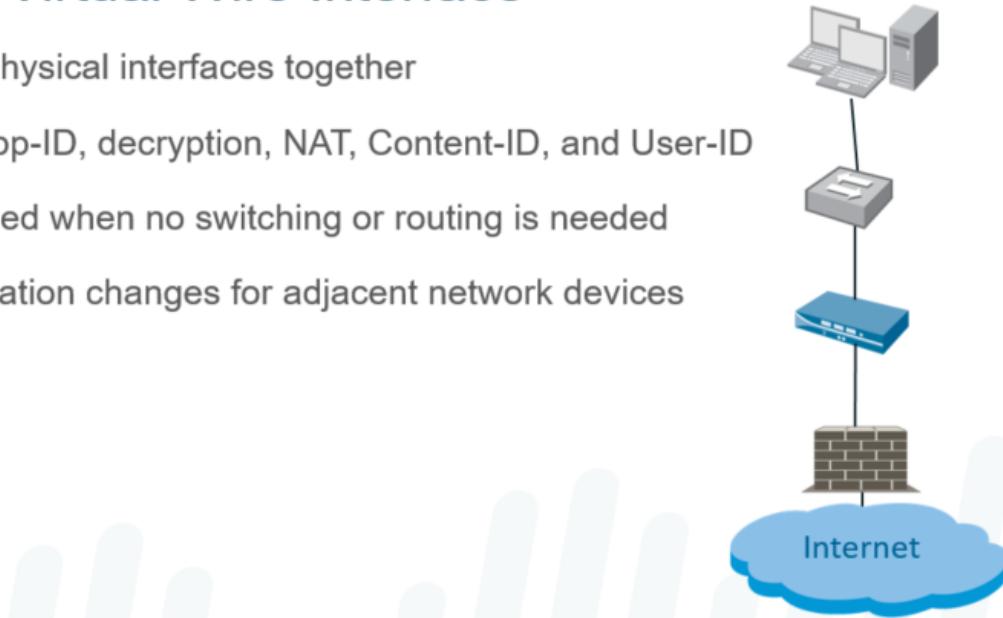
Ethernet ports 1 and 2 are configured as a Virtual Wire by default for certain models. The trust zone can send traffic to zone untrust by default.

A Virtual Wire interface supports App-ID, Decryption, NAT, Content-ID, and User-ID. The Virtual Wire does not support routing or device management.

A Virtual Wire interface typically is used when no switching or routing is required. No configuration changes are needed for adjacent network devices.

Ethernet Virtual Wire Interface

- Binds two physical interfaces together
- Supports App-ID, decryption, NAT, Content-ID, and User-ID
- Typically used when no switching or routing is needed
- No configuration changes for adjacent network devices



This is used as a L2 firewall installation in-line. This way, the firewall can be ‘dropped’ in without any reconfiguration of the network.

Interfaces will be L2, no IP's, L3 routing ,FW managment or IPSec termination point is available.

Create VWire instance, and add the interfaces if they have been set to VWire. If interfaces are not set, save the VWire instance and then go to the interfaces and add them into the VWire under interface type. A Vwire Zone is also needed.

Vwire fully supports 802.1q VLAN tagging, and will pass tagged and untagged traffic as long as there is a security policy to allow it.

Multiple VWire subinterfaces can also be created. Each sub-interface can be set in any zone, and set as L2 or L3 interfaces.

An L3 subinterface can be used for IP-routing, IPSec termination tunnels, and zone traffic routing and traffic control.

!

Configuring a Virtual Wire Object

- A Virtual Wire can allow or block traffic based on 802.1Q VLAN tags
 - 0 = untagged traffic
- Applies security rules to multicast traffic, enables Multicast Firewalling

Network > Virtual Wires > Add

Name	Interface1	Interface2	Tag Allowed	Multicast
vwire-object-1	ethernet1/5	ethernet1/7	1517	

Virtual Wire

Name: vwire-object-1
Interface1: ethernet1/5
Interface2: ethernet1/7
Tag Allowed: 1517
Enter either integers (e.g. 10) or ranges (100-200) separated by commas. Integer values can be between 0 and 4094.
 Multicast Firewalling
 Link State Pass Through

OK Cancel

If the Virtual Wire interfaces have not yet been configured, the interface fields can be left blank.

A Virtual Wire can block or allow traffic based on 802.1Q VLAN tag values. Specific tag numbers (0 to 4094) or a range of tag numbers (tag1-tag2) can be specified to limit the traffic allowed on the Virtual Wire.

A tag value of zero, which indicates untagged traffic, is the default. Multiple tags or ranges must be separated by commas. Traffic that has an excluded tag value is dropped. Tag values are not changed on incoming or outgoing packets.

To allow all traffic, tagged and untagged, set Tag Allowed to 0-4094.

To apply security rules to multicast traffic, select the Multicast Firewalling check box. If this setting is not enabled, multicast traffic is forwarded across the Virtual Wire.

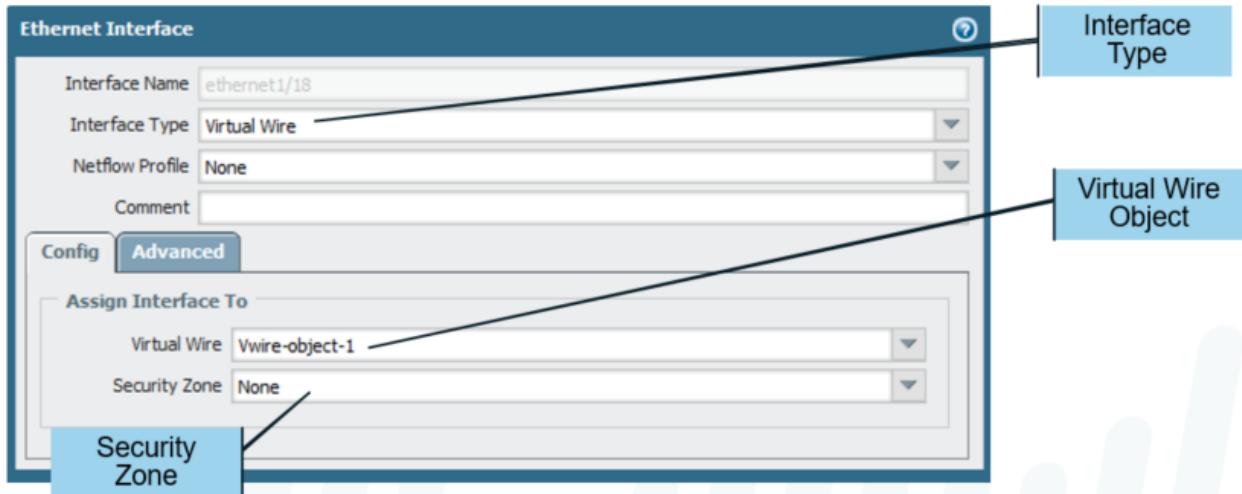
If the Virtual Wire object has not been configured, the Virtual Wire field can be left blank. The interface names can be specified when the Virtual Wire object is created.

A zone is required because traffic will flow between Virtual Wire interfaces. Only zones that match the interface type are listed in the pull-down menu in the interface.

The firewall can generate and export NetFlow Version 9 records with unidirectional IP traffic flow information to an outside collector. NetFlow export can be enabled on any ingress interface in the system. This feature is available on all platforms except the PAN-4000 Series models.

Configuring Virtual Wire Interfaces

Network > Interfaces > Ethernet



Layer 2 Interfaces:

Layer 2 switches traffic between 2+ interfaces. This makes the networks into a single ether broadcast domain.

Steps to create a Layer 2 interface:

create a vlan object under Network >

configuring the L2 interfaces

L2 does not participate in STP, but forwards STP packets.

L2 can do SSL Decrypt, User-ID, App-ID, Content ID, QoS.

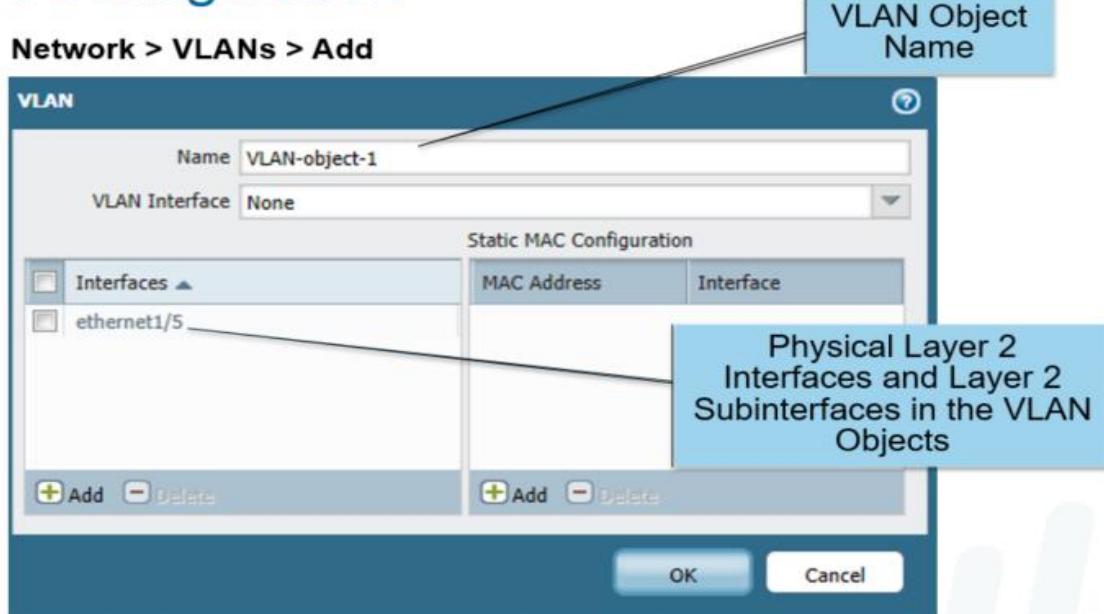
Cannot do FW management, as no IP address.

Subinterfaces can be added to an 802.1q vlan

More than one VLAN can be added to the same top level port (example: e1/1.1 in vlan1 and e1/1.2 in vlan2). However, as there is no routing function, an external router, and security policies would be needed to route the data between the vlans.

Best practice is to use L3 subinterfaces to provide inter-VLAN routing.

VLAN Configuration



Layer 3 Interfaces:

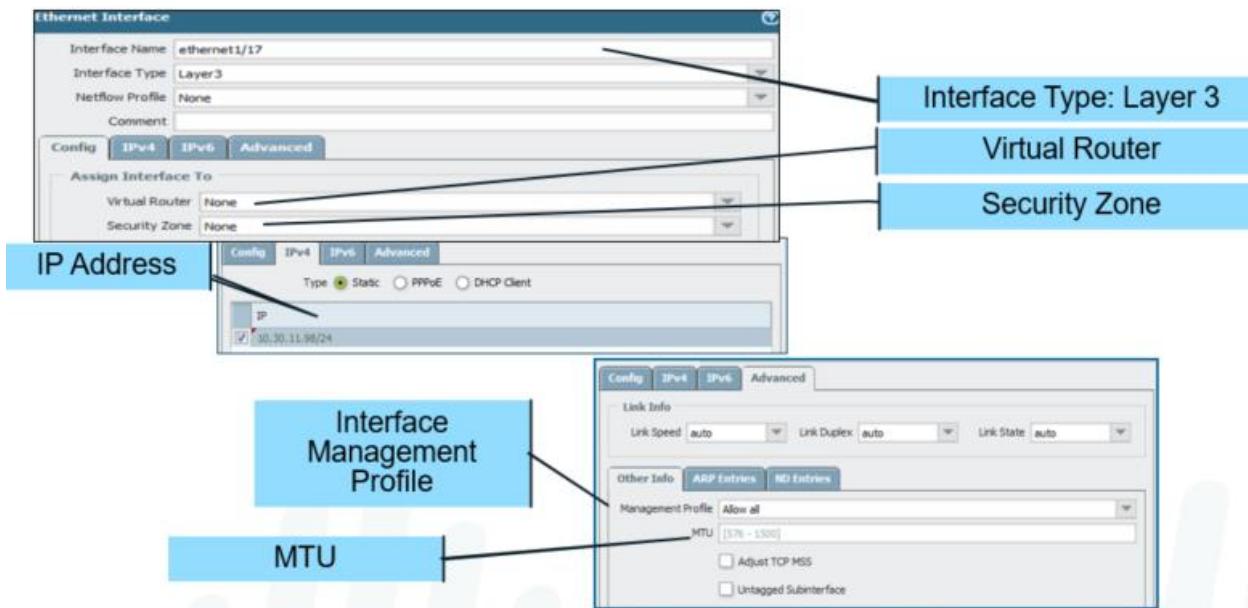
Configuring a Layer 3 Interface

Network > Interfaces > Ethernet

- Interface Type: Layer 3
- Security zone
- IP address
 - Static or DHCP client
 - DHCP server or DHCP relay
- Interface management profile
 - Allows or denies management protocols like SSH and HTTP on the MGT interface
- Virtual router
 - Contains a set of static and dynamic routes used by a specified group of interfaces

Configuring a Layer 3 Interface

Network > Interfaces > Ethernet



To configure a Layer 3 interface, the minimum required properties are the IP address, zone, and virtual router.

When the Palo Alto Networks firewall operates in the Layer 3 mode, it can provide routing and Network Address Translation functions.

All Layer 3 interfaces in a specific virtual router share the same routing table.

Layer 3 interfaces can be configured as a DHCP client for situations where the firewall must have a dynamically assigned IP address.

Layer 3 interfaces can also be configured to provide access to the management interfaces by assigning them a management profile.

The local MTU setting on an interface overrides the global MTU setting set in Session Settings. To enable jumbo frames on the device and set a default global MTU value, select Device > Setup > Session and edit the Session Settings.

You can assign multiple IP address to the same interface, though they shouldn't be in the same subnet.

You can configure the firewall to be a Point-to-Point Protocol over Ethernet (PPPoE) termination point to support connectivity in a digital subscriber line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.

You can configure the firewall interface to act as a DHCP client and receive a dynamically assigned IP address. The firewall also provides the capability to propagate settings received by the DHCP client interface into a DHCP server operating on the firewall. This capability is most commonly used to propagate DNS server settings from an Internet service provider to client machines operating on the network protected by the firewall.

The default gateway received from the DHCP server is injected into the routing table as a default route.

Assigning an IP Address to an Interface

Network > Interfaces > Ethernet

The screenshot shows the 'Ethernet Interface' configuration window in Winbox. The interface name is set to 'ethernet1/2'. The 'Interface Type' is selected as 'Layer3'. In the 'IPv4' tab, the 'Type' is set to 'Static', and an IP address '192.168.78.1/24' is listed with a checked checkbox. The window also includes tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced', and buttons for 'OK' and 'Cancel'.

Layer 3 is able to route data between networks.

Each L3 interface needs an IP assigned.

App-ID, Content-ID, User-ID, SSL Decrypt, NAT, QoS are supported.

Can support management as it has an IP (further config would be needed).

Support both IPv4 and IPv6, and support dual stack. (IPv6 must be enabled before it is available).

When configuring interfaces you'll need:

Interface type (L3)

IP Address

Security Zone

Virtual Router (only if you want to route traffic to/from interface).

IPv6:

Interfaces can be set for Static, DHCP or PPPoE

Link Local address prefix is prepended EUI64 interface ID (IPv6)

Enable duplicate address detection can be enabled (ipv6)

Can also be configured to send ipv6 router advertisements (IPv6)

Can also include dns info in ipv6 router advertisements (IPv6)

Advanced Tab (interface)

Link speed, Duplex Settings, MTU setting

Altering the MTU will override the default jumbo frame and default MTU in session settings

TCP-MSS can be updated

Interface management profile can be set here

ARP entries can be manually added (ND entries can be added for IPv6)

LLDP can be enabled and configured from the LLDP tab

Management Profile:

By default, any management traffic sent to or from the firewall goes through the out-of-band management (MGT) interface. Alternatively, a Layer 3 interface can be used to source this traffic and also receive inbound management traffic.

Management features enabled by the profile can be restricted to a specific IP address with the Permitted IP Addresses panel. If configured, only the IP addresses listed can use the services selected when the profile is defined. If the field is left blank, the profile allows any IP address to use the configured services.

Profile can be applied to an L3 interface. Protocols that can be allowed or denied are:

Ping, Telnet, SSH, HTTP, HTTP-OCSP, HTTPS, SNMP, Response Pages, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP

Can be assigned to L3, loopback and tunnel interfaces (interfaces that have an IP address).

Security Policies are required to allow traffic to non-MGT interfaces

Can have a ‘permitted IP’ list that will only allow a specific source IP address or subnet access to that specific set of permitted services.

Interface Management Profile

- Defines which management functions are allowed on a traffic interface
- Management profiles are applied to Layer 3 interfaces

Network > Network Profiles > Interface Mgmt > Add



Layer 3 Sub-interfaces

Assigned to a Layer 2 802.1q vlan

different L3 sub-ints can be added to the same physical interface, but can only route at layer 3 between them if there is a route at (and security policy for the traffic) in the VR.

Configured under Network > Interfaces > Ethernet

The configuration is the same as a standard Layer 3 interfaces configuration, with the exception of adding a vlan tagged

Untagged L3 sub-ints can be used, but the ‘untagged interface’ must be selected on the main interface advanced tab.

Virtual Routers:

Used for Layer 3 IP routing

Supports one or more static routes

Supports multiple dynamic routing protocols, including RIPv2, OSPFv2, OSPFv3, BGPv4

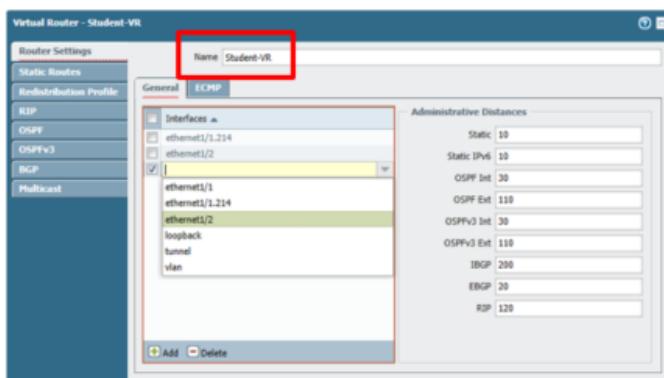
Supports Multicast routing protocols PIM-SM and PIM-SSM (both using pimv2)

IGMP v1, v2, v3 are also supported on host-facing interfaces.

Virtual Routers

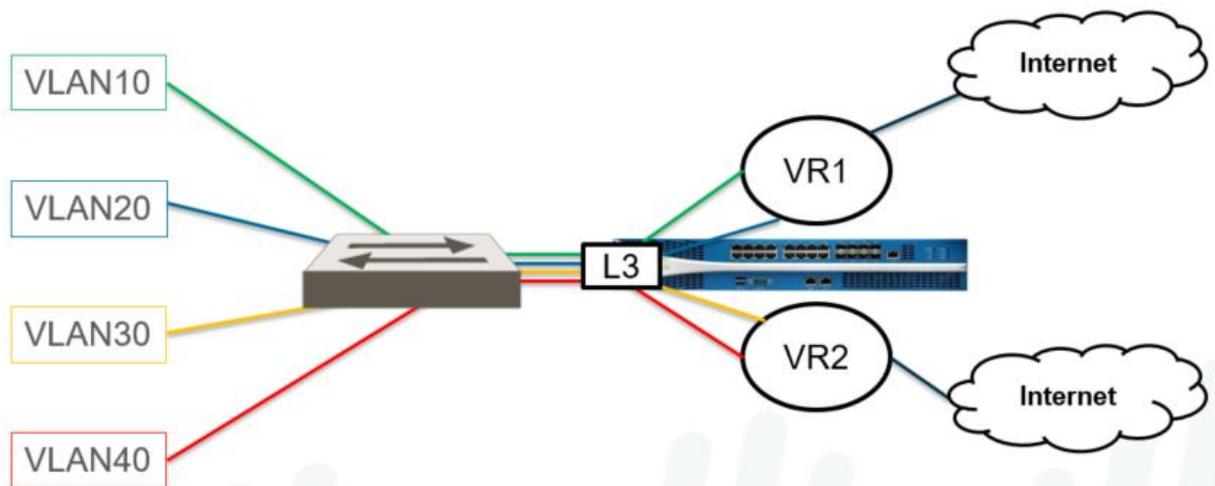
- All interfaces assigned to a virtual router share the same routing table
 - The routing table of a virtual router can be defined by static and dynamic (RIP, OSPF, BGP) routes
 - Allows for the configuration of different routing behavior for different interfaces

Network > Virtual Routers



Virtual routers can be linked together so that traffic can be routed between more than one virtual router.

Multiple Virtual Routers



Configure under Network > Virtual Routers

Give Name

Add L3 main, sub ints or tunnel interfaces

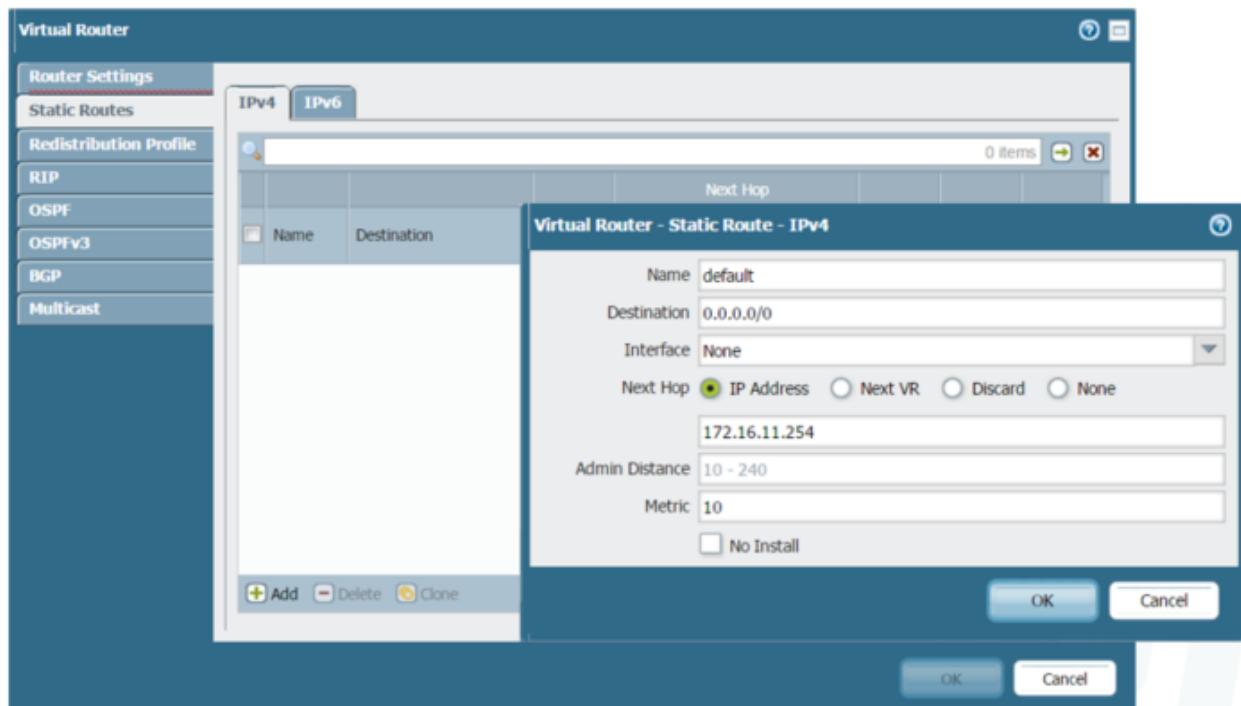
When interfaces are added, the connected routes are automatically populated into the routing table for traffic forwarding

Administrative Differences are used to determine routing decisions when identical destination routes are present.

To add a default static routes:

Virtual Router Static Routes

Network > Virtual Routers



click: Network > Virtual Routers > Static Routes > Add

Give the VR a name

add a default of [0.0.0.0/0];(https://0.0.0.0/0;) specify the interface this route will forward packets on (security policy will be needed to route the traffic).

Set the next hop type from the list: IP Address, Next VR, Discard or None. Typically a default route is sent to a next hop IP address (upstream to an edge router or ISP link). Next VR sends it to the specified Virtual router (not this one), Discard will Discard (and no log). None is used if there is no text hop for the route.

Set any changes to the admin distance that are needed. Administrative distance defaults are specified by the type of route (static, connected, ospf, bgp, etc). leaving this blank will set it to the default value.

Set any metric changes desired. This is useful if you have multiple links out and want to prefer one over the other. If the preferred link fails, the other route can be used to forward packets.

Select which routing table to install the route in: Unicast, Multicast, Both or no install. No install would stage the route, but would not be actively used.

Bi-Directional Forwarding can be selected. Both endpoints must support BFD. (see docs for more details)

BFD is not supported on the PA-200 or the PA-500

Multiple Static Default Routes

Multiple SDR's can be configured

Route with lowest metric will be installed in the forwarding table

Path Monitoring can be used to determine if the route is usable.

if Path Monitoring detects a failure, FW will switch to the higher metric route until the lower metric path is restored.

Virtual Router Dynamic Routes

Standards-based support for:

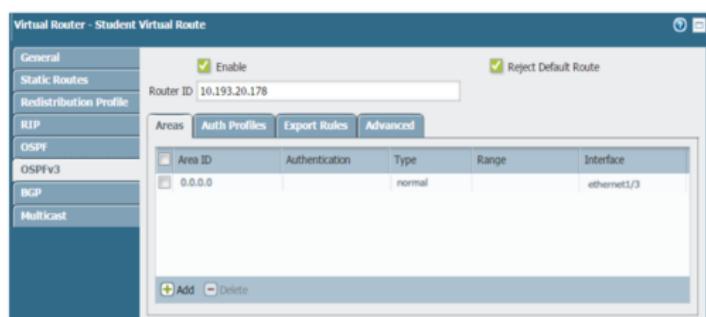
- OSPF v2 and v3
- RIP v2
- BGP v4

Routing support across IPsec tunnels

Multicast routing support for:

- PIM-SM
- PIM-SSM
- IGMP

Network > Virtual Routers



Virtual routers provide support for static routing and dynamic routing using the Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, and Border Gateway Protocol (BGP).

The multicast routing feature allows the firewall to route multicast streams using Protocol Independent Multicast Sparse Mode (PIM-SM), and PIM Source Specific Multicast (PIM-SSM) for applications such as media broadcasting (radio and video) with PIMv2.

The firewall performs Internet Group Management Protocol (IGMP) queries for hosts that are on the same network as the interface in which IGMP is configured. PIM-SM and IGMP can be enabled on Layer 3 interfaces.

IGMP v1, v2, and v3 are supported. PIM and IGMP must be enabled on host-facing interfaces.

Standards-based support for OSPF: With PAN-OS 6.0, OSPF v2 and OSPF v3 are supported.

Path Monitoring can be configured under: Network > Virtual Routers > Static Routes > Add

On the bottom of the static route configuration, click the check on Path Monitoring

Multiple failure conditions can be added. single or multiple source/dest entries can be set as criteria. select either 'any' or 'all' when configuring more than one condition.

On the source IP, a drop-down provides all IP's configured on the firewall. Generally the IP on the interface being configured for path monitoring is selected.

Add the destination IP to send ping requests

Set interval for ping interval and ping counts.

If the lowest metric link fails monitoring, and then is restored, the 'Preemptive hold time' setting will be the timeout that the firewall will wait before failing traffic back to the lower metric link. This is defaulted to 2 minutes, but can be changed.

Troubleshooting Routing:

The 'More Runtime Stats' on the Network > Virtual Routers page will pull up a new screen to show the stats on the current VR.

Routing and Route table has all known routes (RIB)

Forwarding Table has all routes of where traffic will be forwarded to (FIB)

Static Route Monitoring tab will show the status of all Path Monitors configured.

The More Runtime Stats link displays detail tabs to check the configuration of the supported dynamic routing protocols: RIP, OSPF, and BGP.

Troubleshooting Dynamic Routing

- Confirm virtual router runtime stats
- On the active firewall,
select **Network > Virtual Router** and click **More Runtime Stats**

	Name	Interfaces	Configuration	RIP	OSPF	BGP	Multicast	Runtime Stats
	default	ethernet1/1 ethernet1/1.1... ethernet1/2 ethernet1/2.1... ethernet1/5 ethernet1/5.1 ethernet1/5.2 more...	Static Routes: 4		Enabled Area Count: 2 Subnet Count: 6 Neighbor Count: 1 Virtual Link Count: 0 Virtual Neighbor Count: 0			More Runtime Stats

More Runtime Stats

- The routing table shows internal network routes and shows default routes propagated from the upstream routers.

Network > Virtual Router > More Runtime Stats

Routing	RIP	OSPF	BGP	Multicast	Route Table						
Protocol	Protocol	Protocol	Protocol	Protocol	Destination	Next Hop	Metric	Flags	Age	Interface	
					0.0.0.0/0	172.20.6.254	10	A S		ethernet1/1.106	
					172.20.1.0/24	172.20.6.254	11	A Oi	83757	ethernet1/1.106	
					172.20.2.0/24	172.20.6.254	11	A Oi	83757	ethernet1/1.106	
					172.20.3.0/24	172.20.6.254	11	A Oi	83757	ethernet1/1.106	
					172.20.4.0/24	172.20.6.254	11	A Oi	83757	ethernet1/1.106	
					172.20.5.0/24	172.20.6.254	11	A Oi	23385	ethernet1/1.106	
					172.20.6.0/24	0.0.0.0	10	Oi	83757	ethernet1/1.106	
					172.20.6.0/24	172.20.6.1	0	A C		ethernet1/1.106	
					172.20.6.1/32	0.0.0.0	0	A H			
					172.20.7.0/24	172.20.6.254	11	A Oi	80491	ethernet1/1.106	

VLAN Interfaces:

VLAN are Layer 2 802.1q network

VLAN objects can be assigned and IP address, and connected to Layer 3 networks for Layer 3 routing

Configure under Network > Network > VLAN > Add

All vlan interfaces will start with ‘vlan’ – add the ID number (NOT a vlan ID, but matching them is recommended to avoid confusion).

Interface must be assigned to an exiting vlan

If one doesn’t exist or a new VLAN interface is needed, selecting ‘New VLAN’ on the drop down can be done to create a new VLAN.

Select the virtual router to add the interface to

Select the Security Zone to add the interface to.

Loopback Interfaces:

Loopbacks are logical interfaces that do not have a physical presence. They are assigned in a security zone and can be reached by their IP through another physical main or sub interface.

Typical use includes Management UI access, Global Protect interface, or IPSEC tunnel interface termination point.

Configure under Network > Interfaces > Loopback

Loopback interfaces always start with ‘loopback’, which cannot be changed. the ID number is set by the admin

Configured the same as a Layer 3 interface; Only exception is a loopback IP must be a /32 host IP.

Set the VR and the Security Zone the LB will be added to.

Policy-Based Forwarding:

Normally, when traffic enters the firewall, the ingress interface virtual router dictates the route that determines the outgoing interface and destination security zone based on the destination IP address.

With policy-based forwarding (PBF), you can specify other information to determine the outgoing interface, including:

- Source and destination IP addresses
- Source zone
- Source user
- Destination application
- Destination service

The initial session on a given destination IP address and port that is associated with an application does not match an application-specific rule. The session is forwarded according to subsequent PBF rules that do not specify an application or the forwarding table of the virtual router.

All subsequent sessions on that destination IP address and port for the same application matches an application-specific rule.

To ensure forwarding through PBF rules, application-specific rules are not recommended.

Policy-Based Forwarding

Supersedes the forwarding information in the virtual router



- Reverts to the virtual router table if the PBF policy destination is unreachable
- A single session is forwarded by the PBF policy the same way

PBF rules are used to send specific traffic to an interface that is not the default route the traffic would follow from the routing table.

Use cases would include a private leased line you want to use for unencrypted traffic or traffic that needs low latency (VoIP, etc), while letting non-critical encrypted traffic over a DIA (direct internet access) circuit using an IPSec Tunnel.

PBF can be set using specific criteria, including source zone or interface, source user, destination IP and/or port.

Includes a Path Monitoring feature; if the interface the PBF is sent out goes down, the traffic will be able to go out the other interface.

[Configure under Policies > Policy Based Forwarding](#)

Name the Policy

Enter the criteria: Source IP, Zone and/or User-ID

Specify destination/application/service. It is NOT recommended to use the application, as it may take several packets to identify the traffic, and it may not be forwarded based on the PBF.

Enter the details of where the traffic will be forwarded, including egress interface and optional next-hop. The Path Monitoring can also be configured.

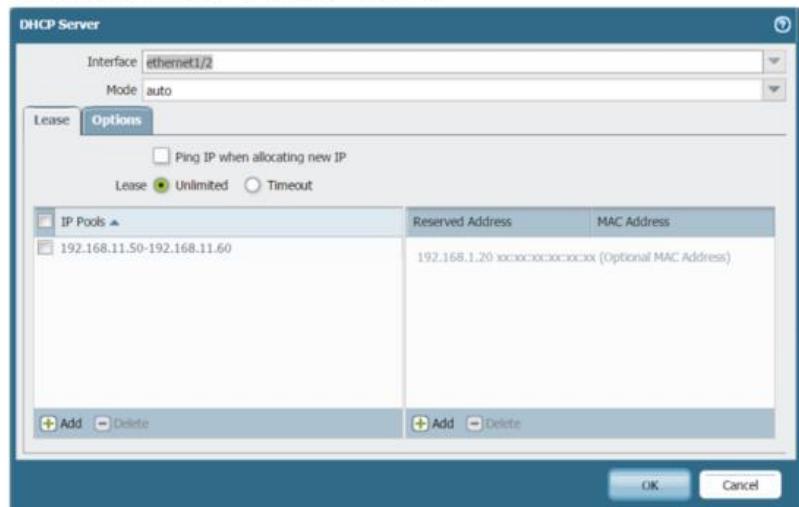
Symmetric Return can also be set to be enforced here.

DHCP in Palo Alto:

DHCP Server

- When an interface is configured as a DHCP server, it assigns addresses to DHCP clients

Network > DHCP > DHCP Server

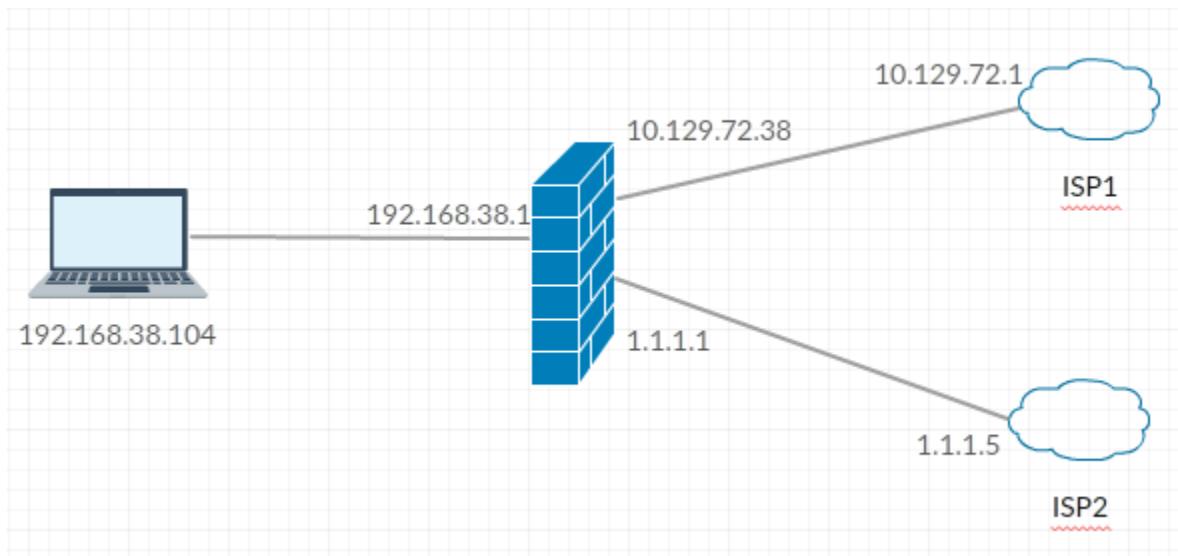


ECMP (Load Balancing) on the Firewall:

Equal Cost Multipath (ECMP) is a new feature introduced in PAN-OS 7.0. It provides multipath support for "equal cost" routes going to the same destination. There is a max of 4 equal cost paths supported. ECMP load balancing is done at the session level, not at the packet level—the start of a new session is when the firewall (ECMP) chooses an equal-cost path.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Layer3	allow-ping		10.129.72.38/24	default	Untagged	none	L3-Untrust
ethernet1/3	Layer3	allow-ping		192.168.38.1/24	default	Untagged	none	L3-Trust
ethernet1/11	Layer3	allow-ping		1.1.1.1/24	default	Untagged	none	VPN

Note: ethernet1/1 and ethernet1/11 are ISP interfaces configured in different zones L3-Untrust and VPN respectively. However, these interfaces can be configured in same zone also



Route configuration with both default routes having "equal-cost"

✓	Name	Destinat...	Interface	Next Hop		Admin Distance	Metric	BFD
				Type	Value			
<input type="checkbox"/>	default-1	0.0.0.0/0	ethernet1/1	ip-address	10.129.72.1	default	10	None
<input checked="" type="checkbox"/>	default-2	0.0.0.0/0	ethernet1/11	ip-address	1.1.1.5	default	10	None

NAT policy to be able to route traffic over internet:

Original Packet									
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
1	Trust-NAT	none	└─ L3-Trust	└─ L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 10.129.72.38/24
2	Trust-NAT-1	none	└─ L3-Trust	└─ VPN	any	any	any	any	dynamic-ip-and-port ethernet1/11 1.1.1.1/24

Note: If both ISP interfaces are in the same zone, then destination interfaces need to be added to the NAT policy as in the following screenshot:

Original Packet									
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation
1	Trust-NAT	none	└─ L3-Trust	└─ L3-Untrust	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 10.129.72.38/24
2	Trust-NAT-1	none	└─ L3-Trust	└─ L3-Untrust	ethernet1/11	any	any	any	dynamic-ip-and-port ethernet1/11 1.1.1.1/24

Security policy configuration to allow the traffic: (covers both scenario when interfaces are in same or different zone)

	Name	Source		Destination		Application	Service	Action
		Zone	Address	Zone	Address			
1	Trust-to-Untrust-2	L3-Trust	any	L3-Untrust VPN	any	any	any	Allow
2	intrazone-default	any	any	(intrazone)	any	any	any	Allow
3	interzone-default	any	any	any	any	any	any	Deny

Enabling ECMP on the firewall:

Interface	Weight

Route installed for ECMP has a "E" flag in it:

Destination	Next Hop	Flags	Interface	MTU
0.0.0.0/0	10.129.72.1	uge	ethernet1/1	1500
0.0.0.0/0	1.1.1.5	uge*	ethernet1/11	1500

Note:

- Max Path 2 means that only 2 equal cost paths will be installed in FIB table. If there are more than 2 equal-cost paths that need to be installed in FIB table, change Max Path value. Max supported value is 4.
- Load balance method can be selected according to the requirement. For more information about load balance algorithm, please click [here](#)
- Enable Symmetric Return if reply packet should be sent out the same interface that the request packet came in.

```

admin@Lab70-38-PA-5020> show routing fib virtual-router default ecmp yes
total virtual-router shown : 1

-----
virtual-router name: default
interfaces:
  ethernet1/1 ethernet1/3 ethernet1/11

route table:
flags: u - up, h - host, g - gateway, e - ecmp, * - preferred path

maximum of fib entries for device: 64000
maximum of IPv4 fib entries for device: 32000
maximum of IPv6 fib entries for device: 32000
number of fib entries for device: 8
maximum of fib entries for this fib: 64000
number of fib entries for this fib: 8
number of fib entries shown: 2

destination      nexthop      flags  interface      mtu  weight  hit  nh_id/mask
----- 0.0.0.0/0      10.129.72.1    uge   ethernet1/1    1500 100  19609  0/1
                           1.1.1.5       uge*  ethernet1/11   1500 100  19601  1/1
-----
```

----- END -----

Day 05 and 06

1. Security Policies

IntraZOne

InterZone

Universal

Unused Rules

Actions (Allow, Deny, Drop, reset client, reset server, Reset Both)

Profile Setting

Log Setting

Policy Schedule

2. NAT

Dynamic NAT

Dynamic IP and Port

Static NAT

Destination NAT

- 1. Destination NAT Example—One-to-One Mapping**
- 2. Destination NAT Example—One-to-Many Mapping**
- 3. Destination NAT with Port Translation Example**

U-Turn NAT

- 1. WebServer in same Zone**
- 2. Webserver in Diffirent Zone**

!

show running security-policy

test security-policy-match from trust to untrust application web-browsing

show session id

show log traffic show-tracker equal yes

show running nat-policy (View NAT rules on the dataplane)

show running global-ippool (View NAT pools by index)

show running ippool (View NAT pools in use)

test nat-policy-match from L3-untrust to L3-untrust destination 172.16.5.1 source 15.1.3.71 protocol 255

Security Policy fundamental concepts:

- > All traffic must match a session and security policy (stateful firewall)
- > Basics are a source and destination zone
- > Granular includes Source/Dest Address, ports, application, URL Categories, Source user and HIP profiles.
- > Sessions are established for bidirectional data flow.

Policies > Security has the current security rules

Three types of security rules:

- > Intrazone – all traffic within a zone. this traffic is allowed by default.
- > Interzone – all traffic between zones. This traffic is blocked by default.
- > Universal – Allowing all traffic between source and destination. combines intra and interzone traffic.

1. Any created rules have traffic logged by default; system created rules (intra/interzone at the end) are not logged.
2. Rules are evaluated from top to bottom; when a match is found, no further eval is done.
3. Rule Shadowing is when multiple rules match the same scope of traffic.

Security Policy Rule Match Conditions

Policies > Security

	Name	Type	Zone	Address	User	Zone	Address	Application	Service	URL Category	Action	Profile
1	Inbound FTP	universal	pqr Untrust-L3	any	any	pqr Trust-L3	172.16.11.1	ftp	application-d...	any	Allow	none
2	Allow YouTube	universal	pqr Trust-L3	any	any	pqr Untrust-L3	any	youtube	application-d...	any	Allow	none

Rule Type

Interfaces are assigned to Security Zones

User includes one or more individuals and/or groups

HTTP/S only

Address is one or more of:
Address
Address group
Block list
Region/Country-based enforcement

Application includes one or more of:
Applications
Application groups
Application filters

The security policy consists of a list of security policy rules. Each security policy rule consists of objects that describe the endpoints of the communication and the traffic to be matched. Rules can be as specific as required. They are built using objects that hold values of addresses, applications, users, and services.

The configured action, deny or allow, is taken only if a session matches all defined fields of the security policy rule. If a match is not made, the session is compared against the next policy rule on the list. When a match is found, no further policy rules are checked.

Security Policy:

When a session is initiated, the source and destination zones and addresses are determined and the policy rule base is checked. A rule base exists for each zone pair. Rules can be created with multiple source and destination zones, which is commonly done to define access to a DMZ resource that is used in a similar fashion by clients in internal and external zones.

If a rule matches the addresses and can match the application, the session is allowed and the system begins to examine the traffic to determine if the application is in use. For this reason, it can be beneficial to configure specific or default ports for the applications being allowed. If the service is defined as “any”, all sessions must be allowed to proceed until the point where application-layer data is exchanged. Then the firewall can determine which application is inside

the session. If the service is anything but “any”, then many unwanted connections can be dropped immediately. If the traffic and resulting application do not match any rule, the session is dropped.

The policy rules are uni-directional, which means they only allow traffic that is initiated in the direction the policy rule specifies: source zone(s) to destination zone(s). The replies to the client are always allowed as part of the policy. If traffic is intended to be initiated in both directions (bi-directional), two uni-directional policy rules are recommended: one for each direction. You can accomplish the same task by slightly modifying the original rule and turning it into a bi-directional rule.

Security Policy

- List of policy rules is evaluated from the top down
 - The first rule that matches the traffic is used
 - After the match, no further rules are evaluated

Policies > Security

	Source							Destination								
	Name	Tags	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action	Profile			
1	Inbound FTP	none	universal	Untrust-L3	any	any	any	Trust-L3	172.16.11.1	ftp	application-l...	Allow	none			
2	General Internet	none	universal	Trust-L3	any	any	any	Untrust-L3	any	dns	application-l...	Allow	none			
										http						
										ping						
										telnet						
										web-browsing						
3	Allow YouTube	none	universal	Trust-L3	any	any	any	Untrust-L3	any	youtube	application-l...	Allow	none			
4	Allow Facebook	none	universal	Trust-L3	any	any	any	Untrust-L3	any	facebook	application-l...	Allow	none			
5	intrazone-default		intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none			
6	interzone-default		interzone	any	any	any	any	any	any	any	any	Deny	none			

Three Security Policy Rule Types:

PAN-OS has defined rule types for security policies. These rule types are indirectly related to zones, so it is important to understand how these rule types are applied to security zones and how they can be configured within a security policy.

Security policies use “zone rule types” to regulate and log traffic.

The two predefined security rule types behave as follows:

- intrazone-default: default action is to allow all traffic within the same zone.
- interzone-default: default action is to deny all traffic traversing from one zone into another.

Efficient rule-base management is enabled because only a single rule handles the intrazone traffic for a set of zones without affecting the interzone traffic, and vice versa. All intrazone

traffic can be denied without explicit rules by creating a “catch-all” rule. An “any any any deny” rule is no longer needed.

Enable logging on intrazone and interzone traffic.

- Logs that are associated with intrazone-default and interzone-default rules are treated the same as any other logs from other rules.
- No longer need to create explicit rules for every zone pair just to see logs.

Security profiles can be enabled on the intrazone and interzone rules.

- When you define a security policy rule, you must specify the source and destination security zones of the traffic. Separate zones must be created for each type of interface (Layer 2, Layer 3, Virtual Wire, Tap) and each interface must be assigned to a zone before it can process traffic. The interfaces of the firewall themselves are assigned to a specific zone and may be assigned to only a single zone. Though, a security zone can have multiple interfaces assigned to it.
- Security policies can be defined only between zones of the same type. Security policies are evaluated in the order they are listed in the firewall. Traffic is compared against each rule in the list. If the traffic matches the rule no further rules are evaluated. If the rule does not match the next subsequent rule is checked.

A Palo Alto Networks firewall enforces two default rules if traffic has not matched any user-defined security policies. These are our predefined security rules for intrazone and interzone traffic:

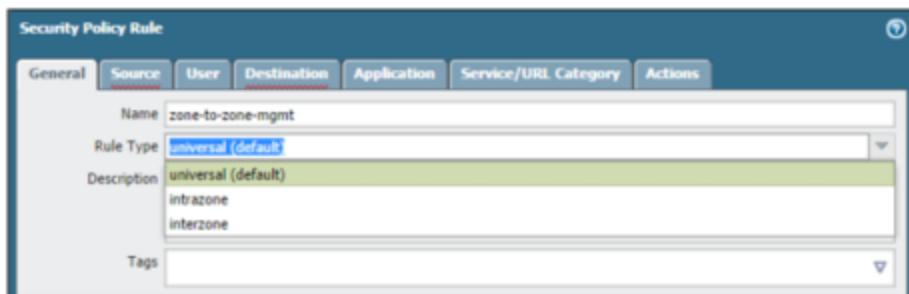
- Traffic within a single zone is allowed (intrazone traffic).
- Traffic between two zones is denied (interzone traffic).

By default, these rules apply when traffic does not match any other security rule. Therefore, these two rules are processed after all of the defined rules of the firewall either from within the local device or from Panorama. These default rules do not generate traffic log entries by default. However, logging may be enabled, which allows you to see all the traffic that is hitting your firewall. To generate traffic logs, you must enable logging by overriding the rule.

Caution: An explicit “deny-all” rule at the end of the user-defined policies is processed before these predefined rules, which denies intrazone traffic.

Three Security Policy Rule Types

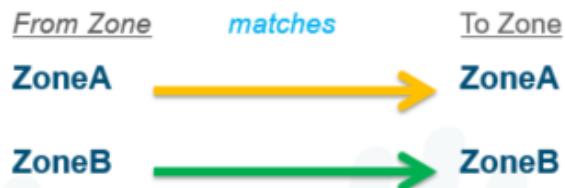
- **Intrazone:** Traffic within the same zone
 - Allowed by default
- **Interzone:** Traffic traversing from one zone to another
 - Denied by default
- **Universal (default):** Traffic applying to both zones (Intrazone and Interzone)
 - Behaves as normal: Checks the rule and applies the action



Rule Type Example: Intrazone

Intrazone Rule Type

	Name	Type	Source		Destination							
1	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	any	Allow	none	none



The intrazone rule type matches traffic within the specified source zone(s), but not between them. That is why you cannot specify a destination zone other than the hard-coded intrazone. For example, an intrazone rule with two source zones, in this case ZoneA and ZoneB, matches traffic only within its respective zone. Such as traffic:

- within ZoneA
- within ZoneB

So, traffic from ZoneA to ZoneA, and traffic from ZoneB to ZoneB match, and in this case be allowed.

Alternatively, interzone traffic (traffic that crosses from one zone to another) from ZoneA to ZoneB, and traffic from ZoneB to ZoneA, is not allowed.

Rule Type Example: Interzone

Interzone Rule Type

Name	Type	Source		Destination		Application	Service	Action	Profile	Options
		Zone	Address	Zone	Address					
interzone-default	interzone	any	any	any	any	any	any	Deny	none	none



The interzone rule type matches traffic between the specified source and destination zones and each rule can match on multiple source and destination zone pairs. For example, an interzone rule with source zones A and B, and destination zones A and B matches traffic as follows:

- from ZoneA to ZoneB
- from ZoneB to ZoneA

This rule does NOT match traffic within ZoneA, nor within ZoneB. The reason is that interzone rule type applies to traffic from any source zone to any destination zone. It does not apply to traffic within a zone, even if the same zone is listed in the Source and Destination columns.

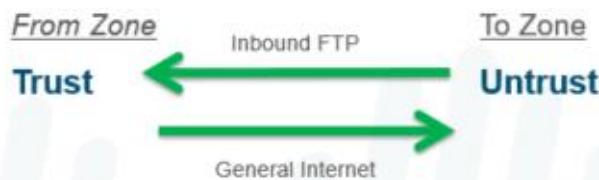
In this example, traffic from ZoneA to ZoneB, and from ZoneB to ZoneA, does match the rule and is allowed. However, traffic from ZoneA to ZoneA, and from ZoneB to ZoneB, does NOT match the rule and is not allowed.

Universal rule: The universal rule type matches intrazone and interzone traffic in the specified source and destination zones. This rule type is the default when creating a new security rule. When upgrading from a version previous to PAN-OS 6.1, all existing rules in the current security rule base are converted to universal rules.

Rule Type Example: Universal (The Default)

Universal Rule Type

Name	Type	Source Zone	Address	Destination Zone	Address	Application	Service	Action	Profile
1. Inbound FTP	universal	Untrust-L3	any	Trust-L3	172.16.11.1	ftp	application-ftp	Allow	none
2. General Internet	universal	Trust-L3	any	Untrust-L3	any	dns	application-dns	Allow	none



Enable Logging in Default Rules

- Two predefined default rules and both are "read only".
 - intrazone-default
 - interzone-default
- Use "Override" to configure additional settings
 - Enables the ability to turn on logging

Office Programs	none	universal	Trust-L3	any	any	any	Untrust-L3	any	Office Programs	application-default	Allow	
Inbound-FTP-Policy	none	universal	Untrust-L3	any	any	any	Trust-L3	172.16.14.1	ftp	application-ftp	Allow	
General Internet	none	universal	Trust-L3	any	any	any	Untrust-L3	any	dns	application-dns	Allow	
									flash	application-flash	Allow	
									http	application-http	Allow	
									ping	application-ping	Allow	
									tel	application-tel	Allow	
									web-browsing	application-web-browsing	Allow	
<hr/>												
intrazone-default	none	universal	untrustzone	any	any	any	any	any	any	any	any	Deny
interzone-default	none	universal	interzone	any	any	any	any	any	any	any	any	Deny
<hr/>												
Override												

Notice within the rule base that two predefined default rules are at the bottom. These two rules are "read only" and so these rules cannot be modified at this time. They are "grayed out" and not active for editing. To edit these rules, click the rule to be modified. Override becomes active, which allows you to change the default setting.

To enable logging, override the default and modify the rule as shown on the next slide.

Logging:

The default action for logging is to log only at the session end. Here we show how to enable session logging at session start and/or end only.

The Actions tab allows you to configure this predefined rule by setting the action, enabling logging, and to also modify the profile settings of your profile types.

The ability to enable logging is a key feature. Without it, a number of policies would need to be created in both directions just to enable intrazone traffic logging.

Benefits of enabling logging on Intrazone and Interzone traffic:

- Logs associated with the intrazone-default and interzone-default rules are treated the same as any other logs from other rules.
- This enables the ability to filter and see the traffic that is being blocked.

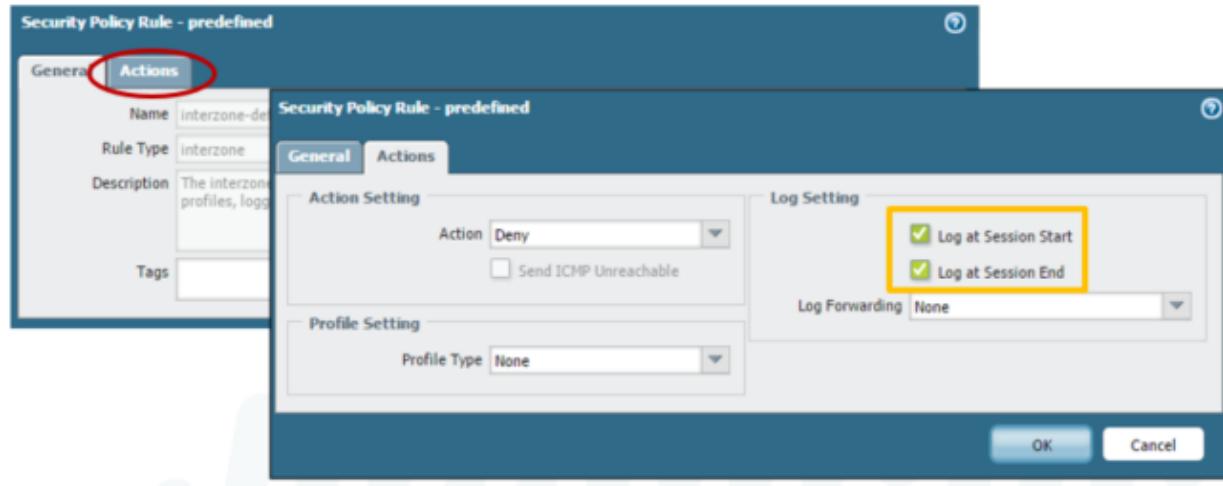
Best Practice:

Care should be taken when activating the Log at Session Start setting, as it can lead to significant logging pressure depending on the type of traffic flowing through the firewall.

Logging at Session End is the recommended setting for deployment. If troubleshooting live traffic, the Session Viewer can be used as an alternative to Log at Session Start.

Logging

Enable logging on the Actions tab of the Security Policy Rule



Session Logs:

- When creating or editing a security rule, an option to log the transaction is available. There are two options to log the transaction, Log at Session Start or Log at Session End.
- Log at Session Start is disabled by default, generates traffic log entry for start of a session.
- Don't enable Log at Session Start except for troubleshooting purposes or for tunnel logs.
- Session start logs are generated on first data packet & not right after three-way handshake.
- Log at Session End is enabled by default, generates traffic log entry for the end of session.
- In Palo Alto Firewall for regular logging, the best practice is to log at Session End.

- The reason for that is that applications are likely to change throughout the session.
- Facebook for example will start as web-browsing and change to Facebook-base app.
- For example, from Facebook-base application to change to Facebook-chat application.
- Logging at Session Start would only show web-browsing which might lack important info.
- Logging at Session Start is used when troubleshooting applications that don't change.
- Logging at Session Start is used when applications that aren't recognized by firewall.
- It is not recommended to log both at Session Start & End as it puts extra load on CPU.

Log Setting:

The Action tab includes the logging settings and a combination of other options.

Log Setting	Description
Log at Session Start	Generates a traffic log entry for the start of a session.
Log at Session End	Generates a traffic log entry for the end of a session.
Log Forwarding Profile	To forward the local traffic log and threat log entries to remote destinations, such as syslog servers.
Schedule	To limit the days and times when the rule is in effect.
QoS Marking	Change the Quality of Service setting on packets matching the rule.
Disable Server Response Inspection	To disable packet inspection from the server to the client, select this option. This option may be useful under heavy server load.

Traffic Logs:

Displays an entry for the start and end of each session. Each entry includes:

- date and time
- source and destination zones
- Addresses
- ports
- application name
- security rule name applied to the flow
- rule action (allow, deny, or drop)
- ingress and egress interface
- number of bytes

Click the Magnifying Glass icon next to an entry to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (count value will be greater than one).

The Type column indicates whether the entry is for the start or end of the session, or whether the session was denied or dropped. A drop indicates that the security rule that blocked the traffic specified any application. A deny indicates that the rule identified a specific application.

If traffic is dropped before the application is identified, such as when a rule drops all traffic for a specific service, the application is shown as not-applicable.

The screenshot shows two windows from the Fortinet WebUI. The top window is titled 'Logs' and displays a table of session logs. The columns include: Recieve Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, and Bytes. There are several entries, with one row highlighted in grey. An arrow points from this highlighted row down to the second window. The second window is titled 'Detailed Session View' and shows a breakdown of a specific session. It includes sections for 'Session Details', 'Source IP', 'Destination IP', 'Protocol', 'Log Details', and 'Session Flow'. The 'Session Flow' section is expanded, showing a detailed timeline of events with various stages like 'Established', 'Data In', 'Data Out', and 'Terminated'.

Logs the start or end of each session as configured in the Security Policy

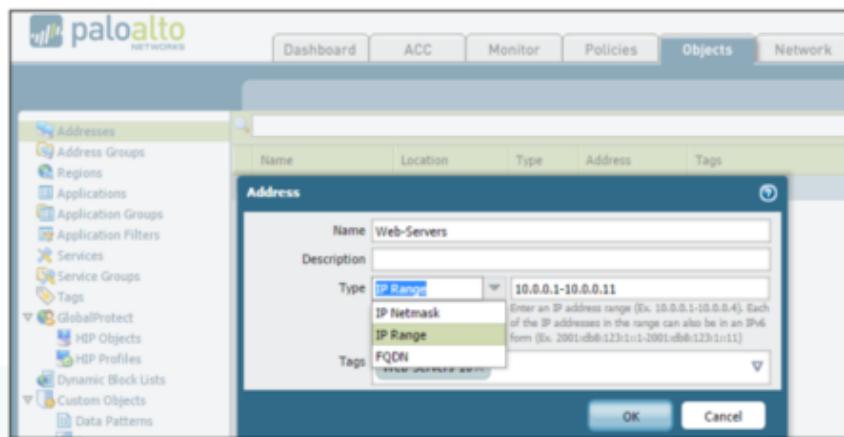
Address Objects:

Address objects are named objects that are configured on the firewall to make it easier for administrators to complete configurations with a predefined address. An address object can include an IPv4 or IPv6 address (single IP, range, subnet) or a FQDN. It allows you to reuse the same object as a source or destination address across all the policy rule bases without having to add it manually each time. In the WebUI, go to Objects > Addresses. Multiple address objects can be specified within a policy. Up to 2,500 address objects can be created.

Address Objects

- Created to reference frequently used IP addresses or ranges in configurations
- Available types:
 - IP Netmask
 - IP Range
 - FQDN
- Color-Coded Tags
 - Address Objects
 - Address Groups
 - Zones
 - Service Groups
 - Policy Rules

Objects > Addresses > Add



Name: Enter a name that describes the addresses to be defined (up to 63 characters). This name appears in the address list when security policies are defined. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

Three Types:

- IP Netmask example: 192.168.80.150/32 indicates one address, and 192.168.80.0/24 indicates all addresses from 192.168.80.0 through 192.168.80.255.
- IP Range example: 10.0.0.1-10.0.0.11
- FQDN example: webservers.company.com
 - The FQDN initially resolves at commit time. Entries are subsequently refreshed when the firewall performs a check every 30 minutes. All changes in the IP address for the entries are picked up at the refresh cycle.
 - The FQDN is resolved by the system DNS server or a DNS proxy object, if a proxy is configured.

Tags: Select the tag(s) that you want to apply to this address object.

You can tag objects to group-related items and add color to the tag to visually distinguish tagged objects. Tags can be added to these objects: address objects, address groups, zones, service groups, and policy rules. The firewall and Panorama support static tags and dynamic tags. Dynamic tags are registered from a variety of sources and are not displayed with the static tags because dynamic tags are not part of the device configuration.

Static Address Objects:

Dynamic address group membership is determined through the use of tags. Logical “and” and “or” operators are used to define filtering criteria.

Tags can be registered dynamically to the firewall through the XML API or VM Monitoring Agent on the firewall, or defined statically through PAN-OS.

Any entity that matches the defined tags becomes a member of a given dynamic address group.

Add tag(s) to existing static address objects

The screenshot shows the Palo Alto Networks PAN-OS web interface. The left sidebar navigation menu includes Address, Address Groups, Regions, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, GlobalProtect, RDP Objects, RDP Profiles, Dynamic Block Lists, Custom Objects, Data Patterns, Spans, Vulnerability, URL Category, Security Profiles, Anti-Virus, and Anti-Spam. The main content area has tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The 'Objects' tab is selected. A sub-menu under 'Address' shows 'Address Groups' and 'Address'. The 'Address' sub-menu is active, and a modal window titled 'Address' is open. In the modal, the 'Name' field is set to 'Database-Servers', the 'Description' field is empty, and the 'Type' dropdown is set to 'IP Range'. The 'Address' field contains '10.0.0.15-10.0.0.25'. Below the address input, there is a note: 'Enter an IP address range [1a..1B.B.B-B.B.B.B]. Each of the IP addresses in the range can also be in an SPA form: [1a..1B.B.B-B.B.B.B]/c1/c2/c3/c4'. The 'Tags' section contains several tags: Database-Servers (highlighted in red), Production, File-Servers, SANs Servers, and Web-Servers-10. The 'Address' table in the background lists two entries: 'Database-Servers' with an IP range of 10.0.0.15-10.0.0.25 and 'Web-Servers' with an IP range of 10.0.0.2-10.0.0.8.

Dynamic Address Groups: Use Case

Dynamic address groups are a way to dynamically populate address groups with IP addresses through the XML API for use in security policies and other types of policies.

Administrators are able to specify IP addresses inside policies dynamically via tags and tag-based filters. They are part of the Palo Alto Networks virtualization solution and are intended for use with VMware ESXi integration. The VM environment is monitored via the vSphere API.

The rate of change in a virtual environment does not match traditional security policy change cycles. A zone-based architecture may be sufficient to keep a consistent policy. However, dynamic address groups that track IP addresses allow policy to follow VM changes in cases where zones are insufficient.

Changes are published to PAN-OS via the RESTful XML API, and policies are adjusted accordingly.

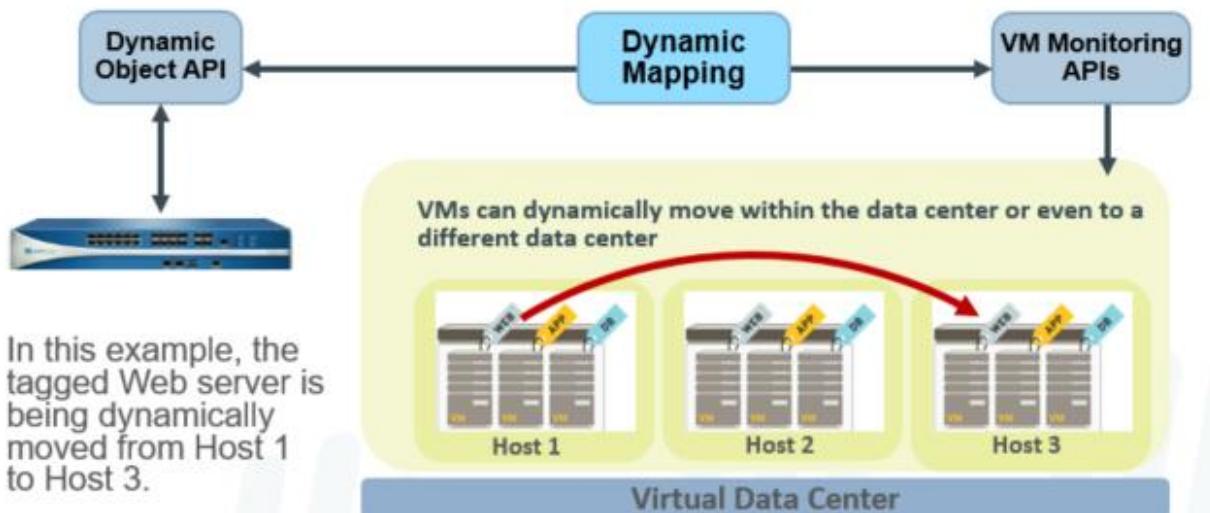
At least 60 seconds passes between an API call and an IP address being registered by the firewall.

Address object refresh (that is AddrObjRefresh) jobs run every 60 seconds on the firewall. This job waits until the following minute has passed if an address object refresh job has just occurred and PAN-OS receives a new XML API update.

These changes do not require a manual commit job and they are persistent when the firewall is rebooted. In this slide, three server types are grouped and tagged accordingly:

- Web server: light gray tag
- App server: yellow tag
- Database server: turquoise tag

This dynamic address grouping and tagging enable the servers to dynamically move from one host to another as necessary without further administration on your part and without requiring a commit operation.



Dynamic Address Groups:

1. Navigate to **Objects > Address Groups > Add**.
2. Set the Type to **Dynamic**.
3. Add Match Criteria from the list of available tags.

They can be combined with the logical operators “and” and “or” to create different combinations of tag-match criteria that must be met for an entity to be associated with the dynamic address group.

A dynamic address group populates its members dynamically using look-ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, if you have a sophisticated failover setup, or provision new virtual machines frequently, and

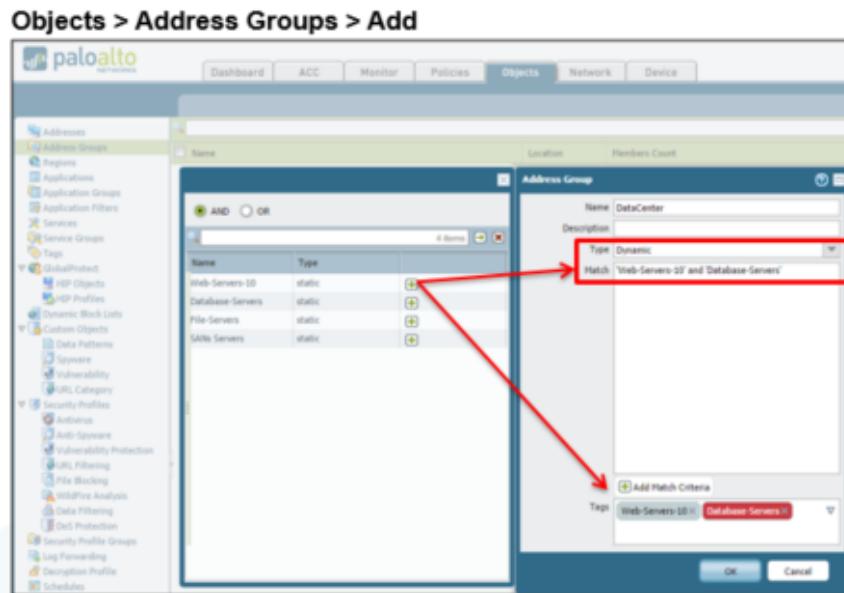
want to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall, you can do so using dynamic address groups.

Unlike a static address group where you specify the network address of a host, the members of a dynamic address group are populated using a match criteria that you define. The match criteria uses logical "and" and "or" operators; each host that you want to add to the dynamic address group must bear the tag or attribute that is defined in the match criteria. Tags can be defined directly on the firewall or on Panorama or they can be dynamically defined using the XML API and registered with the firewall. When an IP address and the corresponding tag (one or more) is registered, each dynamic group evaluates the tags and updates the list of members in its group.

To register new IP address and tags or changes to current IP addresses and tags, you must use scripts that call the XML API on the firewall.

Configured within Address Group instead of Addresses

- Select Dynamic for Type, then add Match Criteria



Apply to Policy:

Add the dynamic address group as match criteria in a policy.

A commit job must be performed to push the candidate configuration into memory as the running configuration.

Dynamic address group members can be changed dynamically at this point.

Entities can be associated with IP addresses, and IP addresses can be associated with tags through the XML API or the VM Monitoring Agent.

It is not necessary to perform successive commit jobs for such changes because they become part of the running configuration.

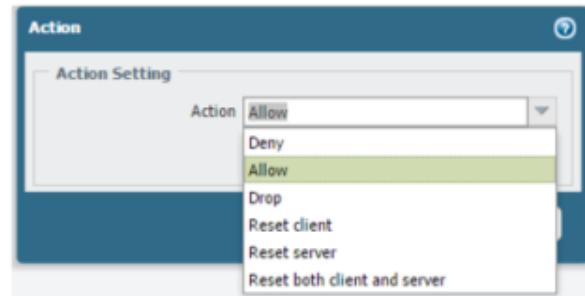
An administrator can view the IP addresses that have been registered dynamically to the address group by clicking the name of the group, moving the cursor over Inspect, and then clicking the More link.

- Apply group in policy same as any other address group and commit
 - Can drill down and click more to see registered IPs

Name	Type	Type	Zone	Address	Value	HTTP Profile	Zone	Address	Application	Service	Action
Office Programs	none	universal	Trust-L3	any	any	Trust-L3	any	any	Office Programs	application-default	Allow
Universal FTP Policy	none	universal	Universal-L3	any	any	Trust-L3	any	172.23.24.2	ftp	application-default	Allow
General Internet	none	universal	Trust-L3	any	any	Universal-L3	any	any	dns	application-default	Allow
DataCenter	none	universal	any	any	any	any	any	any	File	application-default	Allow
									Http	application-default	Allow
									Https	application-default	Allow
									Pop3	application-default	Allow
									Smtp	application-default	Allow
									Telnet	application-default	Allow
									Wan	application-default	Allow
									Web	application-default	Allow
									Web-Form	application-default	Allow
									Web-Service	application-default	Allow
									Web-Server	application-default	Deny

Allow and Deny Action Settings:

- **Allow:** Default action
- **Deny:** Drops packet or reset TCP depending on the application
- **Drop:** Silently drop



The action settings within the security policy rule enable you to specify how the firewall will handle the attempt.

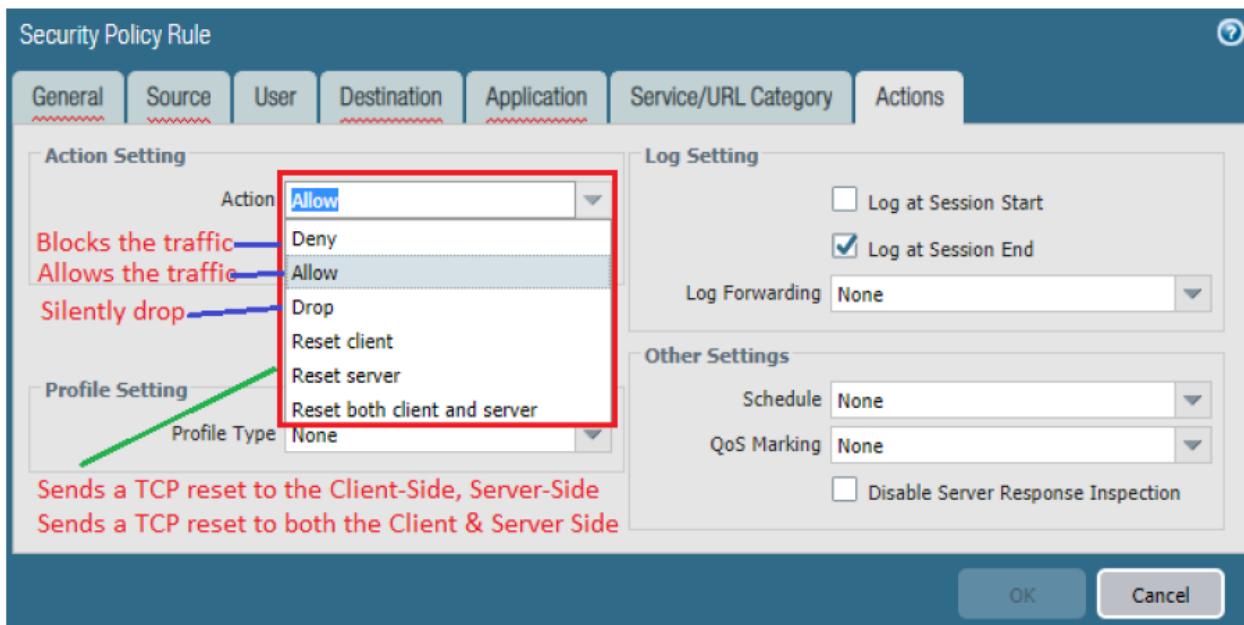
The Palo Alto Networks firewall is based on application intelligence, so the TCP session must be allowed to complete before the application is discovered. If the firewall then silently drops packets, it can break applications and cause them to behave improperly. The applications may hang, continue to send packets blindly, or hold open resources unnecessarily. To gracefully deny the traffic, a TCP reset is needed to clean up the session.

More than half of the applications recognized by the firewall automatically receive a TCP reset. But the administrator can specify which applications will receive a reset, and which applications will cause packet drops, by manually configuring the action in the policy rule.

Action:

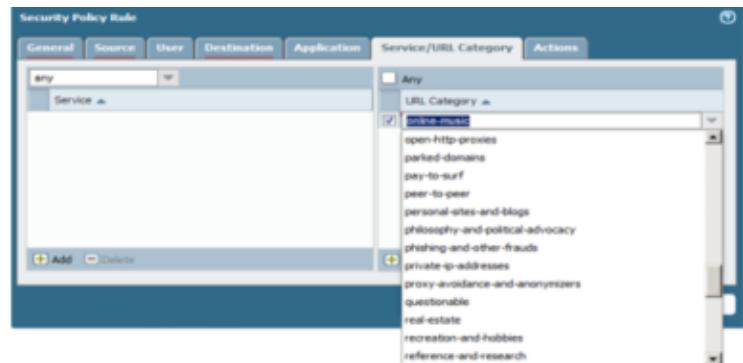
To specify the action for traffic that matches the attributes defined in a rule.

Action	Description
Allow	Allows the traffic.
Deny	Blocks the traffic.
Drop	Silently drops the application.
Reset Client	Sends a TCP reset to the Client-Side device. If session is UDP or ICMP based, an ICMP Unreachable will be sent.
Reset Server	Sends a TCP reset to the Server-Side device. If session is UDP or ICMP based, an ICMP Unreachable will be sent.
Reset Both	Sends a TCP reset to both the Client-Side and Server-Side devices. If session is UDP or ICMP based, an ICMP Unreachable will be sent.



URL Categories in Security Policy rules:

- For HTTP/HTTPS traffic only
- Can include custom URL categories
- Requires a license for noncustom URL categories
- URL lookups are cached for faster retrieval



The URL Category match criteria is used in three different policy types: security, QoS, and captive portal. This field matches URLs against predefined categories provided by the dynamic updates.

In addition to the categories provided by Palo Alto Networks, custom URL categories can be created. This feature requires the URL Filtering license, except for custom categories. If the license expires, only custom categories are used by the policy.

- Policy lookups occur each time the URL category for the session changes.
- Traffic logs show entries for each URL category transition.
- Lookups are cached for faster retrieval.
- The engine checks the data plane cache then checks the management plane cache before querying the external URL lookup servers.
- If the category is not resolved before the web server responds, the security policy looks for a match in a not-resolved category.

URL category matching uses the same block page as the URL filtering profile and does not have either the Continue or Override option.

If more granular URL filtering is required, a URL filtering profile should be used instead. The URL Filtering profile can match specific URLs (for example, www.facebook.com), while the URL category only matches broad categories (for example, social-networking).

URL filtering profiles are discussed in more detail in the Content-ID module.

Managing Policy Rows:

- Options include: Add, Delete, Clone, Override, Revert, Enable, Disable, Move, and High-light Unused Rules
- A policy may be added as new or cloned from an existing policy
- Policies can be reordered to match requirements
- Disabling a rule allows you to retain the entry but disables the rule

Policy Rules										
Name	Source			Destination			Action	Profile		
	Zone	Address	User	Zone	Address	Application				
Allow WebBrowsing	prg Trust-L3	any	any	prg Untrust-L3	any	web-browsing	application-default	none		
NoWebForServer	prg Trust-L3	192.168.15.199	any	prg Untrust-L3	any	web-browsing	application-default	none		

Policy Rules										
Name	Source			Destination			Action	Profile		
	Zone	Address	User	Zone	Address	Application				
NoWebForServer	prg Trust-L3	192.168.15.199	any	prg Untrust-L3	any	web-browsing	application-default	none		
Allow WebBrowsing	prg Trust-L3	any	any	prg Untrust-L3	any	web-browsing	application-default	none		

Task	Description
Add	To add a new policy rule, Click Add at the bottom of the page. Or select rule on which to base the new rule and click Clone Rule.
Modify	To modify a rule, click the rule.
Move	Select rule & click Move Up, Move Down, Move Top, or Move Bottom.
Delete	Select a rule and Delete the existing rule.
Enable/Disable	To disable a rule, select the rule and Disable it; to enable a rule that is disabled, select the rule and Enable it.
Monitor Rule Usage	To identify rules that have not been used since the last time the firewall was restarted, Highlight Unused Rules. Rules not currently in use are displayed with a dotted yellow background.
Reset rule Hit count	The Hit Count is used to track the total traffic hits for the policy rule. To reset the hit count for a specific rule, expand the drop-down and Reset the counter. Alternatively, Reset Rule Hit Counter using the bottom menu. To clear the hit count statistics, you can select All Rules, or can select specific rules and reset hit count statistics only for the Selected rules.
Show/Hide columns	To show or hide the columns that display in the Policies pages, select this option next to the column name to toggle the display of each column.
Apply filters	To apply a filter to the list, select from the Filter Rules drop-down. To add a value to define a filter, click drop-down for the item & choose Filter.
Export Configuration Table	Administrative can export the policy rulebase as PDF/CSV. You can apply filters to create more specific table configuration outputs for things such as audits. Only visible columns in the web interface will be exported.
Override and Revert	Override and Revert actions pertain only to the default rules that are displayed at the bottom of the Security rulebase. Override them in order to edit select policy settings also Revert the default rules, which restores the predefined settings

Individual policies can be managed using the toolbar at the bottom of the Policy pages. Locally-defined policies can be created, deleted, cloned, enabled, and disabled. Policies pushed to the firewall by Panorama must be edited from the Panorama server.

Controls also exist to reorder the policies. Incorrect order can prevent policies from behaving as designed. In the example, an administrator wanted to allow web browsing for all systems except the server at IP address 192.168.15.199. However, with the Deny rule appearing after the more general Allow rule, the server would still be able to browse the web. Selecting the AllowWebBrowsing policy and clicking Move Down arranges the rules so that they are evaluated in the correct order to deny the server. Policies can also reordered by dragging the entry with the mouse to a new position.

Application in Security Policy rules:

In this tab we will call application, application groups, application filters on our security rules.

Security Policy Rule

Options	Description
Application-Default	To allow traffic on the default destination ports. Application-default ports are the default destination ports used by various application.
Any	Simply means all Ports: 1-65535, TCP or UDP. On any port & protocols
Select	Have to specify exactly what TCP or UDP port

Users in Security Policy rules:

In this tab we will add users, groups if we want to write user based rules.

Security Policy Rule

any Any traffic regardless of user
pre-logon Remote users that are connected to the network
known-user All authenticated users, domain users' group on a domain.
unknown All unauthenticated users or Guest users.
select

Includes selected users as determined by the selection in this window

Options	Description
Any	Any, Includes any traffic regardless of user data.
Pre-Logon	Remote users that are connected to the network using Global Protect.
Known-User	All authenticated users means domain users' group on a domain.
Unknown	Includes all unauthenticated users or Guest users.
Select	Includes selected users as determined by the selection in this window.

HIP:

HIP stand for Host Information Profiles. A HIP enables you to collect information about the security status of your end hosts, such as whether they have the latest security patches and

For HIP checks we need license.

We need to configure HIP object and HIP profile.

Override and Revert Default Rules:

The screenshot illustrates the steps to override and revert default security rules in a network configuration tool.

Top Panel (Security Policy Rule - predefined):

- Row 1: 2 intrazone-default (green icon), intrazone, any, 1, any, (intrazone), any, any, Allow (green checkmark).
- Row 2: 3 interzone-default (green icon), interzone, any, any, any, any, any, Deny (red slash).

A red box highlights Row 1, and a red arrow points from it to the text: "Select the default rules then click on Override to modify the default rules."

Modifying Row 1:

- Action Setting:** Action: Allow (dropdown), Send ICMP Unreachable (checkbox).
- Profile Setting:** Profile Type: None (dropdown).
- Log Setting:** Log at Session Start (checkbox), Log at Session End (checkbox), Log Forwarding: None (dropdown).
- Buttons:** OK (highlighted with a red box) and Cancel.

A red box highlights the "Override" button in the toolbar below the dialog, and a red arrow points from it to the text: "Select the default rules then click on Override to modify the default rules."

Bottom Panel (Security Rule):

- Row 1: 1 Policy-1 (blue icon), universal, any, any, any, any, any, application-default, Allow (green checkmark).
- Row 2: 2 intrazone-default (green icon), intrazone, any, 1, any, (intrazone), any, any, Allow (green checkmark).
- Row 3: 3 interzone-default (green icon), interzone, any, any, any, any, any, Deny (red slash).

A red box highlights Row 2, and a red arrow points from it to the text: "First select Default Rule which already Overriden Click on Revert, to Revert the default rules, which restores the predefined settings."

Toolbar Buttons:

- Add, Delete, Clone, **Override** (highlighted with a red box), Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, Reset Rule Hit Counter.

Revert Confirmation Dialog:

Do you really want to revert 1 "Security Rule" entry?

Yes (highlighted with a red box) and No buttons.

A red box highlights the "Revert" button in the toolbar below the confirmation dialog, and a red arrow points from it to the text: "First select Default Rule which already Overriden Click on Revert, to Revert the default rules, which restores the predefined settings."

NAT (Network Address Translation)

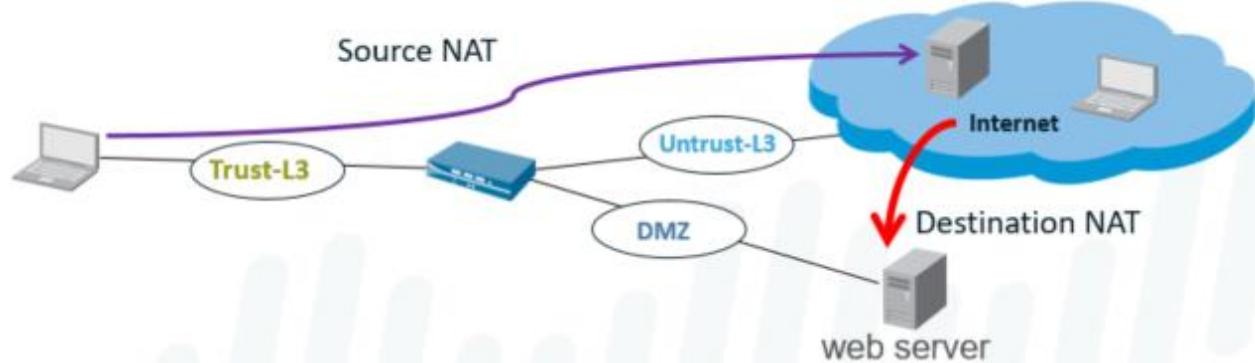
- > NAT stands for Network Address Translation.
- > NAT is often used to translate private IP addresses to public IP addresses.
- > NAT is a process that involves translating Private IP addresses into Public IP addresses.
- > The process of translating one IP address to another is known as NAT.
- > Router and Firewall is a device, which is used for network Address Translation.

- > NAT can provide Internet connectivity to many LAN users over single public IP address.
- > Network Address Translation (NAT) technique helps a lot to save IPv4 address space.
- > There are many forms of Network Address Translation (NAT) & Port Address Translation.
- > Network Address Translation used to reduce the requirement of the Public IP address.
- > Network Address Translation increase security of Internal Computer Networks.
- > NAT Translate Private IP into Public IP address & Public IP address into Private IP address.
- > NAT used to connect a device with Private IP address to the Wide Area Network Internet.
- > Network Address Translation hide an organization internal network from external network.
- > Network Address Translation modifies only the Layer 3 header of OSI reference model.
- > PAT, translation of an IP address and Port to another Internet Protocol address and Port.
- > Port Address Translation (PAT) modifies both the Layer 3 and Layer 4 header of OSI model.
- > Palo Alto Firewalls supports both source & destination address and/or port translation.

Use Network Address Translation policies to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports.

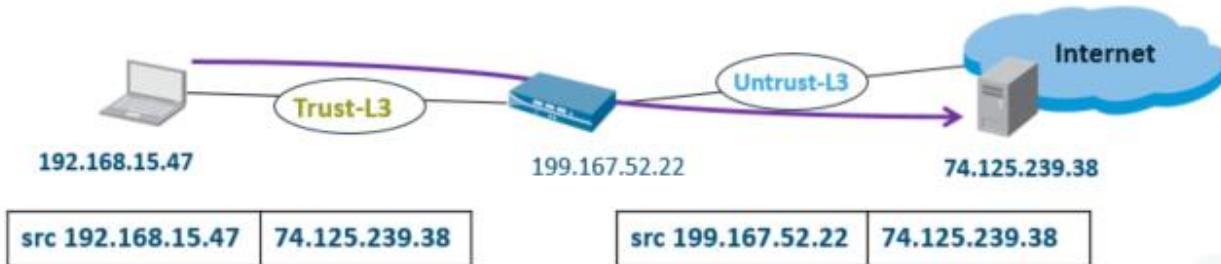
When configuring NAT on the firewall, a security policy must also be configured to allow the NAT traffic. The security policy is matched based on the post-NAT zone and the pre-NAT IP address.

- **Source NAT:** is commonly used for internal users to access the Internet
- **Destination NAT:** is used to provide external access to public servers on the private network



Source NAT and Source NAT Types:

Source NAT changes the source address in Internet Protocol header of a packet. Source NAT may also change the source port in the TCP/UDP headers. It is used when an internal host needs to initiate a connection to an external host. Device performing NAT changes private IP address of source host to public IP address.



Source NAT Types:

- Static IP
 - 1-to-1 fixed translations
 - Change the source IP address while leaving the source port unchanged
- Dynamic IP
 - 1-to-1 translations of a source IP address only (no port number)
 - Private source address translates to the next available address in the range
- Dynamic IP/Port (DIPP)
 - Multiple clients use the same public IP addresses with different source port numbers
 - Assigned address can be set to Interface address or Translated address

The firewall supports these types of source address translation:

- Dynamic IP/Port: Multiple clients can use the same public IP address with different source port numbers. Dynamic IP/Port NAT rules allow translation to a single IP address, a range of IP addresses, a subnet, or a combination of these. In cases where an egress interface has a dynamically assigned IP address, it can be helpful to specify the interface itself as the translated address. By specifying the interface in the dynamic IP/port rule, NAT policy updates automatically to use any address acquired by the interface for subsequent translations.
- Dynamic IP: Private source addresses translate to the next available address in the specified address range. Dynamic IP NAT policies allow you to specify a single IP address, a range of IP addresses, a subnet, or a combination of these as the translation address pool. By default, if the source address pool is larger than the translated address pool,

new IP addresses seeking translation are blocked while the translated address pool is fully utilized. This behavior can be changed by clicking the Advanced (Dynamic IP/Port Fallback) button that specifies Dynamic IP/Port configurations to be used if the pool is exhausted.

- Static IP: Use static IP to change the source IP address while leaving the source port unchanged. A typical use case for this NAT type is an internal server that must be available to the Internet.

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/1

IP Address: 192.168.100.100/24

Destination Address Translation

Translated Address:

Translated Port: [1 - 65535]

WAN Interface:

WAN IP Address:

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type: Dynamic IP

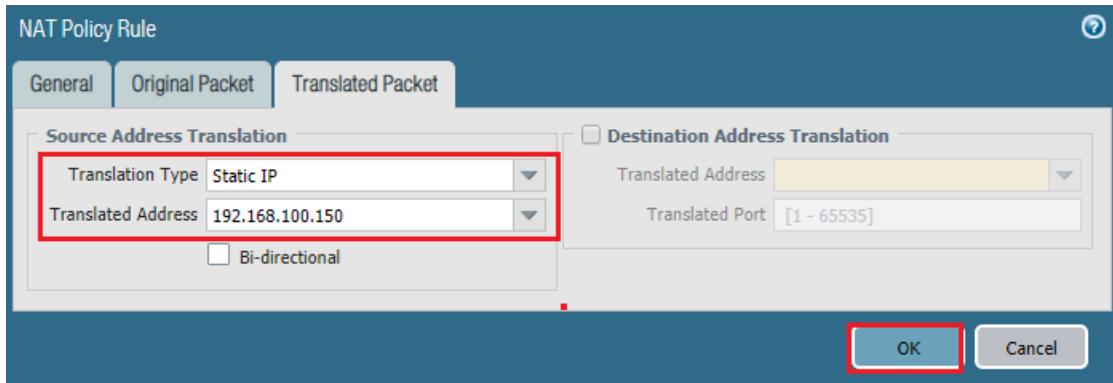
Translated Address:

- 192.168.100.150
- 192.168.100.151

Add Delete

Advanced (Dynamic IP/Port Fallback)

OK Cancel



Destination Network Address Translation (DNAT):

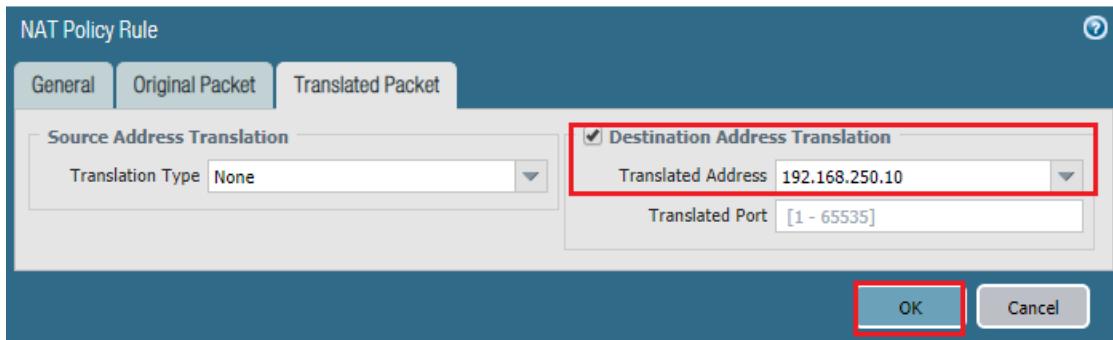
Destination NAT changes the destination address in IP header of a packet. Destination NAT may also change the destination port in the TCP/UDP headers. Redirect incoming packets with destination of public address to private IP address. Destination Network Address Translation (DNAT) is performed on incoming packets. Where the PA firewall translates a public destination address to a private address. DNAT is a 1-to-1, static translation with option to perform port forwarding or translation. Users over Internet Accessing a Web Server hosted in a Data Center is a typical example. Destination NAT also offers the option to perform port forwarding or port translation.

Static IP:

Use static IP to change destination IP address while leaving destination port unchanged.

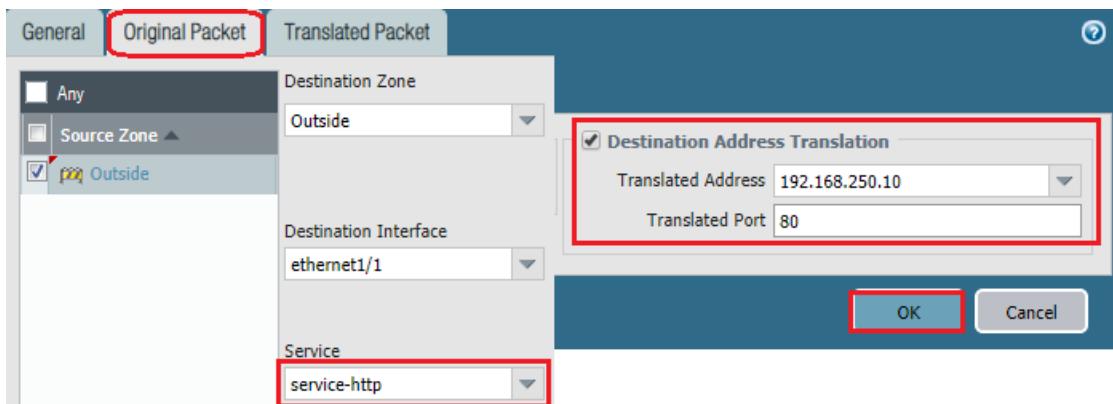
Statically translates original destination address to same translated destination address.

Original packet have single destination IP address, range of IP addresses, or list.



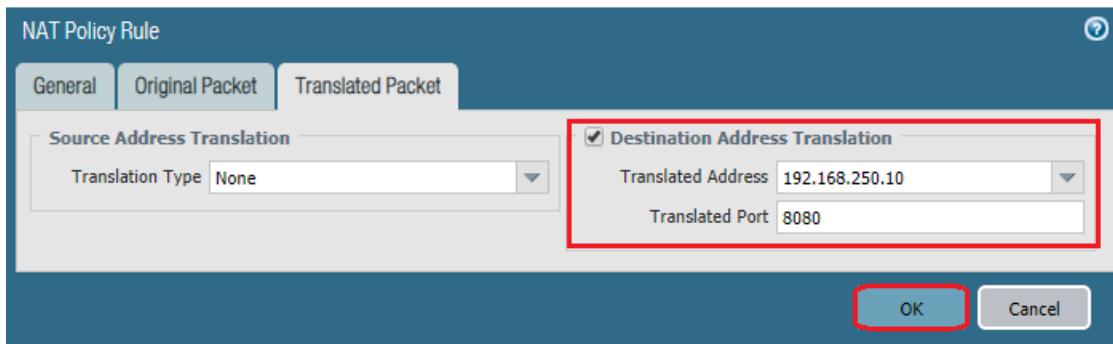
Port Forwarding:

Can translate public destination address and port number to private destination address. Technique used to manage traffic through NAT policies based on destination port numbers. It is used to map a single public IP address to multiple private servers and services. The destination ports can stay the same or be directed to different destination ports.



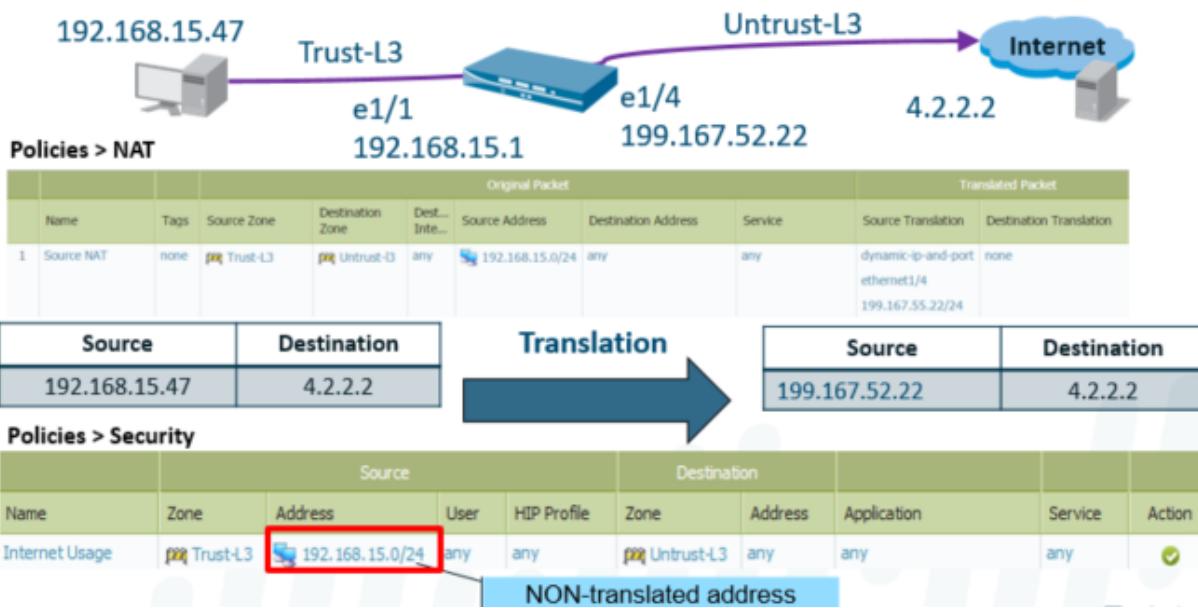
Port Translation:

Translate public destination address & port no to private destination address different port. Port Translation keeping the real port number private and change the destination port. It is configured by entering Translated Port on Translated Packet tab in NAT policy rule. Example is suppose the web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the public Internet Protocol (IP) and TCP Port 80. The destination NAT rule is configured to translate both IP address and TCP port to 8080.



NAT Example:

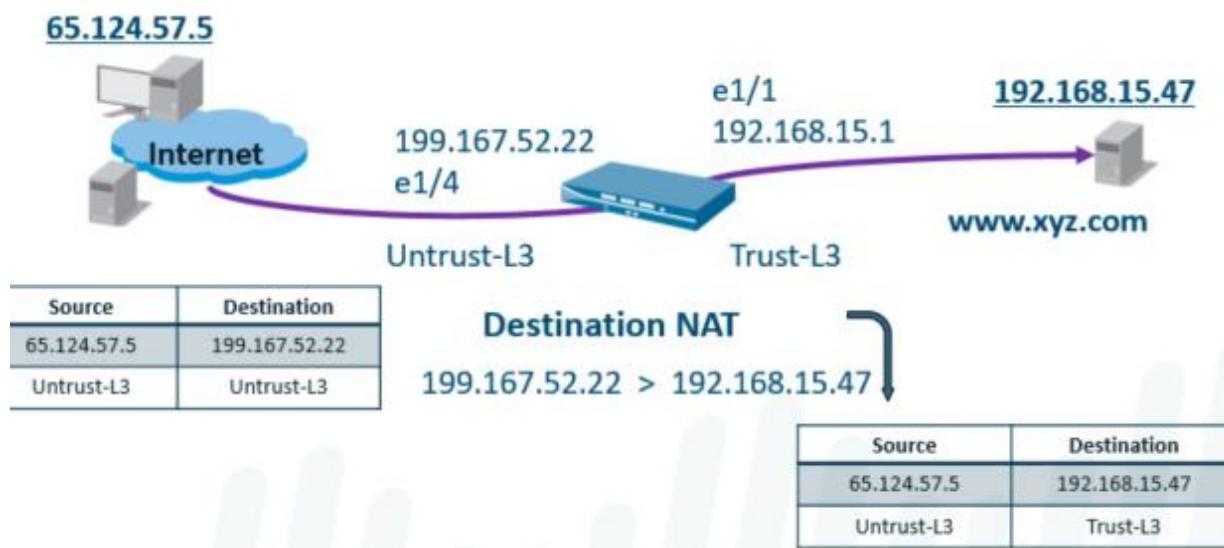
Example 01: In this example, a host with the IP address 192.168.15.47 exists on a private network. The user at this address wants to connect to a server on the Internet. To prevent the exposure of the private IP address, the firewall administrator has configured a NAT policy so that all traffic from the private network appears to come from the address on the ethernet1/4 interface.



Example 02: In this scenario, a user at an external system with the IP address 65.124.57.5, queries the DNS server for the IP address of the web server www.xyz.com.

The DNS server returns an address of 172.16.15.1, the external address of the firewall interface in the Untrust-L3 zone. To reach the web server, the destination IP address must be set to the private IP 192.168.15.47.

Remember: A security policy must cross zones. Also, the security policy is enforced after the NAT policy is evaluated.

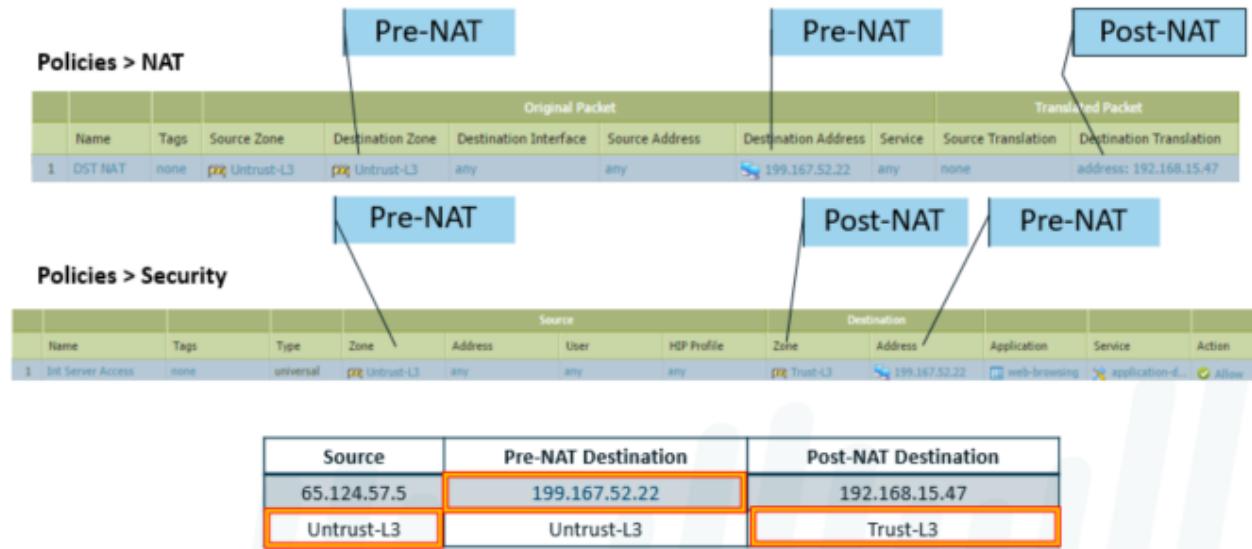


Destination NAT Example Policies:

NAT rules must be configured to use the zones associated with pre-NAT IP addresses configured in the policy. For example, when translating traffic that is incoming to an internal server (which is reached via a public IP by Internet users), you must configure the NAT policy using the zone in which the public IP address resides. In this case, the source and destination zones would be the same.

As another example, when translating outgoing host traffic to a public IP address, you must configure the NAT policy with a source zone that corresponds to the private IP addresses of those hosts. The pre-NAT zone is required because this match occurs before the packet has been modified by NAT.

Security policy differs from the NAT policy in that post-NAT zones must be used to control traffic. NAT may influence the source or destination IP addresses and can potentially modify the outgoing interface and zone. When creating security policies with specific IP addresses, note that pre-NAT IP addresses are used in the policy match. Traffic subject to NAT must be explicitly permitted by the security policy when that traffic traverses multiple zones.



Network Address Translation:

NAT policy is evaluated after the destination zone route lookup

NAT policy is applied just before packet is forwarded.

NAT types are Source and Destination, and these are from the perspective of the firewall.

Source NAT configuration: Source NAT is generally used from traffic on private internal IP's to a publicly routable IP (user inside to server outside). Types of Source NAT's include:

Static IP: fixed 1-to-1 translation; used when a NAT IP needs to remain the same IP and Port. This can be done with an IP address range, but the translation will always be static 1:1; in a 10-IP range, a x.y.z.2 source will always translate to z.y.x.2 destination.

Dynamic IP: 1-to-1 ip address translation only (no port number); can be used with a single or pool of IP's. Generally used for a set number of internal hosts with a matching number of external IP's, but static isn't required.

Dynamic IP and port (DIPP): This is used for multiple IP's to one or a few IP's, by allowing the connection to use another port than the default service. This is generally used for internet access outbound from home and business connections.

To use Source NAT:

Create a NAT policy rule: Original packets (IP's of client(s)) that will be using the NAT (source address), destination address (if needed), and the type of source translation (Static, Dyn, DynDIPP), and the IP to translate to. A security policy will be needed to allow the traffic. The **security policy will include:**

Source Address (private/internal client IP's/subnet)

Source Zone where client IP's reside

Destination Zone (where IP to NAT to exists)

Any application or services

Allow the traffic on the policy

Bidirectional NAT's can be configured (only available for static NAT).

To configure, check the 'bidirectional' checkbox in the NAT configuration source nat translated packet tab.

DIPP NAT oversubscription is when a DIPP Source NAT uses more than the available 64,000 ports available per ip address. This is done by using the destination IP of new sessions outbound to 'ride' the same active port as other traffic going to that IP address.

Destination NAT configuration:

Destination NAT is used for external traffic coming into a private or secured location inside your network.

Types of Destination Nat:

Static IP: 1:1 translation of inbound traffic.

Optional Port Forwarding: Can route to multiple internal servers based on Port number (25 to mail, 80 to web, etc)

Configuration:

Create a Destination NAT policy, defining the source and destination (pre-nat on both)

Incoming: (any or specific) to Destination (external routable IP) – Untrust to Untrust typically for example, with a destination translation to the internal IP address

Create a security policy that permits the post NAT zone (and IP's if needed) to the Pre-Nat destination IP/app/service/action

Security Policy does pre-nat source/dest, post-nat destination zone.

Destination Nat Port Forwarding Configuration:

When configuring the Destination NAT address under the 'Translated Packet' tab, put in the translated port of the destination

A destination NAT can be set with different destination translation IP's and ports from the same external facing IP, as long as the service is specified.

----- **END** -----

Day 07 and 08

High Availability

- 1. Network Failure (Power Failure, ISP Failure, Device Failure)**
- 2. Prerequisites for HA (HW, SW, License)**
- 3. HA Types (Active/Passive, Active/Active)**
- 4. HA Interfaces (HA1 & HA1-B (Control Link), HA2 (Data Link) & HA2-B)**
 - > Control Link Ports :: tcp-28 || tcp-28769,28260
 - > Data Link Ports :: IP Protocol number 99 or UDP-29281
 - > Ethertype 0x7261
- 5. Link Monitoring**
- 6. Path Monitoring**
- 7. Failover Triggers**
- 8. HA States**

9. Split Brain

10. (Virtual Wire, Layer 2, or Layer 3) Support Active/Passive HA

Active/Active HA

HA3 Interface

Session Owner (L7 Processing i.e. app-id, content-id, threat scanning, Logs)

-> First Packet, Active-Primary

Session Setup (Layer2 through Layer4 NAT, Route, Zone Protection, QoS, VPN)

-> First Packet, Active-Primary

Packet Flow in a Cluster

1. New Session

2. Packet Matching the existing session

3. Asymmetric Flow

Active/Active Deployment

-> **(Virtual Wire, Layer 3) Support Active/Active HA**

1. V-Wire Deployment

2. Floating IP

->**Floating IP addresses and virtual MAC addresses move between devices on failover**

->**Supports VPN and NAT implementations**

->**Can use external load balancers to spread traffic across devices**

3. Arp Load sharing

->**A single IP address is shared between devices**

->**Unique MAC address for each interface supporting the shared IP address**

->**Devices respond to client ARP requests based on source IP address**

->**Requires a Layer 2 connection device**

->**show high-availability ?**

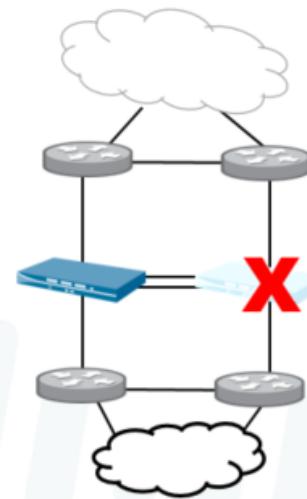
->**less mp-log ha_agent.log**

->show log system

->show counter global filter aspect aa delta yes

High Availability:

- A High Availability (HA) cluster is a pair (2) of firewalls that are grouped together to prevent a single point of failure on the network
- Prerequisites:
 - Same model
 - Same PAN-OS version
 - Same types of interfaces
 - Same set of licenses



To perform access control functions properly, a network firewall must be placed at the single point through which all traffic must pass. Because all traffic must pass through the firewall, it is vital that the traffic-flow remains uninterrupted, even in the event of a device or network failure. A well-designed security infrastructure needs to offer high availability tools to create a resilient, scalable, and easy to manage solution.

A PAN-OS HA pair consists of two identical Palo Alto Networks Next-Generation Firewalls with identical software that enforce the same overall security policy and share the same configuration settings. A heartbeat connection between the two devices ensures seamless failover in the event that a device goes down.

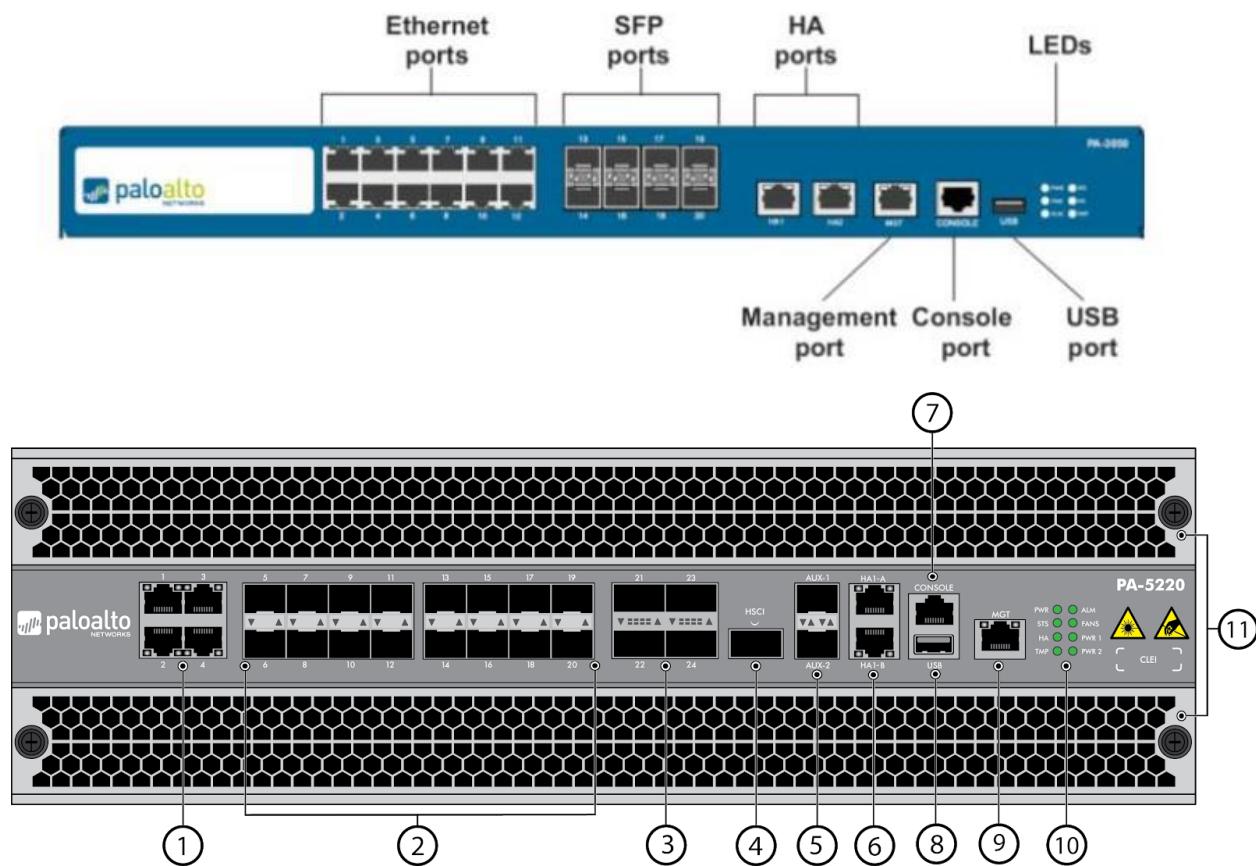
Ensuring seamless failover with either type of high availability requires careful planning of the network design. Refer to the document “Designing Networks with Palo Alto Networks Firewalls” on Knowledge Point for additional information.

High Availability is used to synchronize the following: active and candidate configurations (including objects and policies), routing information, and session states (even for sessions traversing VPN tunnels).

The High availability (HA) is a deployment in which two firewalls are placed in a group. Their configuration is synchronized to prevent a single point of failure on your network. Heartbeat connection between firewall peers ensures failover in event peer goes down. Setting up two firewalls in an HA pair provides redundancy & ensure business continuity. Firewalls in an HA

pair use HA links to synchronize data and maintain state information. Some models of Firewall have dedicated HA ports—Control link (HA1) & Data link (HA2). While others Palo Alto Network Firewall require you to use the in-band ports as HA links. Firewalls with dedicated HA ports such as PA-800, PA-3200, PA-5200 & PA-7000 Series. Use dedicated HA ports to manage communication & synchronization between firewalls. For firewalls without dedicated HA ports such as the PA-200 Series. Best practice use the management port for the HA1 link to allow for a direct connection. And use Palo Alto Network Firewall an in-band port or links for the Data Link (HA2) link.

High availability will not synchronize: most management settings (management IP and admin accounts for example), HA settings (one needs to be primary, one needs to be secondary, and this is often determined by HA settings), and logs.



HA Types:

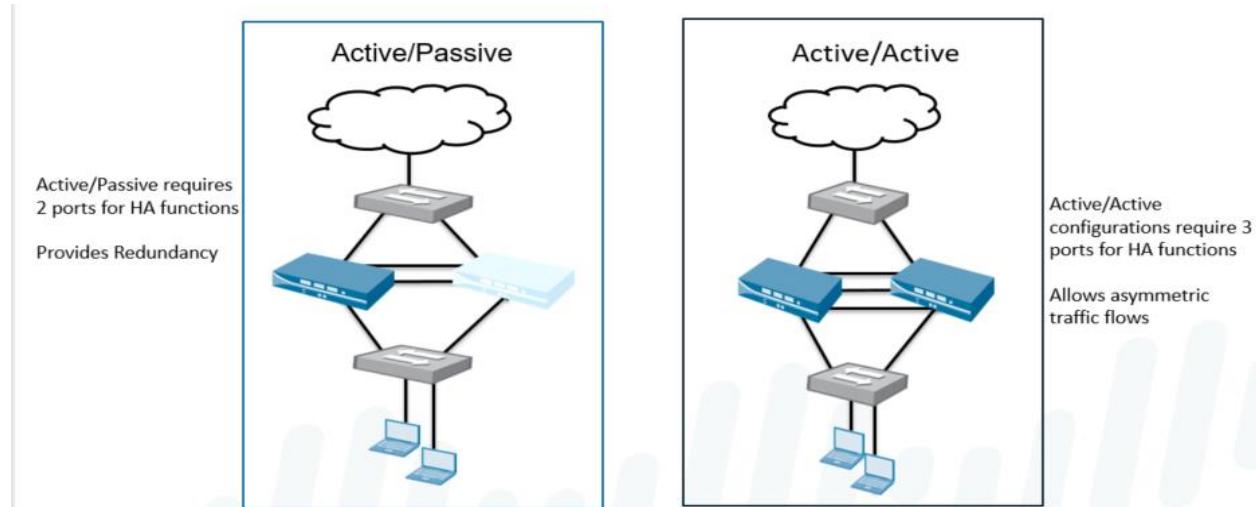
Service providers and enterprises that deliver revenue-generating and business-critical services over the Internet face a myriad of performance and security challenges. However critical those challenges may be, high availability (HA) remains the paramount concern. On Palo Alto Networks firewalls, you can set up two devices as an HA pair. HA allows you to minimize downtime by making sure that an alternate device is available if the primary device fails.

Palo Alto Networks firewalls support stateful active/passive or active/active high availability with session and configuration synchronization. They use dedicated or in-band HA ports to synchronize data—network, object, and policy configurations—and to maintain state information. Setting up the firewalls in a two-device pair provides redundancy and allows you to ensure business continuity.

To perform access control functions properly, a network firewall must be placed at the single point through which all traffic must pass. Because all traffic must pass through the firewall, it is vital that the traffic-flow remains uninterrupted, even in the event of a device or network failure. A well-designed security infrastructure needs to offer high availability tools to create a resilient, scalable, and easy to manage solution.

A PAN-OS HA pair consists of two identical Palo Alto Networks Next-Generation Firewalls with identical software that enforce the same overall security policy and share the same configuration settings. A heartbeat connection between the two devices ensures seamless failover in the event that the a device goes down.

Ensuring seamless failover with either type of high availability requires careful planning of the network design. Refer to the document “Designing Networks with Palo Alto Networks Firewalls” on KnowledgePoint for additional information.



HA Pre-Requisite: To set up High Availability HA on firewalls, need a pair of firewalls that meet fallowing.

-> **The same model**—The PA firewalls in the pair must be of the same hardware model. To setup HA in Active-Active & Active-Passive mode the same type of interfaces require.

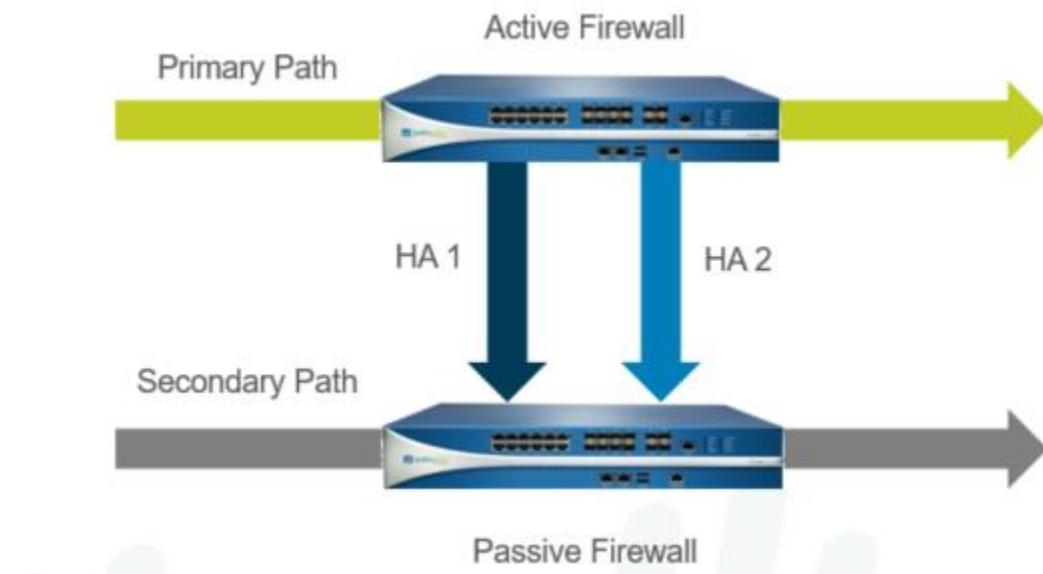
-> **The same PAN-OS version**—The firewalls must be running the same PAN-OS version. And must each be up-to-date on the application, URL, and threat databases the same.

-> **Dedicated HA links**, or combination of the management port and in-band ports type HA. HA interfaces must be configured with static IP addresses only not IP addresses from DHCP.

-> **Licenses** are unique to each firewall & cannot be shared between firewalls same set require.

Active-Passive:

In Active-Passive one firewall actively manages traffic while other is synchronized. In Active-Passive passive is ready to transition to active state, should a failure occur. One actively manages traffic until a path, link, system, or network failure occurs. When active firewall fails, passive firewall transitions to active state and takes over. Active-passive HA is supported in the virtual wire, Layer 2, and Layer 3 deployments. Active-Passive does not increase session capacity or network throughput in firewall. Active-Passive has simple design concept, so it is easier to troubleshooting routing.



There are several deployment options for HA depending upon whether the firewall is deployed as the firewall or behind the firewall in an augmentation role. The mode of implementation (Virtual Wire, Layer 2, or Layer 3) can also influence the options.

An important fact to consider in designing an HA architecture is that the traffic-handling links on the passive device are maintained in a down state. Upstream and downstream devices that are connected to the passive firewall will not see a valid path unless the passive firewall becomes active.

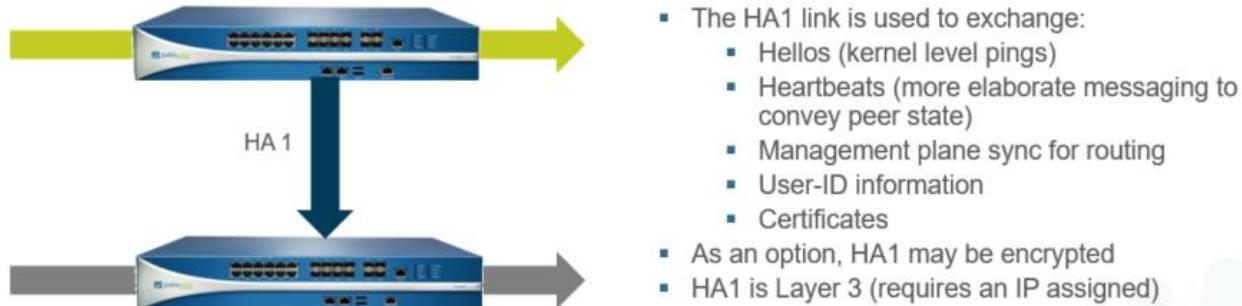
These rules apply to active/passive HA operation and failover:

- The active firewall continuously synchronizes its configuration and session information with the passive firewall over the HA interfaces.

- If the active firewall fails, the passive firewall detects the loss of heartbeats and automatically becomes active.
- If the state synchronization connection is lost, then no state synchronization occurs. If the configuration synchronization is lost, heartbeats are lost. Both devices determine that the other is down, and both become active.
- You can configure the management interfaces on the HA devices to provide a backup path for heartbeat and hello messages using the heartbeat backup configuration option.

Beginning with PAN-OS 7.0, Palo Alto Networks firewalls (physical and VM-Series) support active/passive and active/active high availability configurations, complete with session and configuration synchronization. PA-200 only supports HA Lite without session synchronization capability. Also, the VM-Series firewall in Amazon Web Services supports only active/passive HA.

Control Link (HA1):



The HA1 link is used to **exchange hellos, heartbeats, and the HA state information**. The HA1 link is used to **exchange management plane sync for routing & User-ID info**. HA1 acts to monitor **HA status such configuration synchronization** for active-passive. HA1 acts **keepalive** between HA agents, it senses power cycle, reboot & power down. The PA firewalls also use this link to synchronize configuration changes with its peer. HA1 link is a Layer 3 link and the only HA link that requires an IP address information. Internet Control Message Protocol is used to exchange heartbeats between HA peers. Ports used for HA1 link—**TCP port 28769 and TCP 28260** for clear text communication. Port used for HA1 link- **Port 28** for encrypted communication Secure Shell over TCP. Default monitor hold time is 3000 ms & HA1 link also called Control or management.

Active/Passive configuration support the use of layer 2, layer 3, and v-wire interfaces, but not Tap interfaces.

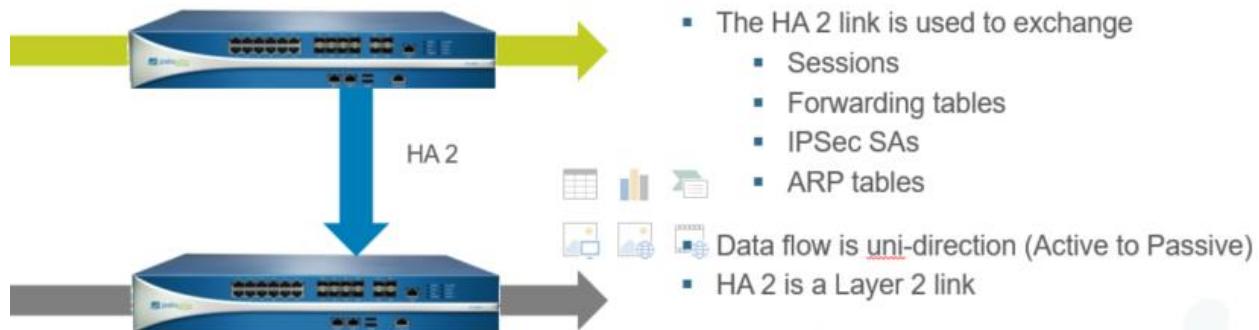
Dedicated interfaces for HA1 and HA2 exist on PA-3000, PA-4000, and PA-5000 Series firewalls. All other devices require data interfaces to be configured for HA use. Links do not have to be directly connected.

Cabling: For devices with dedicated HA ports, use an Ethernet cable (straight through) to connect the dedicated HA1 ports and the HA2 ports on the device pair. For devices that are directly connected, auto-sensing will take place and so you may use either an Ethernet cable (straight through) or a crossover cable.

For devices without dedicated HA ports, select two data interfaces for the HA2 link and the backup HA1 link. Then, use an Ethernet cable to connect these in-band HA interfaces across both devices. Use the management port for the HA1 link and ensure that the management ports can connect to each other across your network.

Please note that heartbeat polling occurs in both directions between the control planes of the active and passive devices to determine the health of each.

Data Link (HA2):

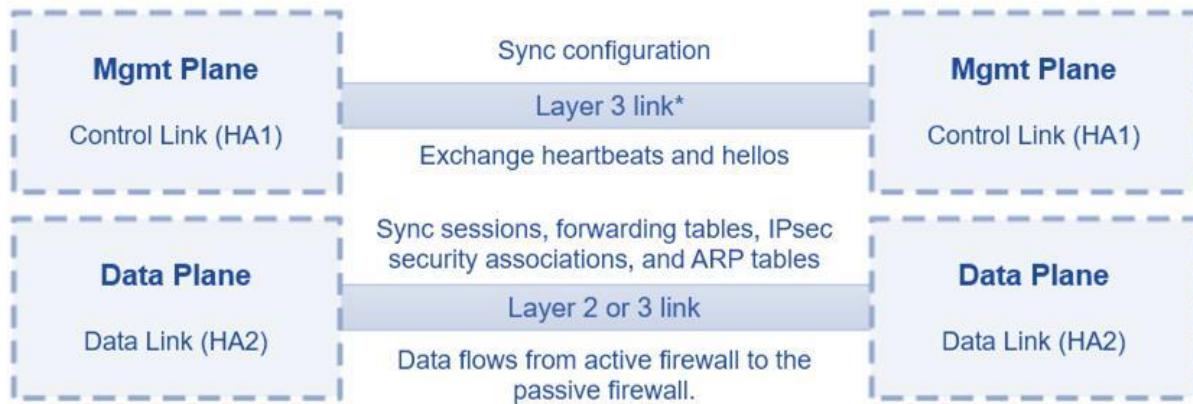


HA2 link is used to **synchronize sessions, forwarding tables, IPSec security associations**. The HA2 link is also used to **synchronize ARP tables** between PA firewalls in the HA pair. HA2 is used to synchronize **HA states, routing info, IPSec security association, ARP table**. Data flow on the HA2 or data link is always **unidirectional except for the HA2 keep-alive**. It flows from active or active-primary firewall to the passive or active-secondary firewall. The Data link are unidirectional and flows from the active firewall to the passive firewall. **HA2 is layer 2 link**, no IP address is required although you can specify layer3 information. A layer 3 link or IP address is required only if the data link are not on the same subnet.

HA Backup Links (HA1-B, HA2-B):

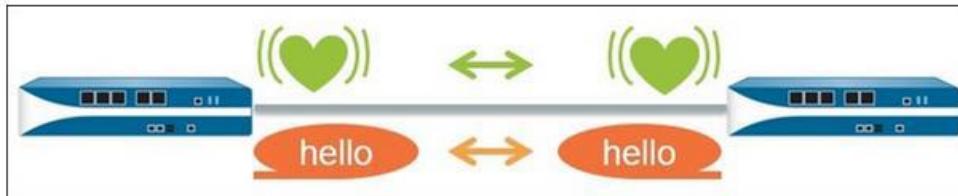
In High Availability HA backup links provide redundancy for the control and data links. Backup and primary links need to be on a different subnet from the primary HA Links. The HA1 backup ports and HA2 ports must be configured on separate physical ports. The ip addresses of the primary and the backup HA links must not overlap each other. The purpose of configuration a backup control link is to avoid the split-brain scenario. The Split-Brain occurs when a non-

redundant control link or HA1 link goes down. Passive firewall concludes that active firewall is down and attempts to start services.



Heartbeat Polling and Hello messages:

The **heartbeat** is an ICMP ping to the HA peer over the Control link, and the peer responds to establish that the firewalls are connected and responsive.



Hello messages are sent from one peer to the other to verify the state of the firewall.

Hello Messages, are send from one peer to the other to verify the state of the firewall. The Heartbeat is an ICMP ping to the HA peer over the Control Link or Management Link. Firewalls use hello message and heartbeats to verify that the peer firewall is responsive. Firewalls use hello message and heartbeats to verify that the peer firewall is operational. Hello messages are sent from one peer to other at the configured Hello Interval to verify. The heartbeat is an Internet Control Message Protocol ping to HA peer over control link. The peer responds to the ping to establish that the firewalls are connected and responsive. By default, In Palo Alto Network Firewall the interval for the heartbeat is 1000 milliseconds. Ping is sent every 1000ms & if there are three consecutive heartbeat losses failovers occurs.

Link Monitoring:

- Monitors physical interfaces (“Link Group”)
- Monitor link state (link up / link down)

Multiple mechanisms can be configured to monitor status of the HA pair. Any of these events can cause a device to enter the nonfunctional state and to trigger a switchover in the event of a failure on the active device.

Link monitoring watches physical interface state on one or more interfaces. A set of interfaces can be grouped to create a link group and any or all logic can be applied to the group.

Physical interfaces to be monitored are grouped into a link group and their state is monitored. Palo Alto Network Firewall, link group can contain one or more physical interfaces or links. A PA Firewall failure is triggered when any or all of the interfaces or link in the group fail. Default behavior is failure of any one link in the link group will cause the firewall to change. The High Availability (HA) state to non-functional to indicate a failure of a monitored object.

Link Group			
Name	Enabled	Group Failure Condition	Interfaces
main	<input checked="" type="checkbox"/>	any	ethernet1/1 ethernet1/2
Add Delete			

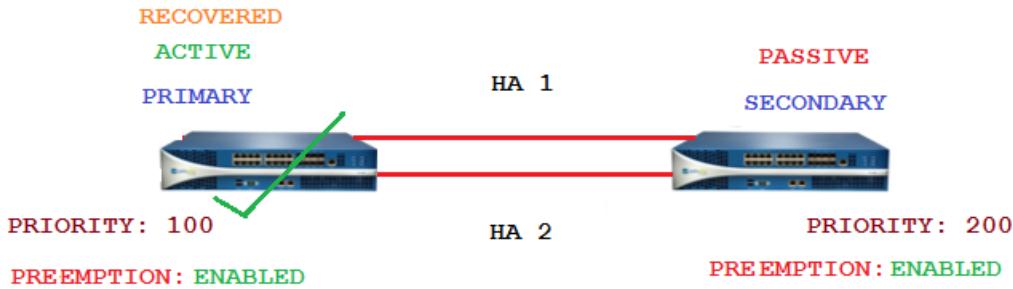
Path Monitoring:

- Define one or more paths to monitor specific destinations
 - Path types: vwire, VLAN or virtual router
 - Uses ICMP Ping to verify IP address reachability
 - Ping interval = 200 ms
 - Down = 10 consecutive ping failures

Path Group							
Name	Type	Enabled	Failure Condition	Source IP	Destination IP	Ping Interval	Ping Count
VR2	virtual-router	<input checked="" type="checkbox"/>	any		10.2.2.5 10.2.2.2	200	10
Add Virtual Wire Path		Add VLAN Path	Add Virtual Router Path	Delete			

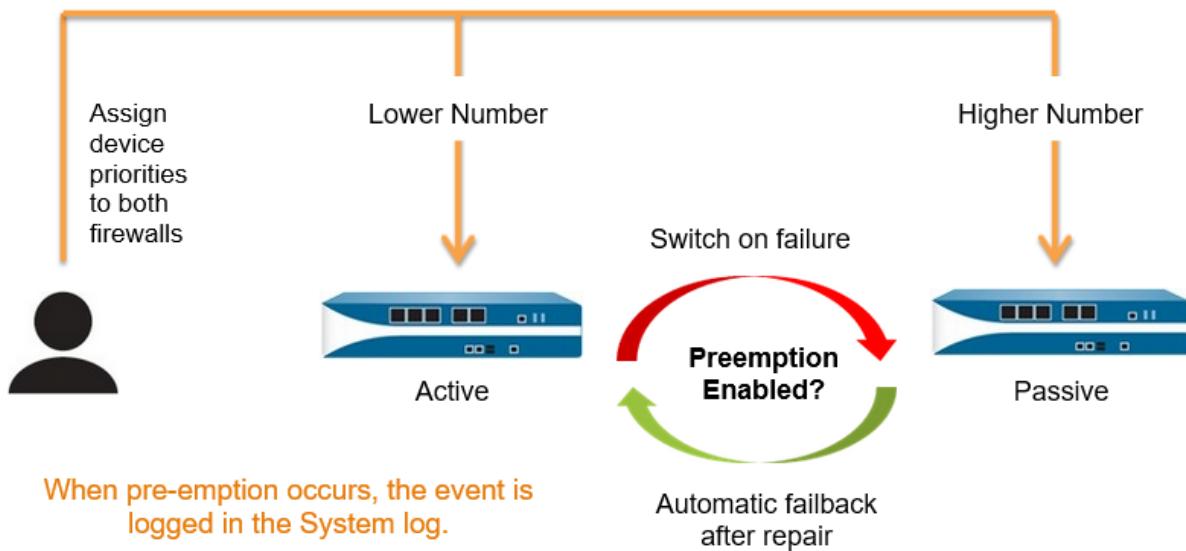
Path Monitoring monitors full path through the network to mission-critical IP addresses. Internet Control Message Protocol pings are used to verify reachability of the IP address. In Palo Alto Next Generation Network Firewall, the default interval for the pings is 200ms. The IP address is considered unreachable when 10 consecutive pings fail. Firewall failure is triggered when any or all of IP addresses monitored become unreachable. Default behavior is any one of the IP addresses becoming unreachable will cause firewall. To change High Availability state to non-functional to indicate failure of monitored object.

Priority:



When two Palo Alto Networks firewalls are deployed in the active-passive cluster. It is mandatory to configure device priority higher priority for passive low for active. Firewall with lower numerical value & therefore higher priority, is designated as active. The device priority decides which Palo Alto firewall will preferably take the active role. Which Palo Alto firewall will take over the passive role when both the firewalls boot up.

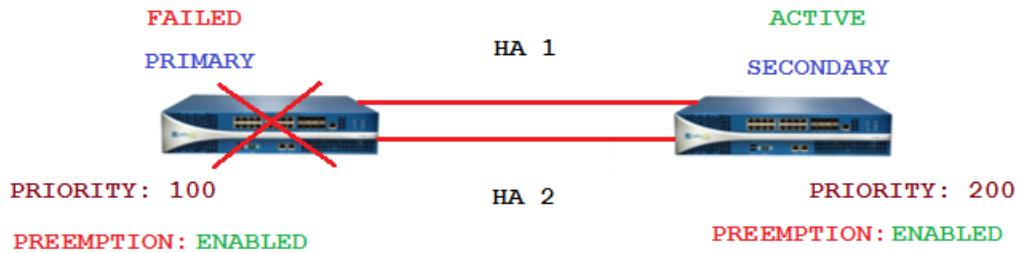
Preemption:



The Preemptive behavior allows firewall with lower numerical value to resume as active. By default, preemption is disabled on the firewalls and must be enabled on both firewalls. Preemption which influences this behavior on the event of it being enabled or disabled. When preemption occurs, event is logged in the in Palo Alto Network Firewall system logs.

Failover and Trigger Settings:

When a failure occurs on one firewall and the peer takes over the task of securing traffic. Procedure by which firewall automatically transfers control to peer when it detects a fault. The failover operation is the process of switching production to a backup facility or firewall. A failover is triggered, for example, when a monitored metric on the firewall in HA pair fails.

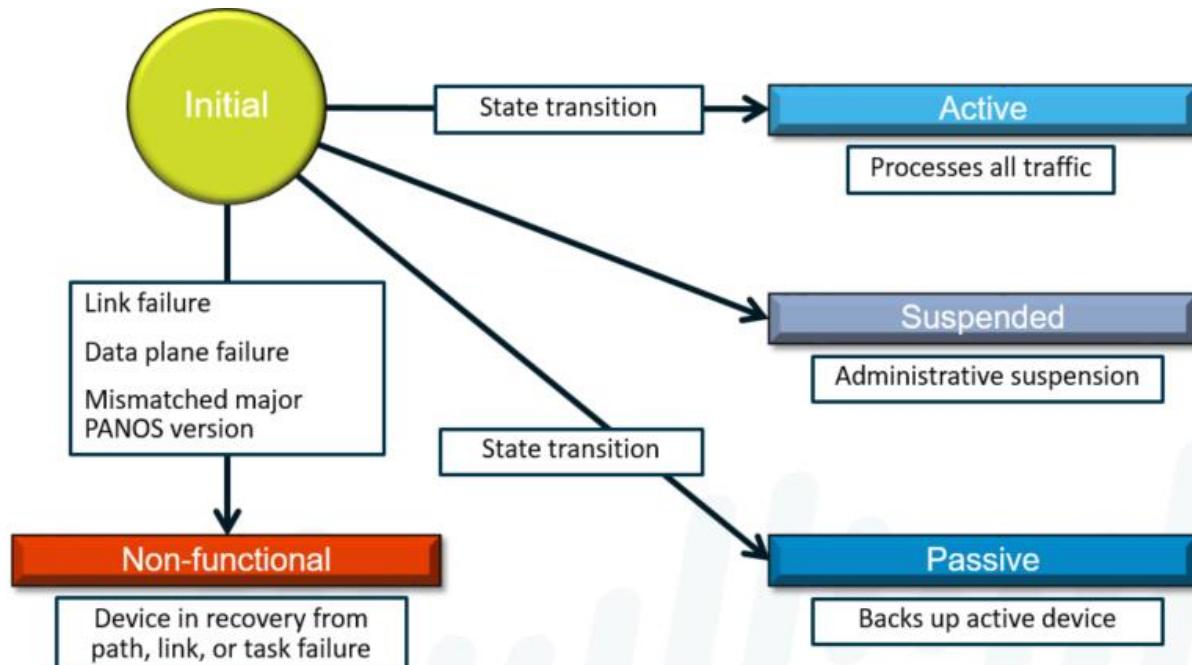


▪ High Availability

- Failover triggers
 - A failover can occur at failure of an **internal health check**
 - Internal health check is a verification of operational status
 - Only on PA-3000, PA-5000, PA-7000
 - Not configurable
- Failover timers
 - Recommended (typical timers)
 - Aggressive (faster failover settings)
 - Advanced (configurable)

Timers	Description	PA-7050	PA-2000 Series	Panorama Virtual Appliance
		PA-5000 Series	PA-500 Series	Panorama M-Series
		PA-4000 Series	PA-200 Series	
		PA-3000 Series		
	VM-Series			
Promotion hold time	Time that the passive device (in active/pассив mode) or the active-secondary device (in active/active mode) will wait before taking over as the active or active-primary device after communications with the HA peer have been lost. This hold time will begin only after the peer failure declaration has been made.	2000/500	2000/500	2000/500

Active/Passive HA States:



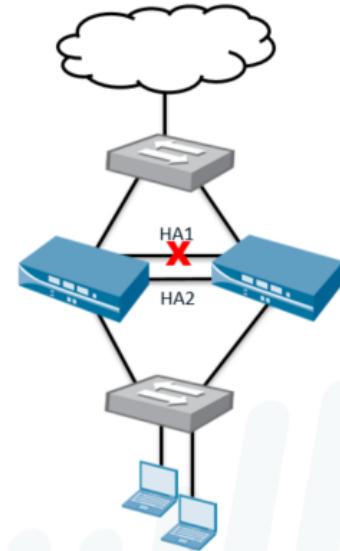
Split Brain:

Split brain is a high-availability term that refers to the situation where both nodes in an HA pair are trying to take control.

- Certain dataplane issues can disrupt traffic, but not result in complete dataplane failure, which leaves the firewall in a partially running state.
- Without a dedicated non-in-band HA1 control link, such dataplane issues could result in HA control traffic not being passed between HA pair members.
- This disruption of traffic would cause both devices to “think” that the other was unavailable and cause both devices to go into an active state at the same time.

The PA-3000, PA-4000, and PA-5000 Series firewalls have dedicated, in-band HA1 control links and would not be subject to this specific split-brain scenario.

- High Availability
 - Split Brain
 - Occurs when HA 1 communication goes down but the device is still functioning
 - Both firewalls think the other is down



Split-Brain: The Solution:

One way to prevent split brain is to select the Heartbeat Backup option when configuring HA.

- This option uses the management (MGT) interface on the HA devices to provide a backup path for only heartbeat and hello messages. No other HA1 functionality is provided.
- The HA1 port on the fully functional device contacts the MGT port via its IP address.
- The MGT interface IP address is shared with the HA peer through the HA1 control link prior to the failure.

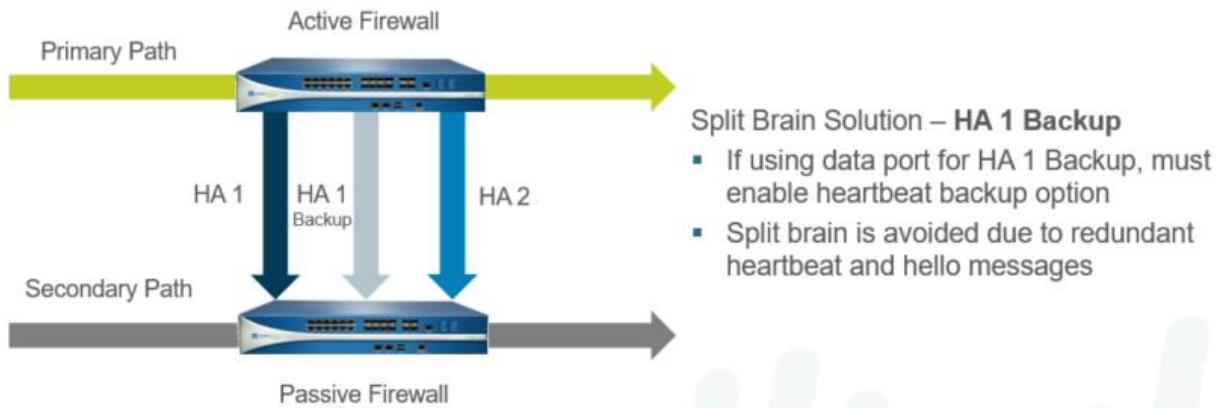
Split brain can also be avoided in many cases by configuring a fully independent backup HA1 link.

- When the HA1 link goes down, the firewall switches all HA1 traffic to the backup HA1 link.
- If either hellos or heartbeats are also failing on the backup link, then the HA1 failure is treated as a device failure.
- Communications failures when using the MGT interface are indicative of a management plane failure and are a clear indicator of a device failure.

When the HA1 traffic successfully fails over to the backup link, a log indicates that the firewall is not failing and all hello and heartbeat protocols behave as they would if they were coming over the HA1 link.

No configuration synchronization or other application synchronization (e.g., User-ID, routes, DHCP) use the backup HA1 link when the primary link is down if the Heartbeat Backup option is selected and the MGT interface is used as the HA1 Backup interface.

Backup HA1 links and the Heartbeat Backup option can be combined on the same HA pair.



Active/Active High Availability:

A PAN-OS HA pair consists of two identical Palo Alto Networks firewalls with identical software that enforce the same overall security policy and share the same configuration settings.

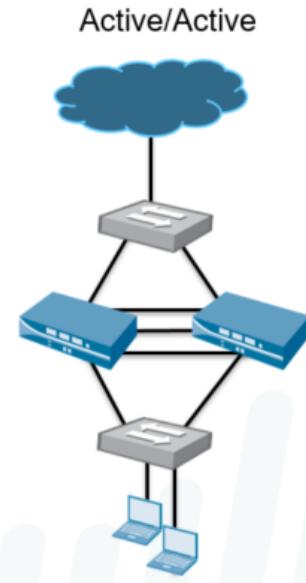
With active/active deployment, both devices are active and processing traffic.

Active/active HA is supported only in the Virtual Wire and Layer 3 modes. Such deployments are most suited for scenarios involving asymmetric routing.

Beginning with PAN-OS 7.0, Palo Alto Networks firewalls (Physical and VM-Series) support active/passive and active/active high-availability configurations, complete with session and configuration synchronization.

In an HA pair, both peers must be of the same model, must be running the same PAN-OS version, and must have the same set of licenses.

- Devices back each other, taking over primary ownership if the other one fails
- Both devices in the pair are:
 - Actively processing and passing traffic
 - Load-sharing the traffic
- No increase in session capacity
- Not designed to increase throughput
- Virtual Wire and Layer 3 modes only
- Recommended only in environments with asymmetric routes



For the VM-Series firewalls, both peers must be on the same hypervisor and must have the same number of CPU cores allocated on each peer.

Note these exceptions: The PA-200 only supports HA Lite without session synchronization capability and cannot be configured for active/active HA. Also, the VM-Series firewall in Amazon Web Services (AWS) only supports active/passive HA.

For devices without dedicated HA ports, select two data interfaces for the HA2 link and the backup HA1 link. Then, use an Ethernet cable to connect these in-band HA interfaces across both devices. Use the management port for the HA1 link and ensure that the management ports can connect to each other across your network.

Cabling: For devices with dedicated HA ports, use an Ethernet cable (straight through) to connect the dedicated HA1 ports and the HA2 ports on the device pair. For devices that are directly connected, auto-sensing will take place and so you may use either an Ethernet cable (straight through) or a crossover cable.

While in Active/Active pairs, the member Devices have specific tasks they perform:

Active-Primary – processing traffic and acting as the primary device

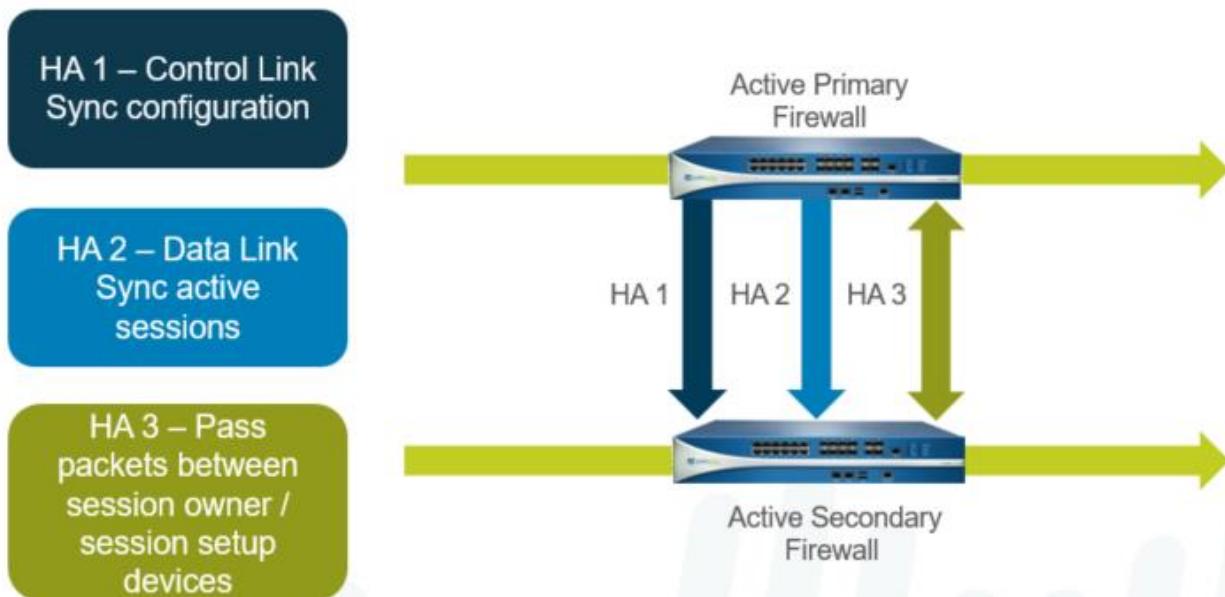
Handles User-ID agent connections

Runs DHCP server/relay

Matches NAT / PBF rules

Active-Secondary – processing traffic, backs up Active-Primary

Active-Active HA Links:



In addition to the HA1 and HA2 links used in active-passive, active-active deployments require a dedicated HA3 link. This link is used as a packet-forwarding link for session setup and asymmetric traffic handling.

Due to this requirement, carefully consider the sizing of the HA3 link. Excessive packet passing between session owner and setup devices could overrun a single HA3 link. Aggregate interfaces should be considered for HA3 links if the firewall model supports link aggregation.

Each device is assigned a device ID of either 0 or 1 during configuration.

If the devices are assigned the same device ID, the pair will not form successfully.

The device ID is used only to differentiate between the firewalls during configuration.

Active-primary or active-secondary status is determined by an assigned priority value.

Session Ownership:

The device that receives the first packet (in a new session) is the session owner.

All Layer 7 processing in that session is handled by the session owner.

Session Setup:

Session setup may be distributed among devices in HA group using IP modulo or IP hash.

Layer 2 through Layer 4 processing is handled by the session setup device.

In an active-active pair, the packet handling can be distributed between the two devices. Two important functions are handled by the devices in a pair:

Within an active-active pair, the session owner device can be either the firewall that receives the first packet of a new session, or the device in the active-primary state. This device is responsible for all Layer 7 processing (i.e. App-ID, Content-ID, and threat scanning) for this session. This device is also responsible for generating all traffic logs for the session.

The session setup device is responsible for the Layer 2 through Layer 4 processing required to set up a new session.

Address translation is performed by the session setup device.

The session setup device is determined by configuring the Session Setup option in the Active-Active tab. After session setup, the packet is forwarded back to the session owner for all Layer 7 processing to preserve the forwarding path.

The separation of session owner and session setup devices is necessary to avoid race conditions that can occur in asymmetrically routed environments. If the session owner and session setup device are different firewalls, the packets will be passed between the devices over the HA3 link.

Session ownership can be done in one of two ways:

First packet: The device that receives the first packet (in a new session) from the source host owns the session (session owner).

Primary device: The device in the active-primary state owns the session. If this option is selected and the device that received the first packet is not in the active-primary state, the packets are forwarded to the peer device over the HA3 link.

Palo Alto Networks recommends setting the session ownership option to First Packet for production environments.

The Primary Device option is provided as a troubleshooting tool to ensure that all logs are on a single device for ease of access. However, this option potentially adds additional load to the HA3 link, which makes it less desirable for general use.

For devices with dedicated HA ports, use an Ethernet cable to connect the dedicated HA1 ports and the HA2 ports on the device pair. Use a crossover cable if the devices are directly connected to each other.

For devices without dedicated HA ports, select two data interfaces for the HA2 link and the backup HA1 link. Then, use an Ethernet cable to connect these in-band HA interfaces across both devices. Use the management port for the HA1 link and ensure that the management ports can connect to each other across your network.

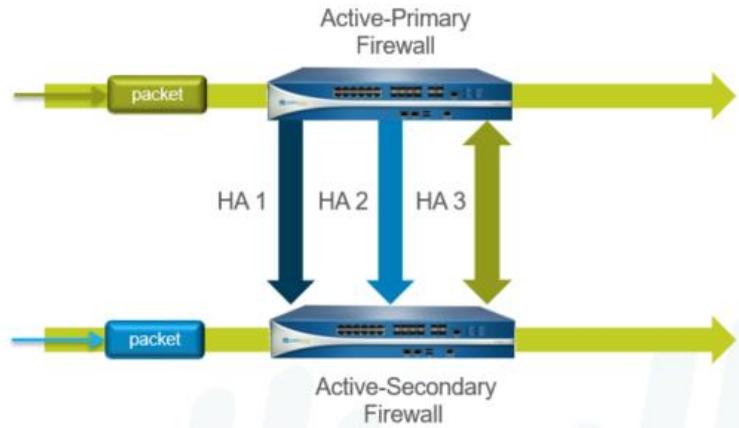
Session Owner:

When a packet arrives at the firewall, it is compared against existing sessions to see if it is part of an established connection. If not, the packet is assigned a session owner. If the receiving

firewall is not the session owner, the packet is forwarded across the HA3 link to the peer device.

Next, the session owner determines the session setup device, based on the HA configuration.

- Performs all Layer 7 inspection
 - App-ID
 - Content ID
- Evaluates Security Policies
- Logs traffic



Session Setup:

- The setup device is responsible for Layer 2 to Layer 4 processing
- Address translation is performed by session setup FW
- If session ownership is set to active-primary firewall:
 - Session setup defaults to active-primary
 - Not recommended since all traffic will be handled by active-primary FW.



Active/Active HA States:

Device states – Active/Active

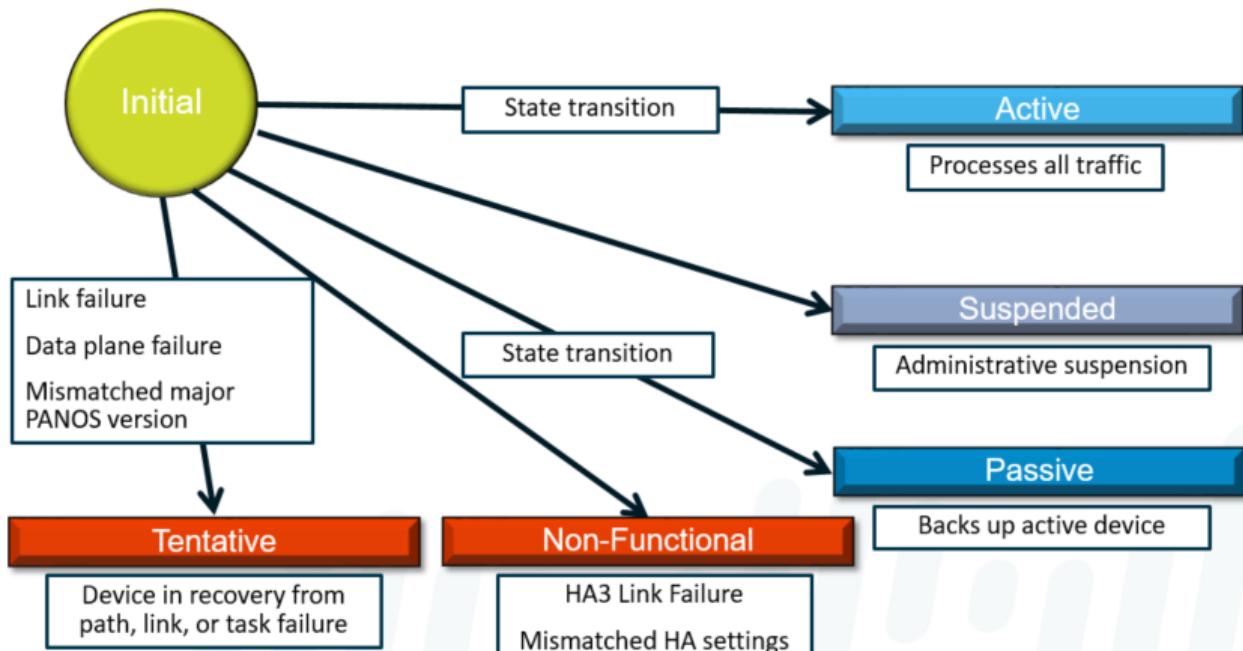
Tentative – State caused by path/link monitor failure

A device in this state will synchronize sessions, and configurations from the peer device.

Non-effected Layer 3 interfaces will stay up and continue participating in routing and packet forwarding utilizing the HA3 interface.

Non-functional – Error state due to mismatched A/A settings, HA3 link down

Suspended – Administrative suspend



Active/Active HA Deployment

Floating IP Deployment:

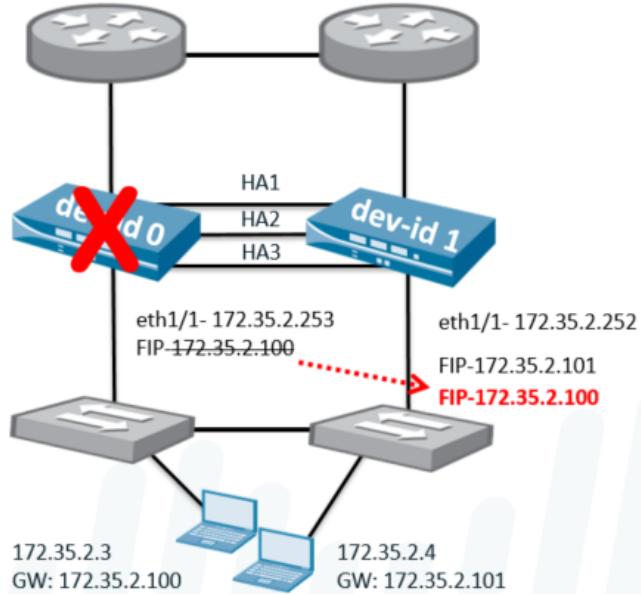
In a floating IP deployment, network redundancy is achieved through the use of IP address that can be moved between the HA devices. The individual devices host the floating IP address on a Layer 3 interface that is also assigned a static address. To ensure no disruption of connectivity due to ARP request errors, a virtual MAC address is assigned with the floating IP, which prevents the need for ARP resets after a failover.

Floating IP addresses are recommended when Virtual Router Redundancy Protocol (VRRP) style functionality is required. Floating IP addresses can be used in VPN and Network Address Translation (NAT) configurations, which allows for persistent connections when a failure occurs on the device offering those services.

End users are configured to connect to the floating IP address instead of the static address of the interface, which allows their connections to seamlessly migrate to the other firewall on failover. Both devices should be configured with floating IP addresses so that traffic can be

distributed among them. Load balancing can be implemented manually (e.g., assign default gateways on different clients to different firewalls) or through the use of external load balancers.

- Floating IP addresses and virtual MAC addresses move between devices on failover
- Supports VPN and NAT implementations
- Can use external load balancers to spread traffic across devices



ARP Load-Sharing Deployment:

A simpler approach to load-sharing and redundancy is ARP load-sharing. In this scenario, a single IP address is shared between interfaces on the HA peers. However, each device is assigned a unique virtual MAC address to be used with the shared address.

The shared address is distributed to end hosts as the default gateway.

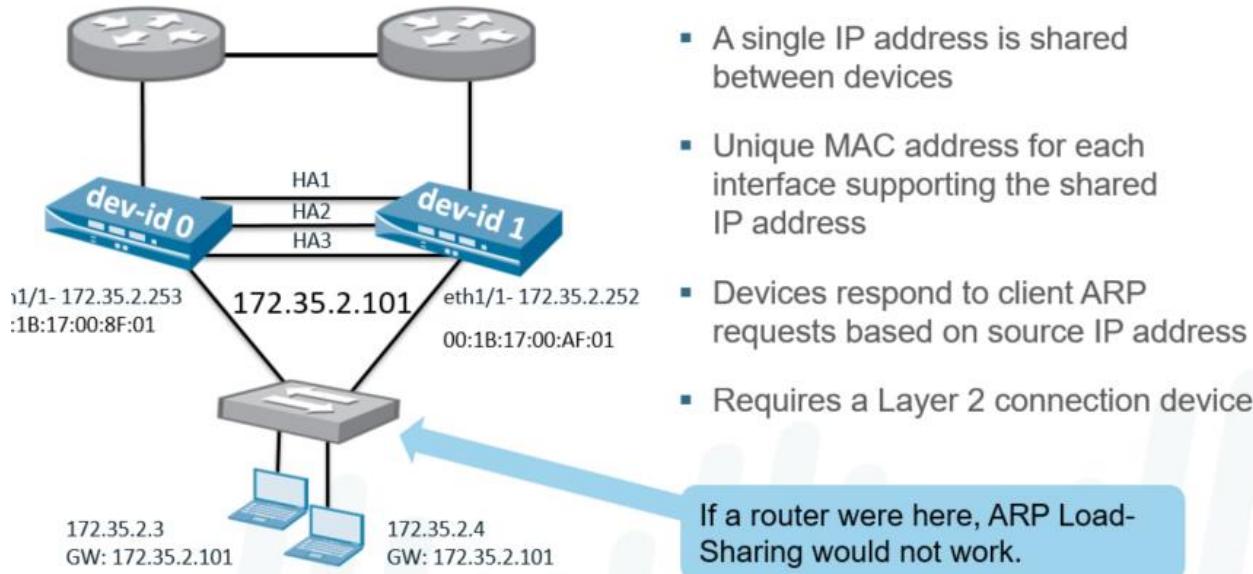
When the end hosts send ARP requests for the shared IP address, one of the firewalls responds with its virtual MAC address.

The responding device is determined by a hash or modulo of the source IP address initiating the ARP request.

The end-user device caches the MAC address locally and uses this address to forward traffic for the life of the ARP cache.

In the event of a firewall failure, the surviving device uses both virtual MAC addresses and sends a gratuitous ARP request to update the MAC table of the connected switches.

ARP load sharing should be used when the firewall and hosts exist on the same broadcast domain. If Layer 3 separation exists, the benefits of ARP load sharing is lost.



- A single IP address is shared between devices
- Unique MAC address for each interface supporting the shared IP address
- Devices respond to client ARP requests based on source IP address
- Requires a Layer 2 connection device

- 2 firewalls can be configured in a High Availability pair
- HA Provides:
 - Redundancy
 - Business Continuity
 - If one firewall fails, the second can continue service with little to no interruption
- HA options can be deployed as:
 - Active/Passive: One active, one standby firewall
 - Active/Active: Both Active, used in specific circumstances, such as asynchronous routing setups
- Items Synchronized include:
 - Networks
 - Objects
 - Policies
 - Certificates
 - Session Tables (not available on the PA-200)
- Items NOT Synchronized:
 - Management Interface configuration
 - HA Settings
 - Logs
 - ACC information
- For a consolidated application and log view, Panorama must be used.
- PA-200 only supports HA-Lite

- Lite is only available due to the low number of ports available on this model

- A/P Deployment

- Only one firewall is active
- One firewall synchronized and ready to process traffic
- No increase in session capacity or network throughput
- Supports VWire, Layer 2, and Layer 3 deployments
- A/P HA has simplistic design to help with implementation.

- A/A Deployment

- Both firewalls are active and processing traffic
- Both individually maintain routing and session tables, sync'd to the other
- Is for use in Asynchronous routing deployments
- No increase in throughput/session tables
- Supported in V-Wire and L3 deployments

- HA Prerequisites

- Both firewalls must be running the same hardware or VM model
- Both firewalls must be running the same version PanOS
- Starting in 7.0, session syncing is an option when upgrading major and minor releases
- Updated and current Threat, URL and App DB's
- Same dedicated HA interfaces
- Licenses are unique to each FW; each needs matching licenses
- Matching Slot configurations (for chassis 5000/7000 series)
- VM's must be on the same hyper-visor, and have same number of CPU Cores

HA Components and Operations

- HA Control Link is L3 link that requires an IP address.

- Used to exchange heartbeats and hellos and HA state info
- Used to exchange routing and user ID information
- Active firewall uses this to exchange config change information

- HA Datalink is a L2 Link, but can be configured in L3 that requires an IP

- L3 is required if the data links are not on the same subnet
- In L2 mode, the Datalink uses ethernet type 0x7261
- The Datalink synchronize sessions, forwarding table, IPSec SA's and ARP tables in the HA Pair
- Dataflow is unidirectional from the Active to Passive firewall.

- Some models have dedicated HA ports, other models will use MGT or other in-band ports

- Dedicated HA Ports are on 3000, 4000, 5000 and 7000 models
- HA1/HA2 ports can be directly connected via ethernet cable
- Recommended to use the MGT port as the control link
 - Any in-band port used must be configured as type HA
- HA Backup Links are recommended for the control link, to prevent the FW's going into 'split-brain' mode
 - Backup links must be on separate physical ports
 - Backup links must be in separate subnets as the primary backup links
- PA-7000 series mandates the use of specific ports on the Switch Management Card (SMC)
 - HA1-A is the control link; connect to same port on the 2nd firewall (or through switch/router)
 - HA1-B is the backup control link; connect to same port on 2nd firewall (or through switch/router)
 - Backup control link cannot be configured on the MGT or NPC Data ports.
 - High Speed Chassis Interconnects (HSCI) are used as the Primary and backup Datalinks
 - If distance is beyond the scope of the HSCI ports, inband ports can be used.
- HA firewalls can be set with a device priority to indicate a preference for which should be active.
 - Enable Pre-empt on both firewalls if you want one firewall to become the active firewall when it is available/brought online.
- Failure Detection
 - Hello and Heartbeats to confirm responsiveness and availability
 - Link Groups can be configured to validate interfaces are up
 - Path groups can monitor remote IP's to validate reachability
 - These items can be configured for any/all and the failure conditions.
 - Internal Health checks are done to validate hardware is healthy
- HA Timers
 - HA Timers enable the firewall to detect failures and fail over
 - Timer profiles simplify setting HA timer settings
 - Advances enables individual timer modification
- HA Heartbeat on the management port
 - Helps to prevent split-brain
 - Happens when a non-redundant control link goes down

Active/Passive HA Configuration

- Prepare In-band Interface

- Set interface type as HA
- Configured under Device > High Availability
 - Each section here can be configured depending on the needs of the deployment
- Enable HA A/P mode under Device > High Availability > General
 - Select Mode (A/A or A/P)
 - Matching Group ID's for the HA Pair
 - Description (useful if configuring multiple HA configurations)
 - Check enable config sync to automatically sync any config changes to the peer
 - Add the Peer IP address
 - HIGHLY recommended to add a backup peer IP Address
- Configure the Control Link
 - Under Device > High Availability > General
 - Select the Control Link (HA1)
 - Select management port or another configured in-band port
 - MGT Port is recommended if a dedicated HA port is not available
 - Add a gateway if the peer is in a different subnet
 - Control link can be encrypted
 - Private keys will need to be exported/imported from the certificate configuration for this to function.
 - Backup link can be configured using an in-band port
- Configure the DataLink
 - If available, configured on the HA2 link
 - If using in-band and the peer is on a different subnet, add a gateway
 - An HA2 keepalive can also be configured.
 - To prevent split-brain, use the action 'log only'
 - Select 'session synchronization' to ensure sessions are sync'd
 - A backup datalink can also be configured
- Election Settings
 - Device Priority can be set if one should be preferred to be the Primary
 - (correction provided by /u/stangri-la) Preemptive can be set if a specific firewall should be primary if available. The firewall with the lower numerical value has the higher priority and will be primary if both are active and pre-empt is set.
 - HA Timer can be changed, however leaving at recommended unless a specific reason is needed for change
- (Optional) set the passive link state to auto

- **Link Monitoring (Optional)**
 - Configured under Device > High Availability > Link and Path Monitoring
 - Different link groups can be configured with different failure conditions
 - Example: Critical links can force a failover if any of the links fail. other links can be set if all links fail (Aggregate interfaces, which would likely be a switch failure, for example).
 - **Path Monitoring (Optional)**
 - Configured under Device > High Availability > Link and Path Monitoring
 - Options for VWire Path, VLAN Path and/or a Virtual Router Path.
 - A VWire will need a source and destination IP
 - Virtual Router monitoring does not need a source, as a route lookup will be done to determine the source.
- Monitoring HA state**
- During Boot, a FW looks for an HA Peer; after 60 seconds, if a peer hasn't been discovered, the FW will boot as Active.
 - If a peer is found, it will negotiate with the peer
 - If Preempt is active, determine who has highest priority – this FW becomes active.
 - If a FW is in a suspend state, it will not participate in a FW election
 - States an A/P FW can be in are:
 - Initial – Transient state when it joins an HA pair
 - Active – normal state, primary and processing traffic
 - Passive – normal traffic is discarded, may process LLDP and LACP traffic
 - Suspended – administratively disabled
 - Non-functional – FW is non-functional and will need to have the issues resolved before it can return to service.
 - States of the individual members can be added as a widget on the Dashboard
 - Add under Dashboard > Widgets > System > High Availability
 - This will show at a glance the status
 - Green: Good
 - Yellow: Warning (normal state for a standby firewall in an A/P pair)
 - Red: Error to be resolved
 - When an HA Pair is initially formed, a manual sync will need to be done. This screen can initiate a 'sync to peer' push.
 - System Log will show the events in an HA Pair negotiation.

----- END -----

Day 09

SSL Decryption and APP-ID

SSL Decryption

- > SSL Encryption Overview
- > Certificate Management
 - 1. Self-Signed vs CA-Issued Certificates
 - 2. Forward Trust and forward untrust Certificates
- > Decryption impact (Resource intensive, Performance impact)
- > Outbound SSL Decryption
- > Inbound SSL Decryption
- > Decryption Profiles
- > SSL Decryption Notification Page
- > Hardware Security Modules

Troubleshooting ::

```
> debug dataplane pool statistics | match proxy  
> show session all filter ssl-decrypt yes state active  
-> show system setting ssl-decrypt setting  
-> show counter global filter category proxy  
-> debug dataplane pool statistics  
-> show system setting ssl-decrypt exclude-cache  
# set shared ssl-decrypt ssl-exclude-cert foo.com  
# delete shared ssl-decrypt ssl-exclude-cert foo.com  
-> show system setting ssl-decrypt certificate  
-> show session all (look for *NS Flag)
```

App-ID

Applications on a Traditional Firewall

Case 1: DNS Traffic – Traditional vs. Palo Alto Networks Firewall

[Case 2: BitTorrent – IPS vs. App-ID](#)

[Case 3: Zero-Day Malware – IPS vs. App-ID](#)

[App-ID Flow](#)

[Application Shift](#)

[App-ID Components](#)

-> [Protocol decoders](#)

-> [Application signatures](#)

-> [Protocol decryption](#)

-> [Heuristics](#)

[Examining UDP Packets](#)

[Examining TCP Packets](#)

[Application Block Response Pages](#)

[Application Updates](#)

[Application Signatures](#)

[Application Dependencies \(example application office-on-demand\)](#)

-> [Applications with Implicitly Used Applications \(Facebook-base\)](#)

-> [Applications that Depend on Applications](#)

[Application Filters](#)

[Application Groups](#)

[App Override](#)

SSL Encryption Overview:

The two broad categories of encryption algorithms are symmetric and asymmetric.

Asymmetric key encryption (public key encryption) uses two different keys for encryption and decryption.

- When data is encrypted with one key, it can be decrypted only by the other key in the pair.
- The advantage of asymmetric encryption is that it allows for a secure transfer of information between parties that have no pre-existing communication.

- With one private key and one publicly-available key, encrypted traffic can be sent between any two users of this system. The disadvantage of this method is that it is slow for computers to perform this type of encryption on the bulk of the messaging.

Symmetric key encryption (pre-shared secret) uses a single key to encrypt and decrypt messages.

- The greatest disadvantage of the method is that the key must be known by both parties before any secure communication can be used.
- The key must be exchanged through an existing secure channel.
- This limitation makes it hard to use for any kind of spontaneous exchange and it is impossible to securely send new key information if the current key is suspect.

- SSL uses symmetric and asymmetric encryption

- Asymmetric Encryption (Key Pairs)

- Authenticates the server
- Exchange the symmetric key



- Symmetric Encryption (Single Key)

- Bulk data encryption |



Pre-shared Secret

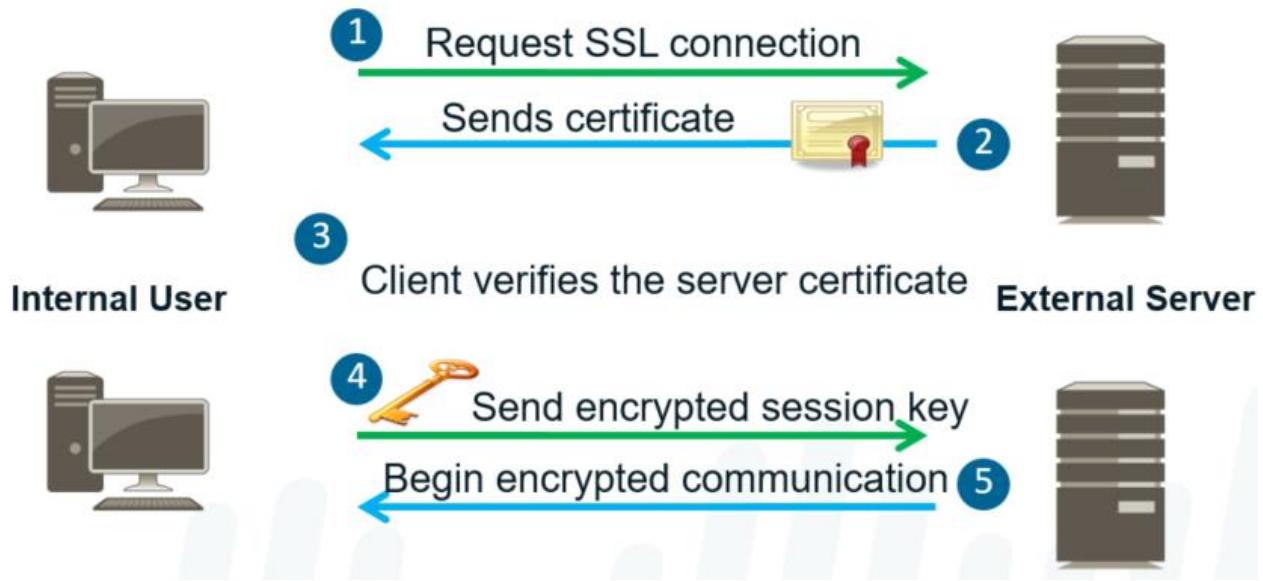
SSL Session Overview:

Secure Sockets Layer represents a protocol for encrypting a HTTP connection between a client and a server where no pre-existing secure channel is present. SSL takes advantage of the strengths of the symmetric and asymmetric encryption schemes.

Initiation of an SSL session follows this basic flow:

- A client requests a SSL connection.
- The server responds with its SSL certificate.
- The client validates the server certificate.

4. If the certificate is valid, the client uses the key to encrypt a symmetric session key and send it to the server.
5. At this point, both sides of the communication have the same symmetric key and can begin sending bulk data over their new secure channel. Periodically, they might need to establish a new session and rekey the communication.



Decryption Overview:

- **Why does the Palo Alto Networks firewall decrypt traffic?**
 - Sessions that attempt to hide their application signature encrypt the Layer 7 information
 - Sessions attempt to hide sensitive data in encrypted file transfers
- **Palo Alto Networks firewall acts as a forward proxy for outbound SSL decryption**
- **Palo Alto Networks firewalls listen on all ports and can decrypt:**
 - SSL inbound and outbound traffic
 - SSHv2
- **You can configure the firewall to decrypt traffic for visibility, control, and granular security.**
- **Decryption policies can apply to SSL and Secure Shell (SSH) traffic.**

- With the **SSH option**, the firewall selectively decrypts outbound and inbound SSH traffic to assure that secure protocols are not being used to tunnel disallowed applications and content.
- **SSL decryption and SSH decryption are disabled by default.**

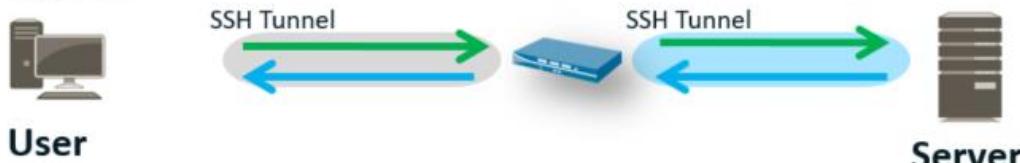
Decryption Policies:

The firewall can be configured to decrypt SSL and SSH traffic going to external sites. With the SSH option, you can selectively decrypt outbound and inbound SSH traffic to assure that secure protocols are not being used to tunnel disallowed applications and content. You can also apply decryption profiles to your policies to block and control various aspects of SSL traffic.

Assume a scenario where a user will connect via an encrypted connection to Facebook. The company policy is to allow employees to read Facebook, but prevent facebook-chat and facebook-posting. If SSL decryption is enabled for the Facebook application, this limitation can be accomplished easily with the Palo Alto Networks firewall. If SSL decryption is not enabled, then the firewall cannot tell what application is inside the SSL connection; let alone that application shifts are occurring within the connection.

Note that the Tap interface does not support SSL forward proxy or SSH decryption.

SSH Decryption



SSL Forward Proxy (Outbound SSL Decryption)



SSL Inbound Inspection



Decryption Impact:

While critical to security, Decryption is the most resource intensive operation on the firewall and will have significant performance impact.

The amount of traffic being decrypted must be considered when sizing a network for an appropriate appliance.

Resource intensive: 1. Impacted by Private Key size. 2. Impacted by Object size.

Performance impact: 1. All firewalls are significantly impacted by Decryption. 2. The PA-7000 series are equipped with additional processors that assist this function.

Certificate Management:

Self-Signed vs CA-Issued Certificates:

Self-Signed	CA-Issued Certificate
Straight-forward configuration through WebUI	More initial work and costs
Ideal for lab environments or test beds	Ideal for multibox deployments
To avoid browser errors, users must trust each firewall certificate independently	Users only need to trust one certificate authority

Certificate Configuration:

The certificate management interface provides access to all of the certificates that may be needed on the firewall. A self-signed certificate can be created for forward proxy SSL decryption or existing certificates and keys can be loaded for forward proxy and inbound SSL decryption.

Using an existing CA ultimately makes deployment of SSL decryption simpler:

- Any environment running Microsoft Active Directory or Novell eDirectory already has a certificate server available.
- The type of certificate needed for SSL decryption is a subordinate CA certificate.
- This certificate needs to be in PEM format, with the certificate in one file and the private key in another file.

Self-signed certificates can be generated easily using the WebUI:

- All fields of the certificate should be filled in.
- The name entered in this interface is the Publisher name on all decrypted certificates.

- If self-signed certificates are used for either the administrative WebUI or the SSL forward proxy, they can be exported from this page.
- After the certificates are exported, they can be added to users' browsers to avoid warning messages about unknown publishers.

Device > Certificate Management > Certificates

The screenshot shows the 'Certificates' section of the Device Management interface. The main table lists a single certificate named 'Self-signed SSL-D'. Below the table is a toolbar with buttons for Delete, Revoke, Renew, Import, Generate, Export, and Import HA Key. A red arrow points from the 'Generate' button in the toolbar to a detailed 'Generate Certificate' dialog box. Another red arrow points from the 'Generate' button in the dialog box to a 'Certificate' configuration window. The 'Generate Certificate' dialog includes fields for Certificate Name, Common Name, Signed By, OCSP Responder, Cryptographic Settings (Number of Bits, Digest, Expiration), and Certificate Attributes (Country, State, Locality, Organization). The 'Certificate' configuration window shows the details of the selected certificate, including its name, validity period, and various checkboxes for certificate types.

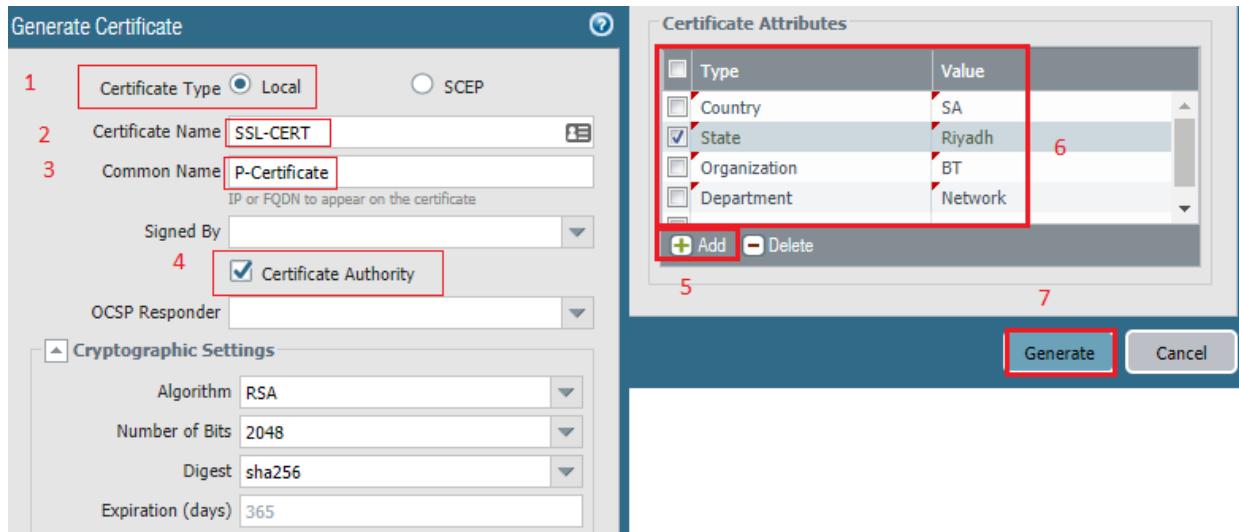
How to Generate Certificate for SSL Decryption and Import it on Client Machine:

Going to Device > Certificate Management > Certificates > Generate

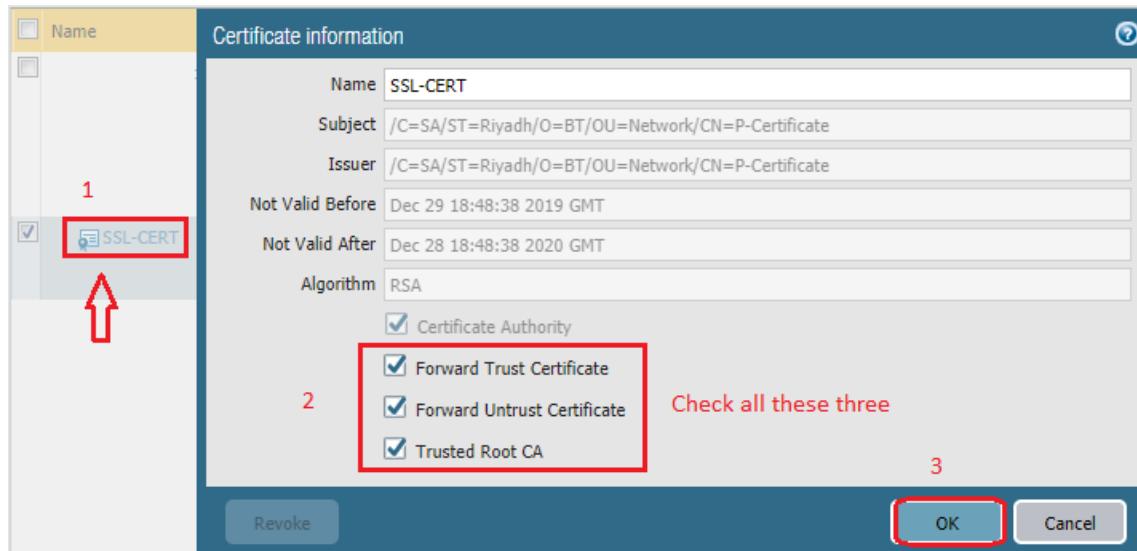
The screenshot shows the 'Certificates' section of the Device Management interface. The top navigation bar has a red box around the 'Device' tab. The left sidebar has a red box around the 'Certificates' link under the 'Certificate Management' section. A red callout with the text 'Click Generate button to create new certificate' points to the 'Generate' button in the toolbar at the bottom of the main content area. A red number '3' is placed near the 'Generate' button. The main content area displays a table of existing certificates, with one entry for 'SSL-Decryption'.

Type a name under Certificate Name (SSL-CERT) > type a name under Common Name (P-Certificate) > check Certificate Authority > leave the default settings under Cryptographic Settings. Under

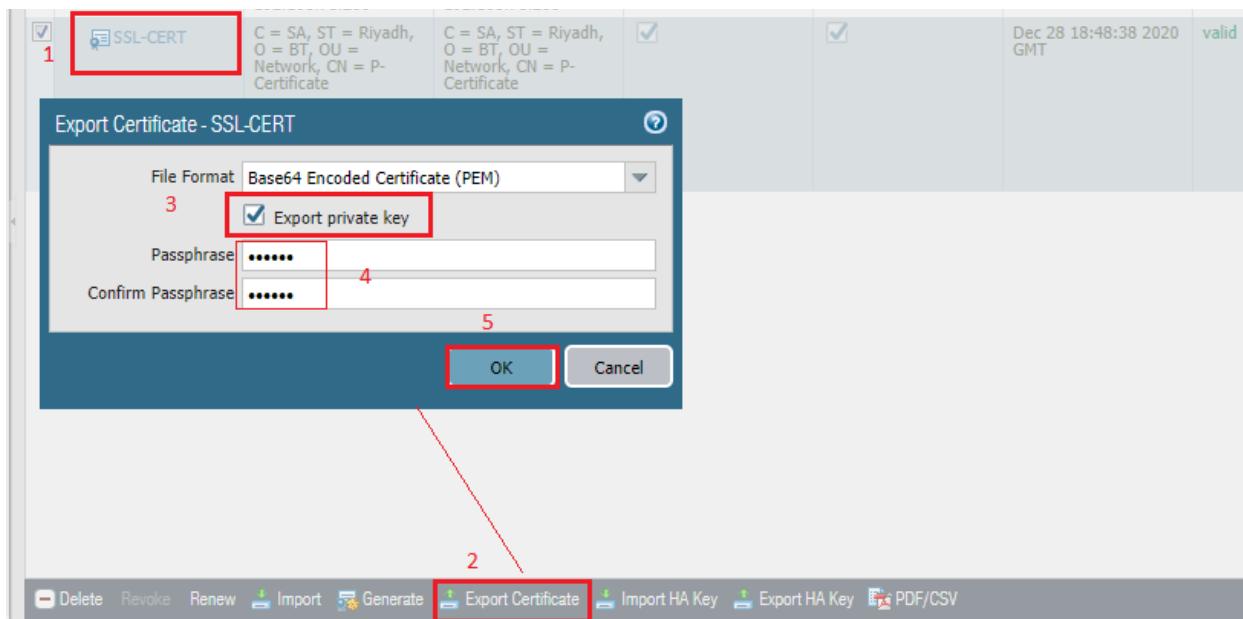
Certificate Attributes > click Add >Country > type and search for your country (SA in my case) > add and fill other Certificate Attributes as needed >Click Generate.



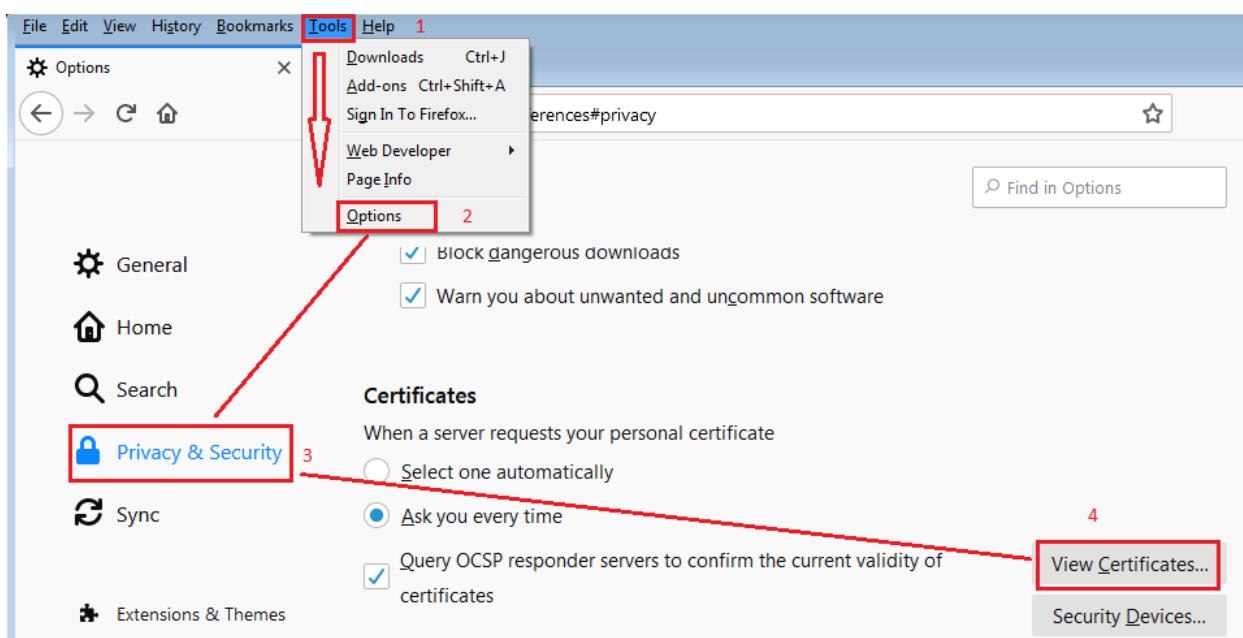
You need to modify the certificate by clicking on the Name of the certificate (SSL-CERT) > check Forward Trust Certificate, Forward Untrust Certificate and Trusted Root CA > click OK.



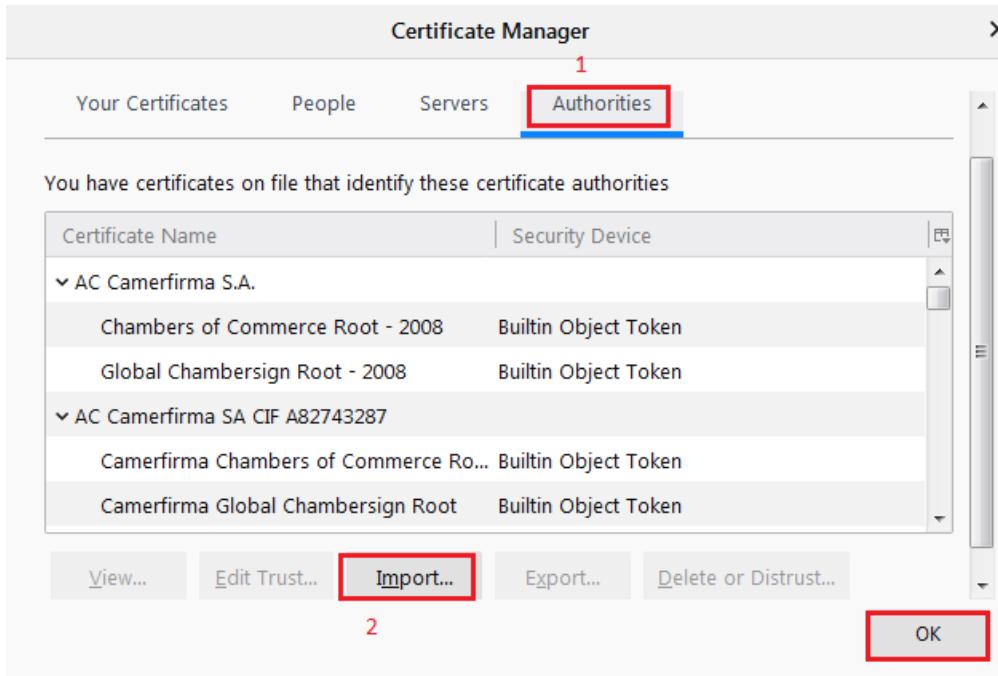
You can export the PAN certificate and install it on the PC web browser by clicking on the Name of the certificate and click Export. Leave the File Format of **Base64 Encoded Certificate (PEM)** > check **Export private key** > type a passphrase twice to confirm > click OK.



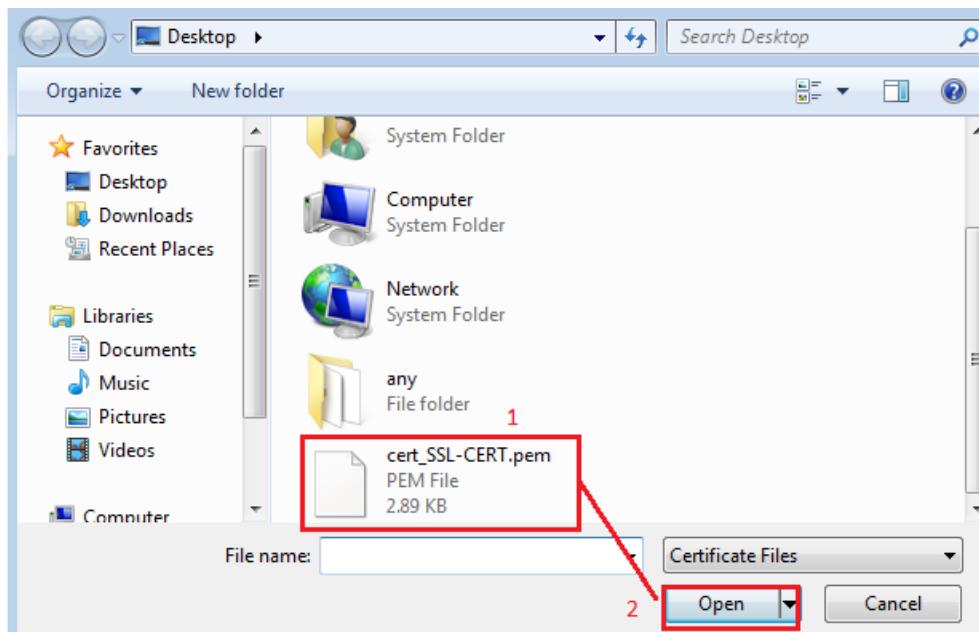
Go to the folder where the PEM certificate got downloaded. Copy the file and manually install the certificate on client PC. On the web browser (Mozilla Firefox) by going to Tools > Options. [Go to Privacy & Security> Certificates > View Certificates.](#)



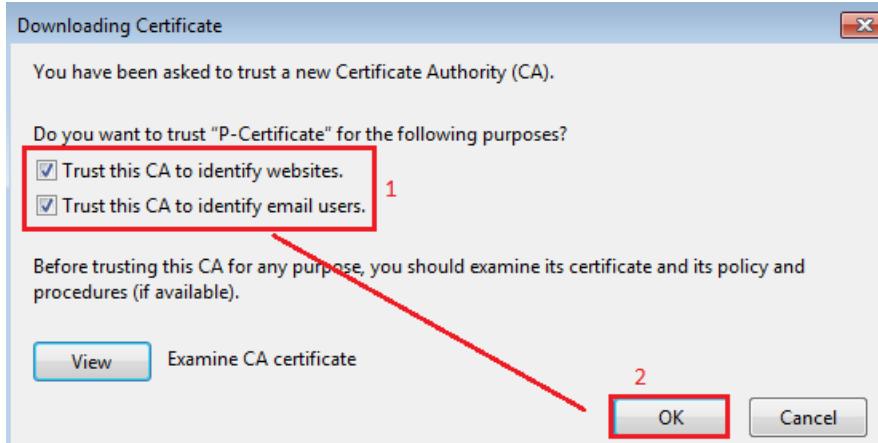
Under [Authorities > click Import And Go to Downloads folder and choose the created PEM certificate > click Open > click Trust the CA to identify websites > click OK](#)



Go to Downloads folder and choose the created PEM certificate > click Open > click Trust the CA to identify websites > click OK.

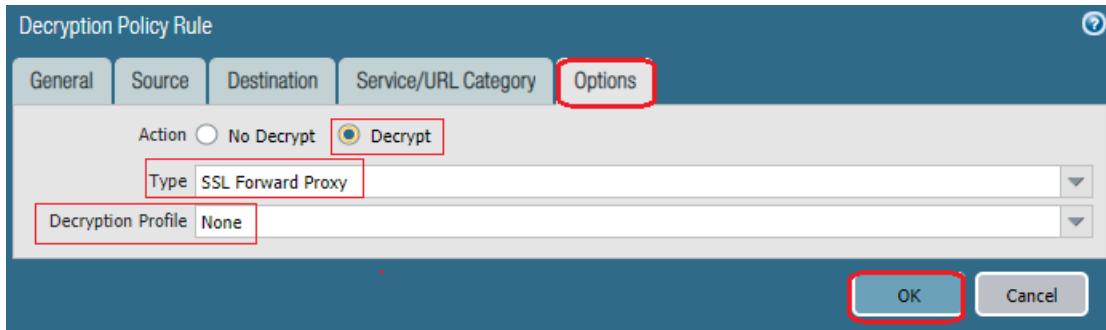


Check Trust this CA to identify websites & Trust this CA to identify email users and Click OK.



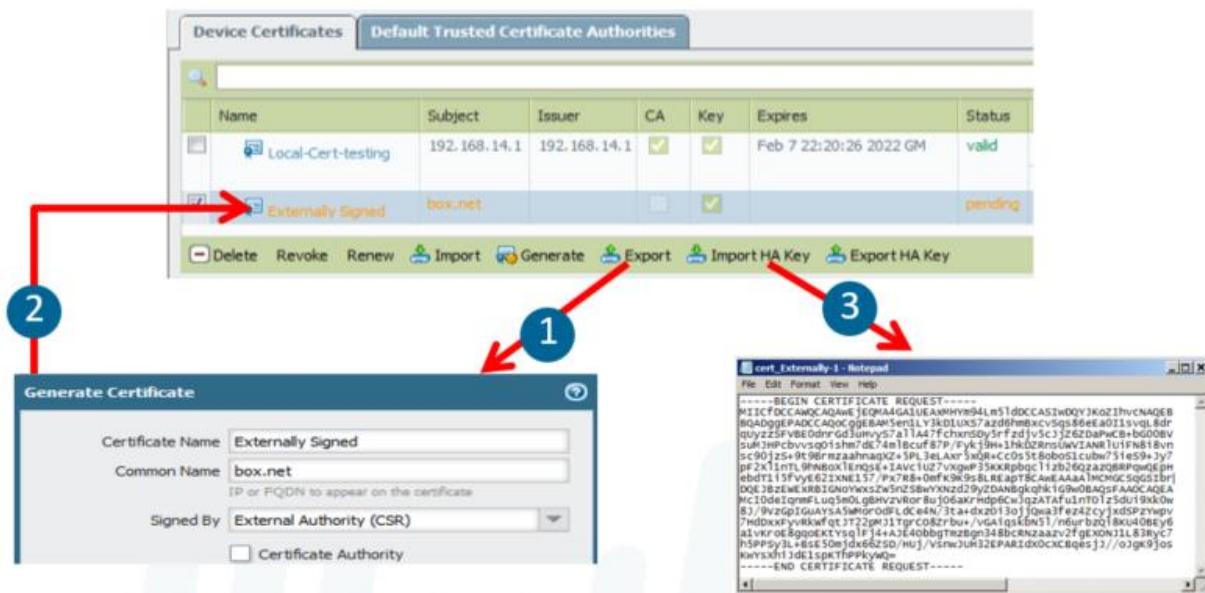
Configure a Decryption policy from left to right. Under General > type the Name of the Decryption rule. Under Source tab > choose Inside under Source Zone > leave the default of Any. Under Destination tab > choose Outside under Destination Zone > leave Any under Destination Address > leave the default of Any.

Under Options tab > select Decrypt under Action > leave the default of SSL Forward Proxy under Type and None under Decryption Profile > click OK.



		Source	Destination			Decrypt Options	
	Name	Zone	Zone	URL Category	Service	Action	Type
1	Decryption-Policy	Inside	Outside	any	any	decrypt	ssl-forward-proxy

Certificate Signing Requests:



The Generate button generates certificate signing requests (CSRs) if the Signed By field is set to External Authority (CSR).

1. A key pair is created on the machine and exported in PKCS10 format.
 2. The administrator then sends the CSR to the CA, which generates the requested certificate.
 3. When the resulting certificate is received from the CA, import it with the same name as the CSR.
 4. When the issued certificate is imported, the certificate signing request is removed and the certificate is added to the private key.

Certificate Revocation:

If both OCSP and CRL are configured, the firewall tries the OCSP method first. If the OCSP server is unavailable, the device uses the CRL method.

To enable CRL or OCSP, go to Device > Setup > Session, and in the Decryption Settings section, open Certificate Revocation Checking.

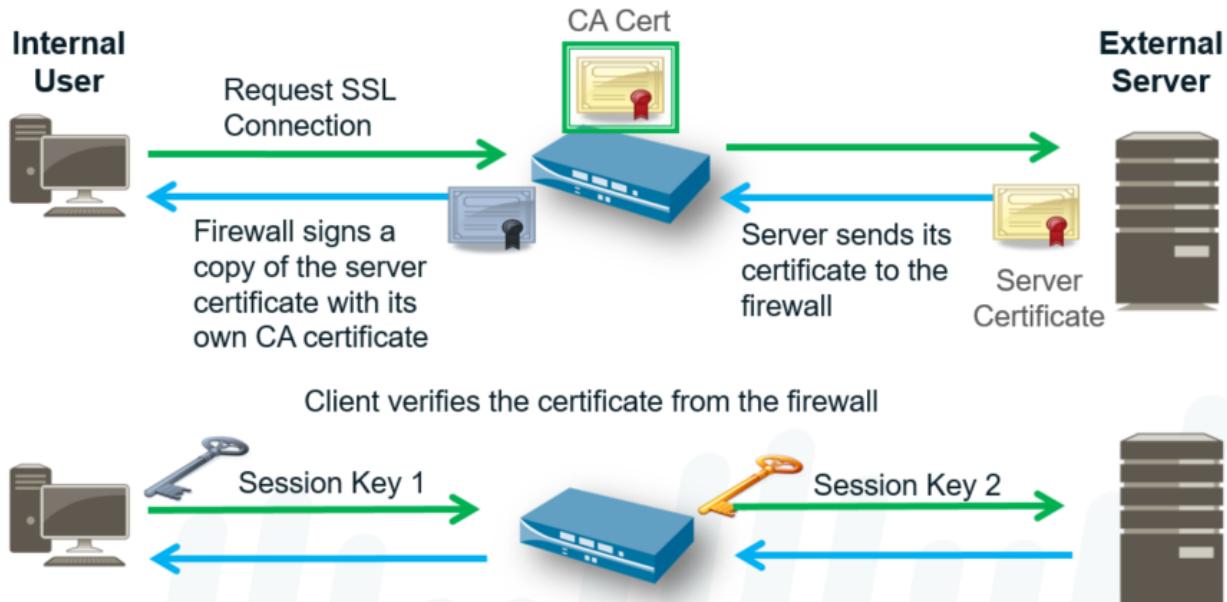
- Palo Alto Networks firewall devices can be configured to check whether a certificate has been revoked by the CA
 - CRL or OCSP can be used to verify certificate status for
 - SSL/TLS Decryption
 - GlobalProtect, captive portal, IPsec VPNs, and MGT access
- Certificate Revocation List (CRL)
 - Each CA issues a CRL listing to a public repository
 - Revoked certificates listed by serial number
 - Palo Alto Networks firewall downloads the CRL for every trusted CA
- Online Certificate Status Protocol (OCSP)
 - Clients send the certificate serial number to OCSP server to check status
 - Palo Alto Networks firewall caches OCSP info for every listed CA

Outbound SSL Decryption:

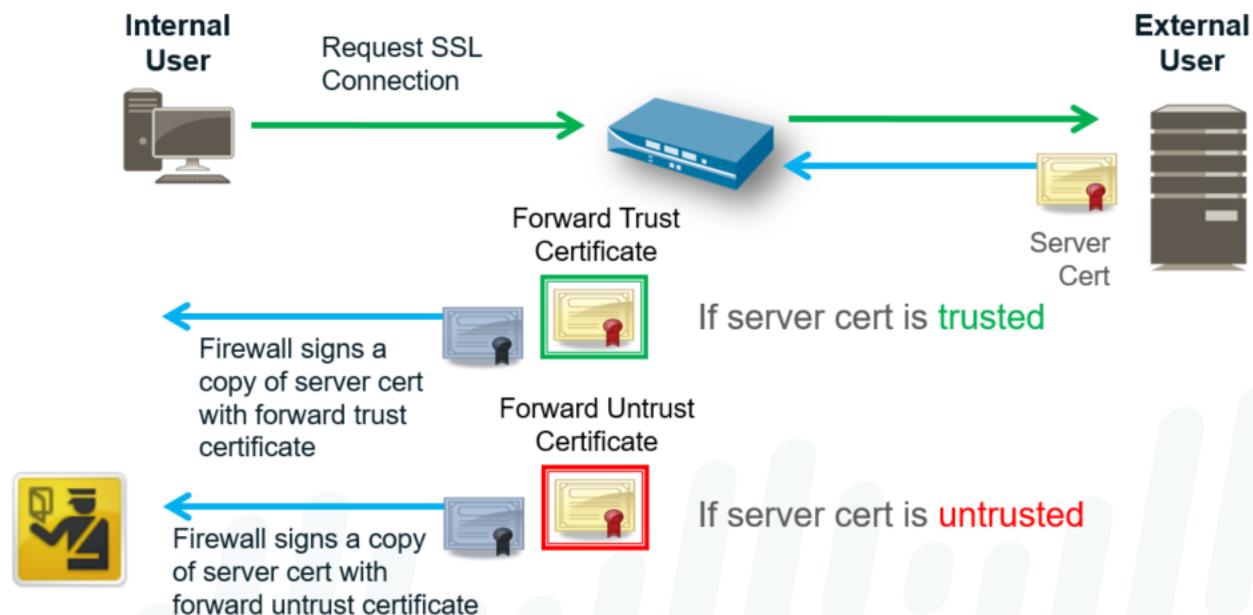
Outbound SSL Inspection by a Forward Proxy:

Use an SSL Forward Proxy decryption policy to decrypt & inspect SSL/TLS traffic. SSL Forward Proxy Decryption Policy inspect SSL traffic from internal users to the web. It prevents malware concealed as SSL encrypted traffic from being introduced to network. SSL Forward Proxy decryption, Firewall resides between internal client & outside server. Firewall uses Forward Trust certificates to establish itself as trusted third party to session. Firewalls provide capability to decrypt & inspect traffic for visibility, control & security. Decryption of outbound SSL traffic is implemented & takes form of SSL Forward Proxy. SSL Forward Proxy, which features the firewall as an intermediate communication node. SSL Forward Proxy decryption deployment commonly referred to as Man in the Middle. It replaces original certificate from a final destination with resigned by a different key. The PAN Firewall can acts as proxy between a client and an HTTPS website or Internet. PAN Firewall decrypt inbound/outbound SSL traffic in order to apply inspection policies. To configure Outbound SSL Decryption, generate self-signed

certificate from Firewall. PA device is configured to decrypt SSL traffic going to external sites as forward proxy.



Forward Trust and Forward Untrust Certificates:



With SSL forward proxy decryption, the firewall resides between the internal client and outside server. The firewall uses forward trust or forward untrust certificates to establish itself as a trusted third party to the session between the client and the server.

When the client initiates an SSL session with the server, the firewall intercepts the server SSL request and forwards the SSL request to the server. The server sends a certificate intended for the client that is intercepted by the firewall.

If the server certificate is signed by a CA that the firewall trusts, the firewall creates a copy of the server certificate signed by the forward trust certificate and sends the certificate to the client to authenticate. (The issuing authority of the firewall-generated certificate is the firewall itself. If the firewall certificate is not part of an existing hierarchy, or is not added to the browser cache of the client, the client receives a warning message when browsing to the site, even if the site is a secure site.)

If the server certificate is signed by a CA that the firewall does not trust, the firewall creates a copy of the server certificate and signs it with the forward untrust certificate and sends it to the client. In this case, the client sees a block page warning that the site they are attempting to connect to is not trusted and the client can choose to proceed or terminate the session. When the client authenticates the certificate, the SSL session is established with the firewall functioning as a trusted forward proxy to the site that the client is accessing.

Configuring SSL Forward Proxy Decryption:

- **Configure a Forward Trust Certificate**
 - Use a self-signed certificate
 - Or use a certificate signed by an internal CA
- **Configure a Forward Untrust Certificate**
 - Use a self-signed certificate
- **Create a Decryption Policy**
 - Choose the URL categories to decrypt
 - Optional decryption profile

Configure a Forward Trust Certificate:

- **The forward trust certificate is a CA cert that signs the server cert sent to the client**
- **The client browser should trust this CA so that no warning message appears**

[Go to in Device > Certificate Management > Certificates](#)

Generate Certificate

Certificate Name	FwdTrstCert
Common Name	192.168.11.1 IP or FQDN to appear on the certificate
Signed By	
<input checked="" type="checkbox"/> Certificate Authority	
OCSP Responder	
Cryptographic Settings	
Number of Bits	2048
Digest	sha256
Expiration (days)	365
Certificate Attributes	
Type	Value
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

Certificate information

Name	FwdTrstCert
Subject	/CN=192.168.11.1
Issuer	/CN=192.168.11.1
Not Valid Before	Dec 8 22:54:55 2014 GMT
Not Valid After	Dec 8 22:54:55 2015 GMT
<input checked="" type="checkbox"/> Certificate Authority <input checked="" type="checkbox"/> Forward Trust Certificate <input type="checkbox"/> Forward Untrust Certificate <input type="checkbox"/> SSL Exclude Certificate <input type="checkbox"/> Trusted Root CA <input type="checkbox"/> Certificate for Secure Web GUI	

Configure a Forward Untrust Certificate:

- The client browser should NOT trust this CA so that a warning message DOES appear

Certificate information

Name	FwdUntrstCert
Subject	/O=NotTrusted/CN=192.168.11.1
Issuer	/O=NotTrusted/CN=192.168.11.1
Not Valid Before	Dec 8 23:00:06 2014 GMT
Not Valid After	Dec 8 23:00:06 2015 GMT
<input checked="" type="checkbox"/> Certificate Authority <input type="checkbox"/> Forward Trust Certificate <input checked="" type="checkbox"/> Forward Untrust Certificate <input type="checkbox"/> SSL Exclude Certificate <input type="checkbox"/> Trusted Root CA <input type="checkbox"/> Certificate for Secure Web GUI	

Device > Certificate Management > Certificates

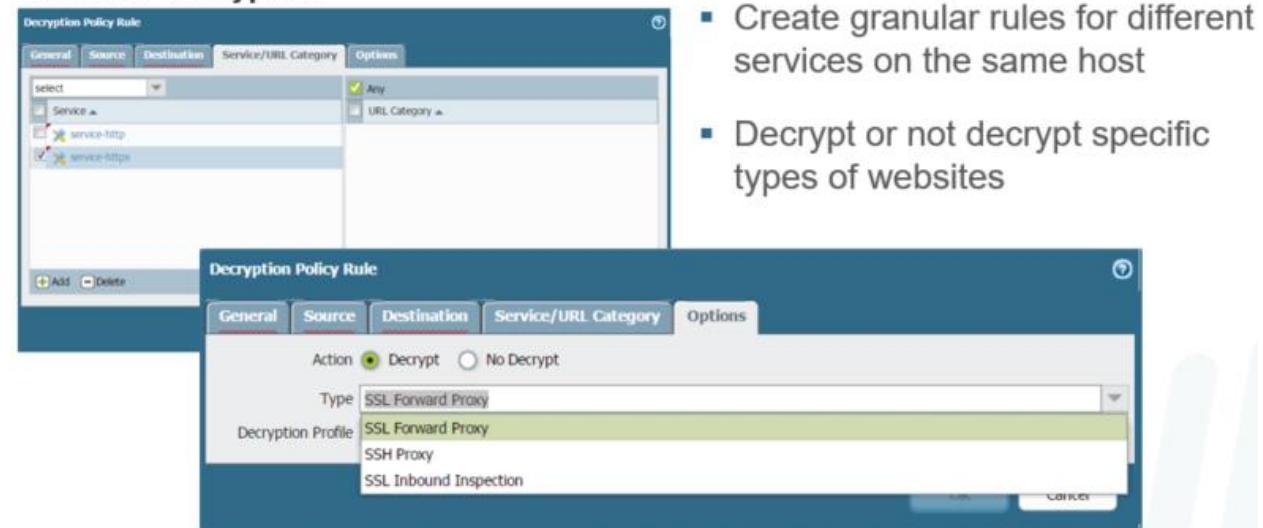
Generate Certificate

Certificate Name	FwdUntrstCert
Common Name	192.168.11.1 IP or FQDN to appear on the certificate
Signed By	
<input checked="" type="checkbox"/> Certificate Authority	
OCSP Responder	
Cryptographic Settings	
Number of Bits	2048
Digest	sha256
Expiration (days)	365
Certificate Attributes	
Type	Value
<input checked="" type="checkbox"/> Organization NotTrusted	
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

- The client browser should NOT trust this CA so that a warning message DOES appear

Create a Decryption Policy:

Policies > Decryption



- Create granular rules for different services on the same host
- Decrypt or not decrypt specific types of websites

SSL decryption policies are similar to the other rule sets in PAN-OS.

- The rules are parsed from top to bottom, comparing traffic to each rule in order.
- When the traffic matches a particular rule, the actions defined are taken and no further rules are checked.

The supported types of decryption policies are:

- SSL Forward Proxy: Decrypts client traffic destined for an external server.
- SSH Proxy: Decrypts SSHv2 traffic, which allows you to control SSHv2 tunneling in policies by specifying the SSH-tunnel App-ID.
- SSL Inbound Inspection: Decrypt SSLs inbound inspection traffic.

Decryption Policy by URL Category:

The SSL decryption policy uses URL filtering to decide which traffic to decrypt or not decrypt:

- User-ID or destination addresses can also be used for the decryption decision, but in practice, the decision is made on the URL Filtering category of the destination address.
- The destination IP address is compared since the URL is not visible.

Organizations may choose not to decrypt specific applications because they feel those destinations are trusted and pose less of a risk. Additionally, local laws and regulations may restrict whether specific types of traffic, such as financial or medical information, are allowed to be decrypted.

Of course, you need a URL Filtering license to use URL Filtering categories, although you could create and use custom categories.

For example, a rule might allow SSL traffic to sites in the finance, health, or shopping URL categories to pass through the device without being decrypted. All other SSL traffic is intercepted and the forward proxy decrypts the connection for inspection.

Policies > Decryption

Name	Tags	Source			Destination			URL Category	Service	Action	Type	Decryption Profile
		Zone	Address	User	Zone	Address						
1 no-decrypt-traffic	none	Trust-L3	any	any	Untrust-L3	any	Finance, services, health-and-medical, shopping	any	no-decrypt	ssl-forward-proxy	none	
2 decrypt-all-traffic	none	Trust-L3	any	any	Untrust-L3	any	any	any	decrypt	ssl-forward-proxy	none	

Subject field of server certificate contains URL category

Decryption in the Traffic Log:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	By	Decrypted
06/22 11:19:03	end	Trust-L3	Untrust-L3	192.168.11.53	pan-training\dagent	10.30.11.69	139	incomplete	allow	General Internet	aged-out		
06/22 11:18:59	end	Trust-L3	Untrust-L3	192.168.11.51	pan-training\dagent	10.30.11.69	139	incomplete	allow	General Internet	unknown	132	no
06/22 11:18:04	deny	Trust-L3							deny	Intrazone-dst-all	policy-deny	82	no
06/22 11:18:02	end	Trust-L3							allow	General Internet	aged-out	569.4k	yes
06/22 11:18:02	end	Trust-L3							allow	General Internet	aged-out	22.4k	yes
06/22 11:18:02	end	Trust-L3							allow	General Internet	aged-out	6.3k	yes
06/22 11:17:59	end	Trust-L3							allow	General Internet	aged-out	82	no
06/22 11:17:59	end	Trust-L3							allow	General Internet	aged-out	132	no
06/22 11:17:59	end	Trust-L3							allow	General Internet	aged-out	7.5k	yes
06/22 11:17:42	end	Trust-L3							deny	Intrazone-dst-all	policy-deny	82	no
06/22 11:16:57	deny	Trust-L3							allow	General Internet	aged-out	82	no
06/22 11:16:50	end	Trust-L3							allow	General Internet	aged-out	132	no
06/22 11:16:49	end	Trust-L3							allow	General Internet	top-fin	12.2k	no
06/22 11:16:42	end	Trust-L3							allow	General Internet	top-fin	49.2k	no
06/22 11:16:42	end	Trust-L3							allow	General Internet	top-fin	122.1k	no
06/22 11:16:42	end	Trust-L3							allow	General Internet	top-fin	29.0k	no
06/22 11:16:42	end	Trust-L3							allow	General Internet	aged-out	7.3k	yes
06/22 11:16:42	end	Trust-L3							allow	General Internet	aged-out	6.3k	yes
06/22 11:16:42	end	Trust-L3							allow	General Internet	top-fin	18.2k	no
06/22 11:16:42	end	Trust-L3							allow	General Internet	top-fin	5.5k	no

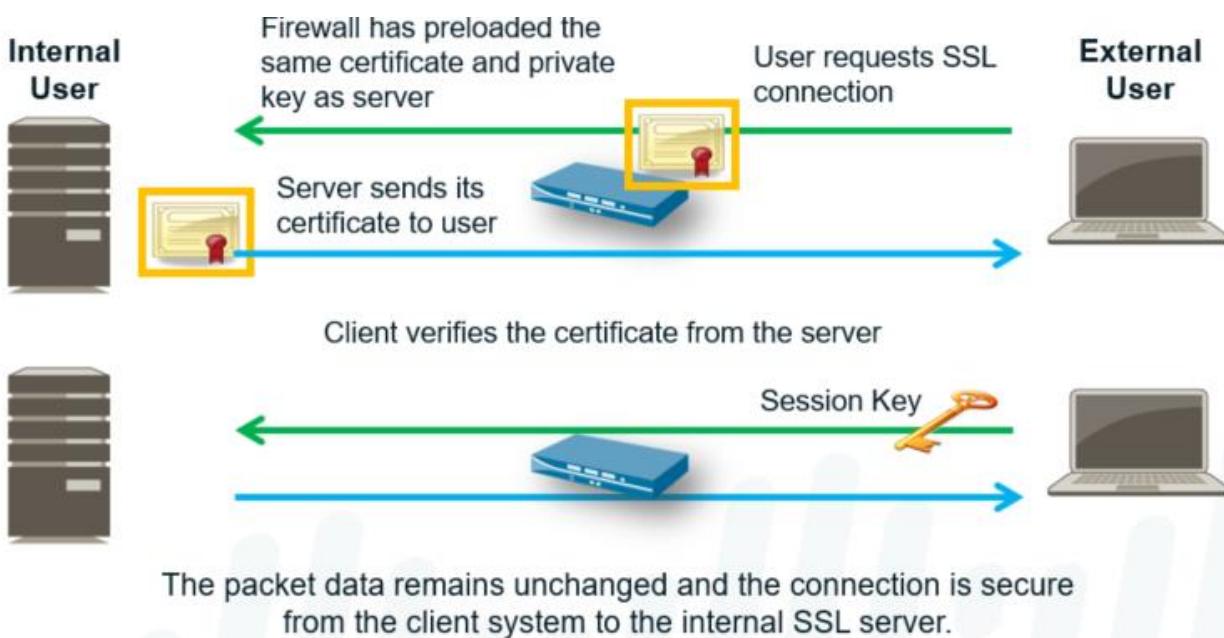
Recommended Ruleset:

- Decrypt everything except sensitive traffic
 - Apply SSL controls to undecrypted traffic via profile
- Create exception rules for specific destination IP, source users, URLs

	Name	Source			Destination					Type	Decryption Profile
	Name	Zone	Address	User	Zone	Address	URL Category	Service	Action		
1	Destination IP Exception Bypass	[p] users	any	any	[p] internet	1.1.1.1	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile
2	Source User Exception Bypass	[p] users	any	paloaltonetwork\mjon...	[p] internet	any	any	any	no-decrypt	ssl-forward-proxy	Lenient Profile
3	URL Exception Bypass	[p] users	any	any	[p] internet	any	Decrypt Bypass	any	no-decrypt	ssl-forward-proxy	Lenient Profile
4	Sensitive Category Bypass	[p] users	any	any	[p] internet	any	financial-services government health-and-medicine military shopping	any	no-decrypt	ssl-forward-proxy	Tight SSL Control
5	Decrypt All Else	[p] users	any	any	[p] internet	any	any	any	decrypt	ssl-forward-proxy	Tight SSL Control

!

Inbound SSL Inspection:



The Palo Alto Networks firewall can inspect inbound SSL traffic for potential external threats and control applications that run over secure channels. This activity is accomplished via application firewall rules, as well as the server vulnerability protection profiles.

To inspect the traffic going to internal SSL servers, the firewall needs a copy of the certificate and key of the internal server. The SSL decryption policy must be configured on the firewall to inspect the inbound traffic. After this configuration is complete, the device can decrypt and read the traffic before it forwards the traffic to the server. The original encrypted data packet is sent to the server and no changes are made to the data. The secure channel is built from the client system to the internal SSL server.

Configure SSL Inbound Inspection:

- Import the internal server certificate on the Palo Alto Networks firewall

Device > Certificate Management > Certificates > Device Certificates

1. Create a decryption policy

- **Destination address:** Server address
- **Type:** SSL inbound Inspection
- **Certificate:** Server Cert

Policies > Decryption

Decryption Policy Rule

General	Source	Destination	Service/URL Category	Options
Action	<input checked="" type="radio"/> Decrypt	<input type="radio"/> No Decrypt		
Type	SSL Inbound Inspection			
Certificate	Server Cert			
Decryption Profile	None			

Other SSL Decryption:

Various applications and clients use SSL encryption. When Web servers communicate with Web browsers via HTTPS, the SSL connection highly conforms to the SSL RFCs.

Standardization is key to ensure that services are available to anyone on the Internet with a Web browser.

Some uses of SSL encryption may deviate enough from the SSL standard or typically available options such that they no longer work when decrypted with a Palo Alto Networks firewall.

Examples:

- Proprietary or nonstandard encryption methods
- Evasive applications
- Client software coded to accept traffic from specific certificates

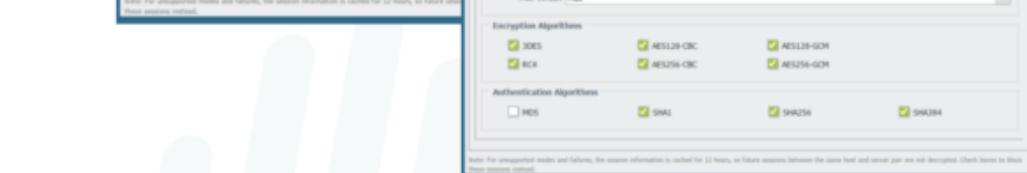
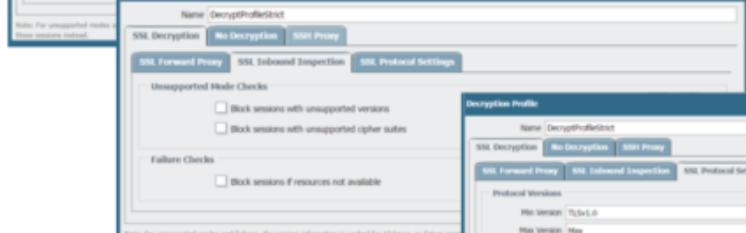
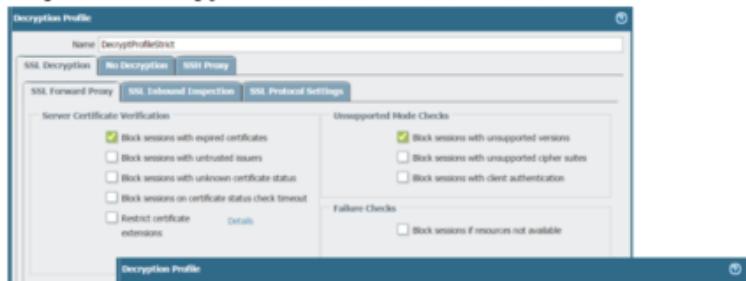
You can also use the decryption profile to:

- Enforce the use of strong cipher suites for decrypted traffic, which includes support to specifically enforce the use of the Suite B Ciphers aes-128-gcm and aes-256-gcm.
- Enforce the use of minimum and maximum protocol versions.
- Enforce certificate validation on a per-policy basis.

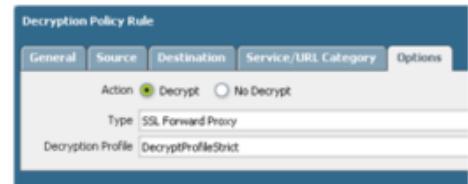
- Define different traffic that you want to be decrypted using TCP port numbers, which enables you to apply different decryption policies to the traffic of a single server.
- Traffic being transmitted using different protocols can receive treatment.

The decryption profiles can be applied to decryption policies to block any sessions that the firewall cannot decrypt. Decryption may fail if none of the cryptographic algorithms offered by the client and server are supported. Profiles allow you to treat specific decryption failures differently, based upon your organization's requirements.

Objects > Decryption Profile



Policies > Decryption



No Decryption:

Even if the decryption policy action is No Decrypt, the profile can be configured to block sessions with certificates that are expired or untrusted.

Select No Decryption to block and control specific aspects of traffic that you are excluding from decryption. Normally, 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 these boxes to block those sessions instead.

You can use the No Decryption tab to block traffic that is matched to a decryption policy configured with the No Decrypt action (Policies > Decryption > Action). Use these options to control server certificates for the session, even though the firewall does not decrypt and inspect the session traffic.

Block sessions with expired certificates: Terminate the SSL connection if the server certificate is expired. This action prevents a user from being able to accept an expired certificate and continuing with an SSL session. A traffic log entry is generated.

Block sessions with untrusted issuers: Terminate the SSL session if the server certificate issuer is untrusted.

Decryption Profile

Name: No Decryption Block Expired Certs

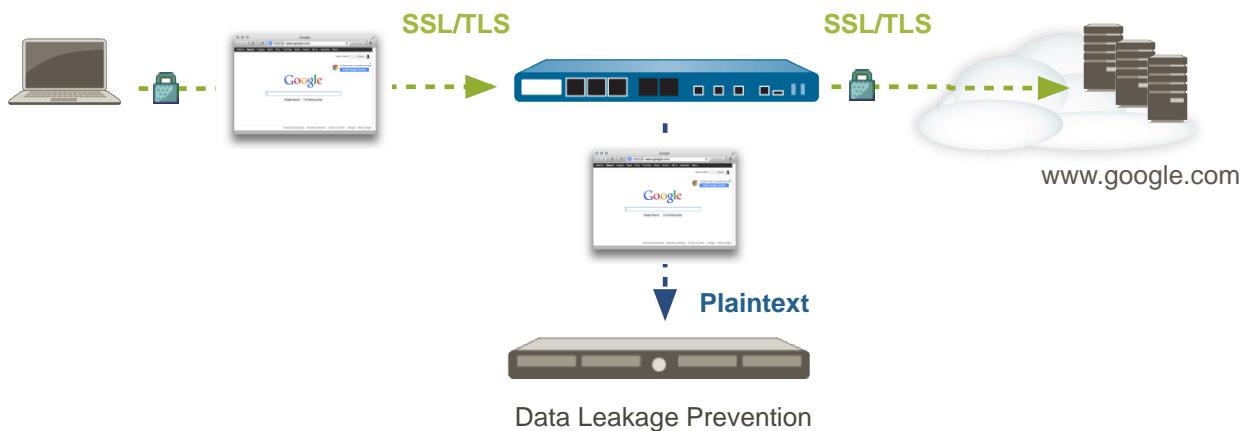
SSL Decryption **No Decryption** **SSH Proxy**

Server Certificate Verification

Block sessions with expired certificates
 Block sessions with untrusted issuers

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.

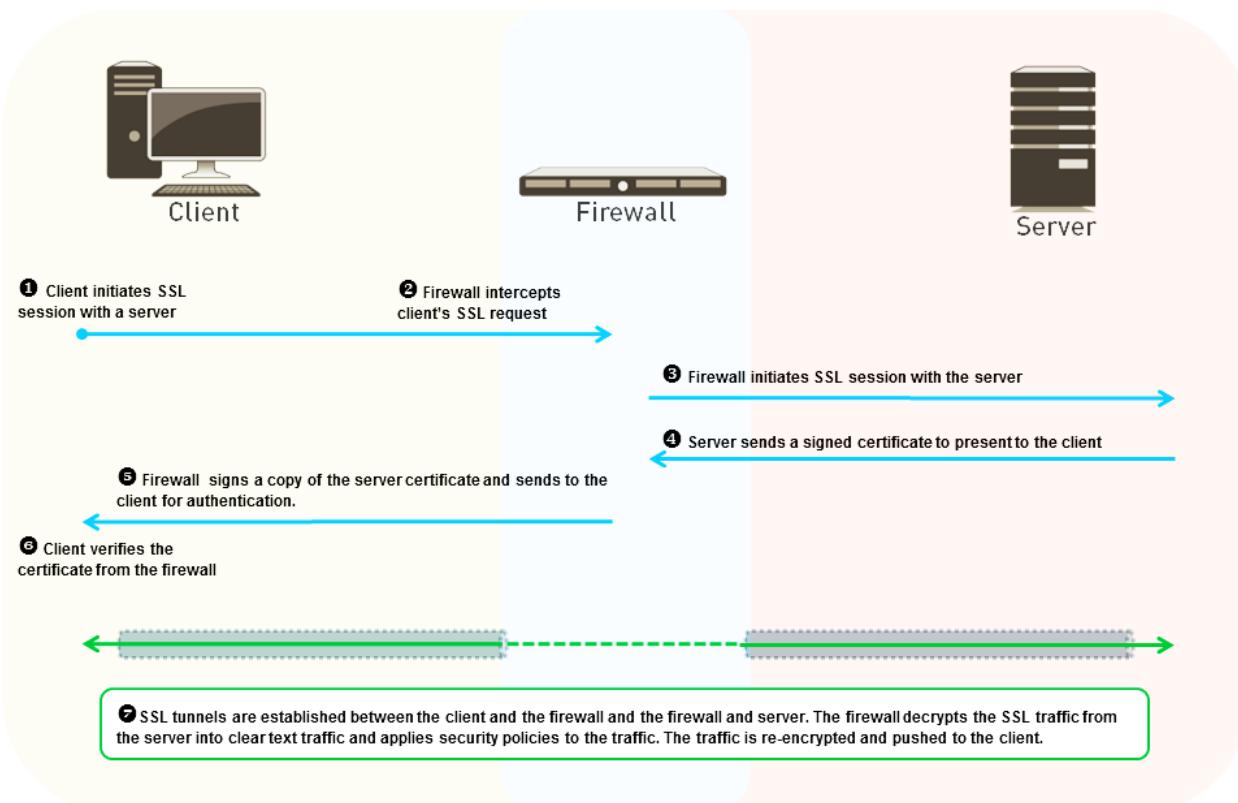
Decryption Port Mirroring:



- Export decrypted flows out of a dedicated interface on the firewall
- Used for: data leak prevention (DLP), network forensics

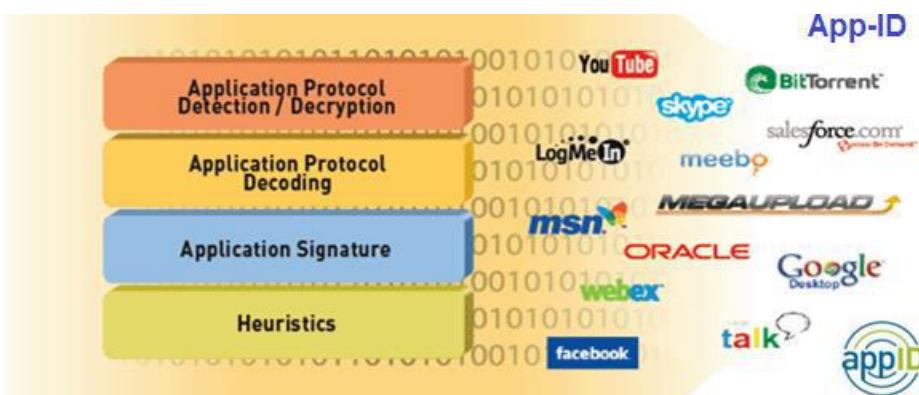
- The Decryption Port Mirror feature provides the ability to create a copy of decrypted traffic from a firewall and send it to a traffic collection tool that is capable of receiving raw packet captures, such as NetWitness or Solera, for archiving and analysis.
- This feature is necessary for organizations that require comprehensive data capture for forensic and historical purposes or data leak prevention (DLP) functionality.
- Decryption port mirroring is available only on the PA-3200 Series, PA-5200 Series, and PA-7000 Series platforms and requires a free license to be installed to enable this feature. This free PAN-PA-DECRYPT license is a perpetual license with no expiration and can be requested from the Support portal.

SSL Decryption Operation:



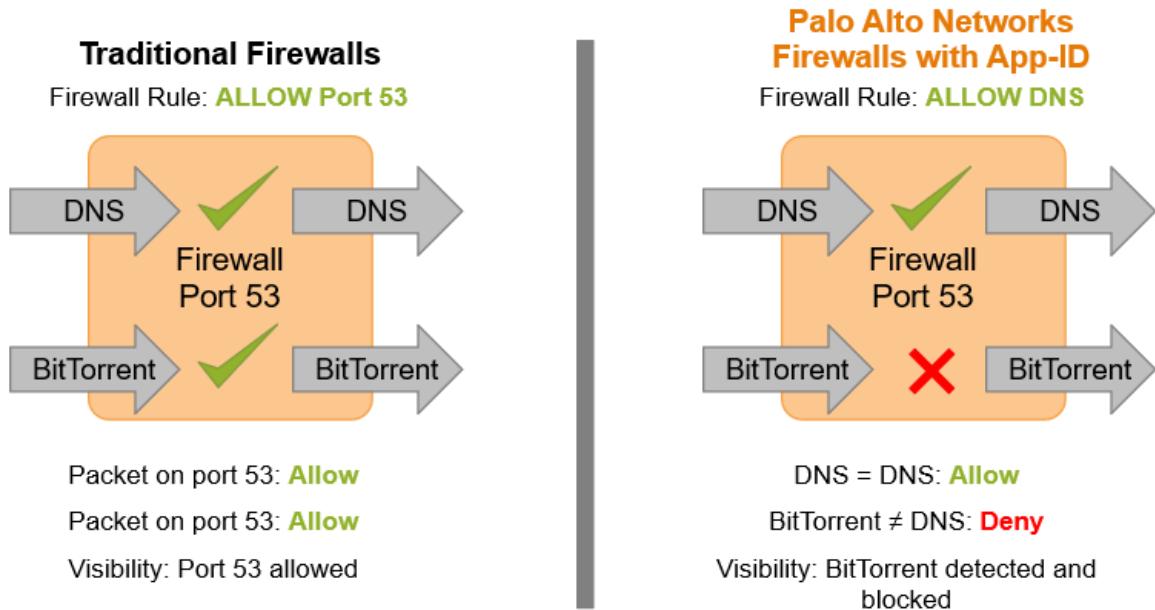
APP-ID

Application Identification or App-ID is a main component of Palo Alto devices. Traditional Firewalls classify traffic by port and protocol, PA Firewall use App-ID. Application is specific program who's communication can be labeled & monitored. Application is specific feature whose communication can be labeled and controlled. Port-based rules use Service, App-ID or Application-based rules use the application. Application rules allow only the application traffic that is allowed & no other traffic. Unknown traffic trying to pass application policy is blocked, because it doesn't match. Application Identity for UDP can generally identify the application on the first packet. App-ID for TCP take several packets to identify, as 3-way handshake needs to be done. Then the application data will need to be examined, depending on the application data. Application Database is updated weekly with new and updated application identifiers. App-ID identification of applications ensures the success of proper Layer 7 inspections. Application Signatures today over 4000, Application Protocol Decoders, and heuristics. These elements are responsible for visibility of L7 traffic traversing P Networks firewalls. Apps are categorized and classified by App-ID engine, allowing proper identification. During classification process, Palo Alto Networks defines main applications (Parent App). Some directly dependent (or Child App), which are part of these main applications. Link to verify Application Identity or inside firewall applipedia.paloaltonetworks.com.

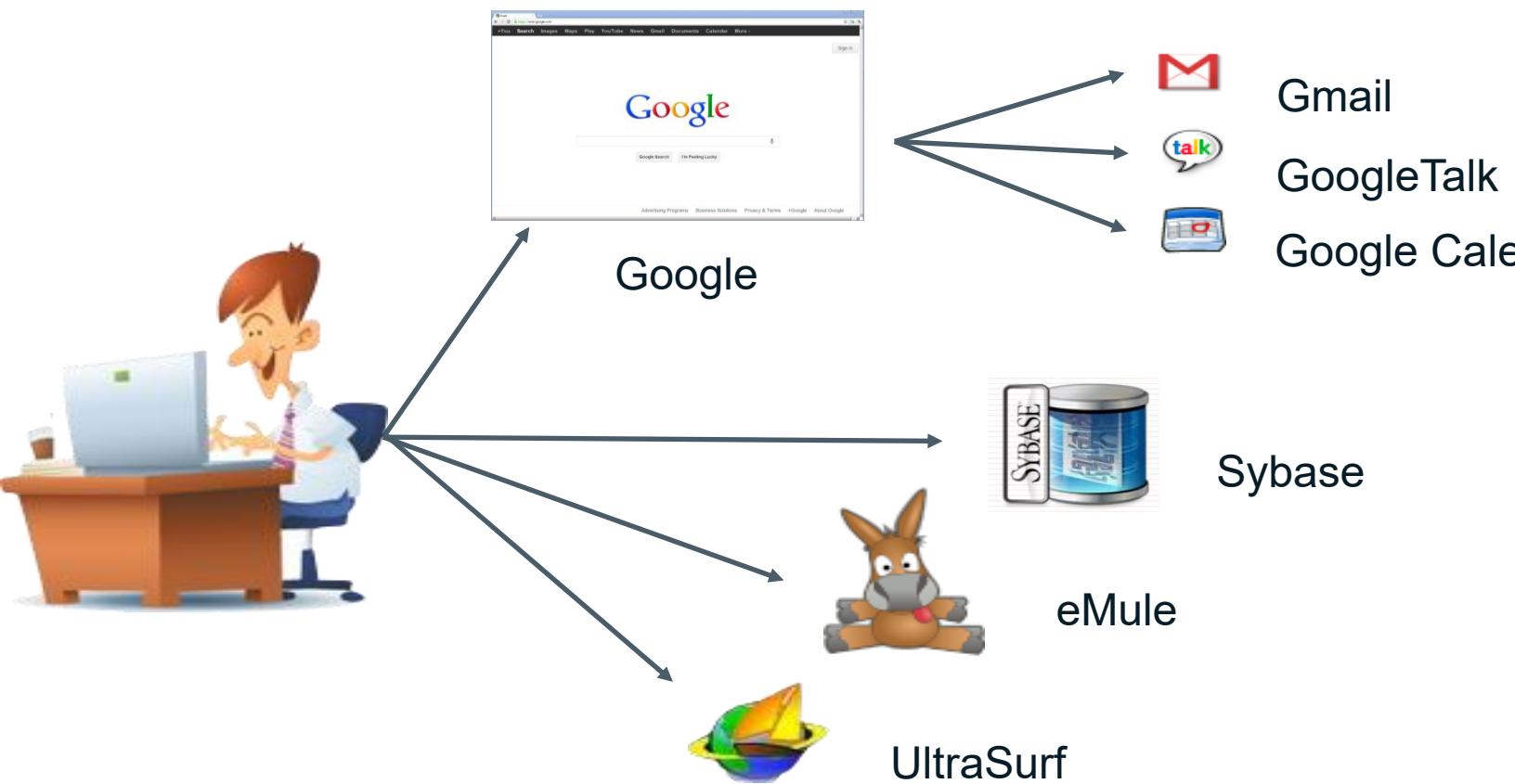


- Application identification is at the core of PAN-OS security, QoS, and PBF policies
 - Each session contains the information that is necessary to identify the applications traversing the firewall
 - Accurate traffic classification is the heart of any firewall, with the result becoming the basis of the security policy. Traditional firewalls classify traffic by port and protocol, which, at one point, was a satisfactory mechanism for securing the perimeter. Today, applications can easily bypass a port-based firewall by hopping ports, using SSL and SSH, sneaking across port 80, or using non-standard ports. App-ID is the Palo Alto Networks traffic classification mechanism that addresses the traffic classification limitations that plague traditional firewalls.

- App-ID uses multiple identification mechanisms to determine the exact identity of applications traversing the network. We discuss these methods in the following slides.



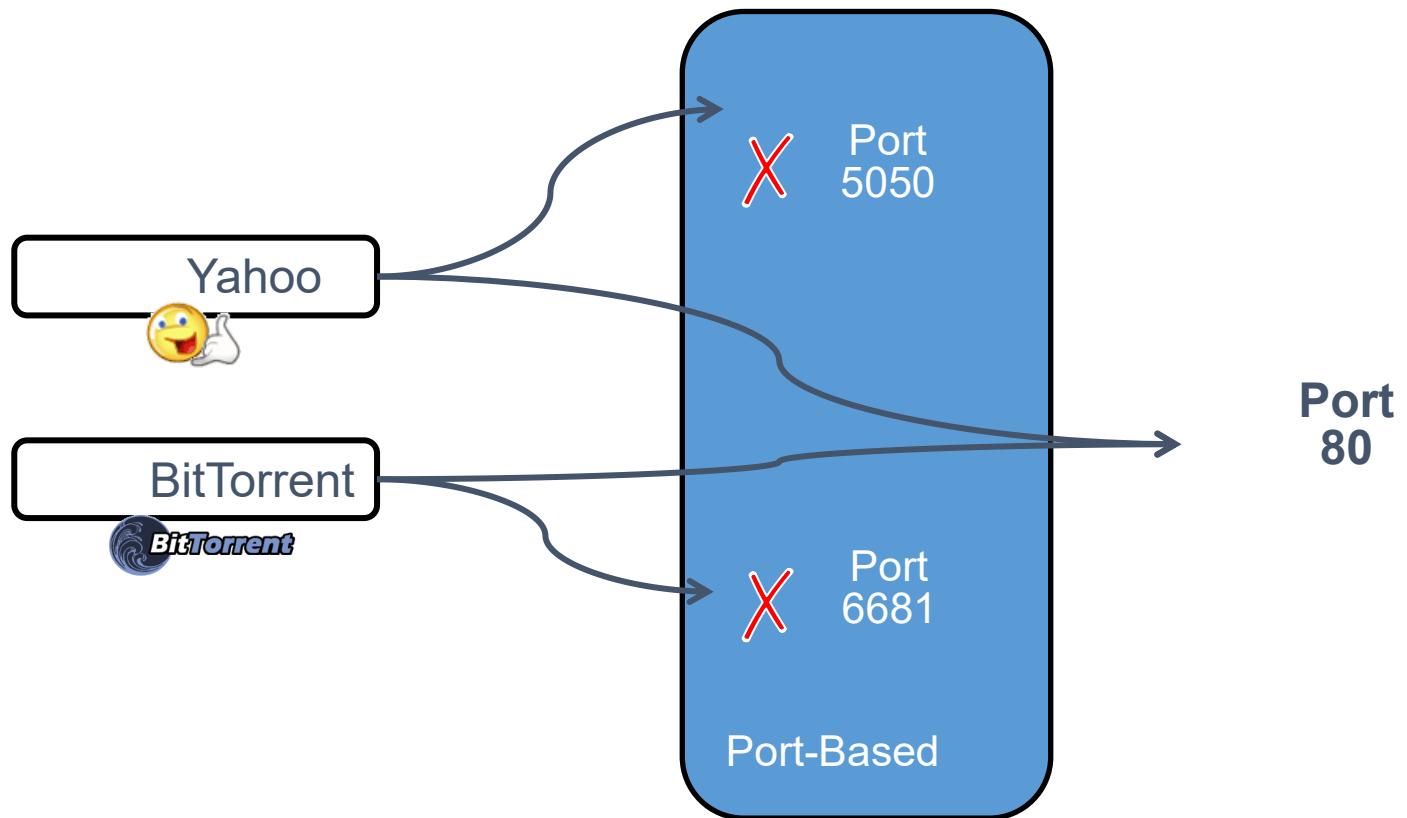
What is an Application?



The term “application” does not have an industry-accepted definition in the way that “session” or “packet” do. Applications can be delivered through a web browser, a client-server model, or a decentralized peer-to-peer design. In Palo Alto Network terms, an application is a specific program or feature that can be detected, monitored, and blocked if necessary.

Applications include business tools and services, which must be allowed, as well as entertainment or personal services, which may need to be blocked.

Evasive Applications:

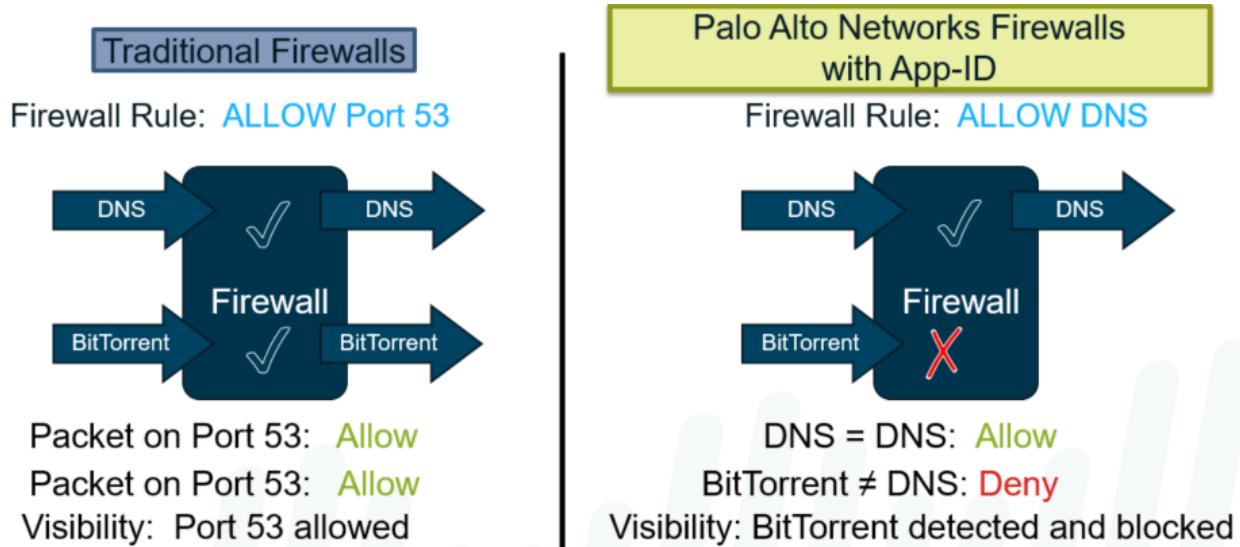


One category of applications that are difficult to track and control are those applications that change port numbers as needed. These applications are known as “evasive applications.” In a traditional, port-based firewall, Yahoo Messenger is defined as any TCP traffic destined for port 5050. In reality, Yahoo Messenger can automatically try other common ports, including port 80, if port 5050 is blocked.

Other applications can be configured by the user to be evasive by using a nonstandard port. The BitTorrent client traditionally uses a port number of 6681 or greater. It is a simple procedure to force BitTorrent to use a common port like 80 instead.

Many application proxies will take well-behaved, fixed-port applications and tunnel them through any port the user wants. The net result is that the destination port of any given connection has no bearing on the service or application that is generating the traffic.

Scenario 1: DNS Traffic – Traditional vs. Palo Alto Networks Firewall



Traditional firewalls use port blocking to control traffic. To allow a service, such as DNS, which uses port 53, the traditional firewall is configured to allow Port 53 traffic.

The Palo Alto Networks Next-Generation Firewall is configured to allow the DNS service. And when it is configured to run with the application default, the Palo Alto Networks firewall allows only DNS traffic on port 53 and denies all other traffic that is not DNS on this port. In this way, the Palo Alto Networks firewall protects the network from evasive applications.

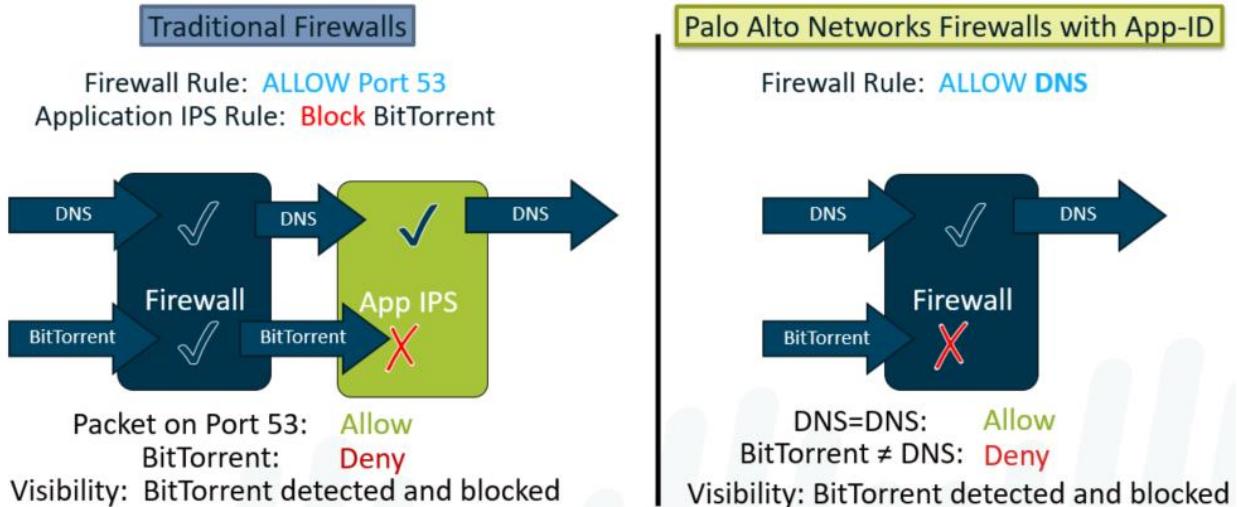
This protection does not happen on the network protected by the traditional firewall. On that network, DNS would be allowed on port 53, but so would other evasive applications attempting to use port 53, such as BitTorrent in this example here, thus exposing the traditional firewall's network and leaving it unprotected.

Scenario 2: BitTorrent – IPS vs. App-ID

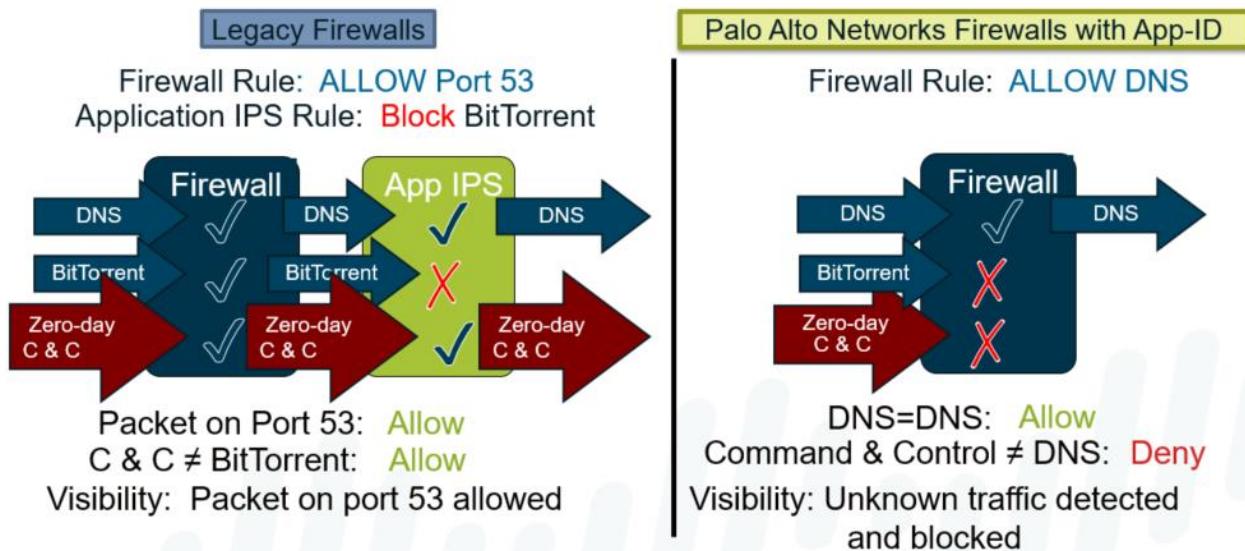
On traditional networks, an application Intrusion Protection System (IPS) can be added to the traditional firewall environment to provide a second layer of traffic filtering. After the traffic is processed by the traditional firewall, it is passed to the application IPS for further analysis. In this example, the BitTorrent traffic sent on port 53 traverses the firewall because it is using an allowed port, but is blocked by the application IPS.

Conversely, with the Palo Alto Networks firewall, which is configured to allow DNS only, the BitTorrent attempt is blocked regardless of the port number used. On a Palo Alto Networks

firewall, all traffic that is not specifically allowed is denied regardless of the port number used. This is the valued benefit of App-ID by Palo Alto Networks.



Scenario 3: Zero-Day Malware – IPS vs. App-ID



The previous two examples dealt with a well-behaved, known threat. The situation changes if the threat is unknown, like a zero-day virus.

In the application IPS blade example, the zero-day virus using Port 53 is allowed through the firewall because it is using an allowed port. However, since the IPS appliance does not know about this new threat, the malware is not blocked and is passed onto the network. This is an

inherent problem with application block policies – you cannot block what you do not know. Not only does the 0-day malware get through, but there are no logs generated that identify this problem.

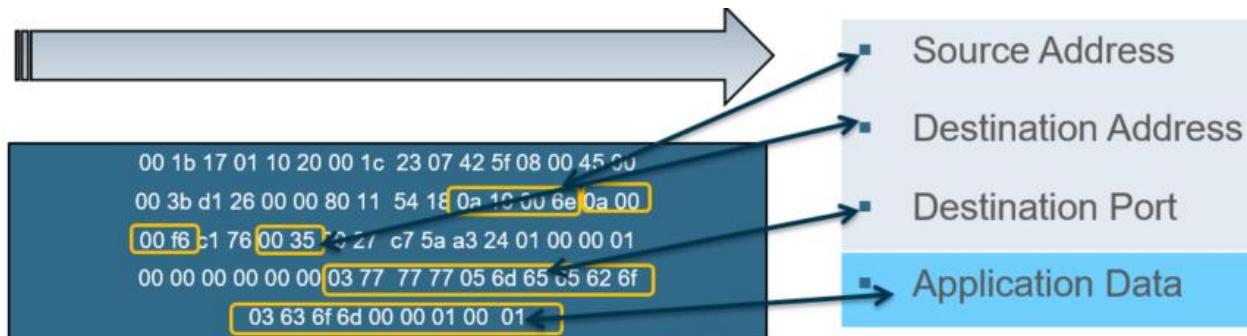
The Palo Alto Networks firewall is configured to allow only DNS traffic. Even if the zero-day malware is unknown to PAN-OS, it is not allowed to pass because it does not match the allowed DNS service. Additionally, the blocked traffic is logged for later analysis.

Examining UDP Packets:

When the Palo Alto Networks firewall examines UDP packets, it often only has to examine a single UDP packet to identify the application.

In most cases, all the information that the firewall needs is contained in a single packet.

This example shows a single packet DNS query for www.google.com. This packet contains all source and destination addressing information. It also includes the application data that will be used to identify the traffic so it can be processed by security policy.

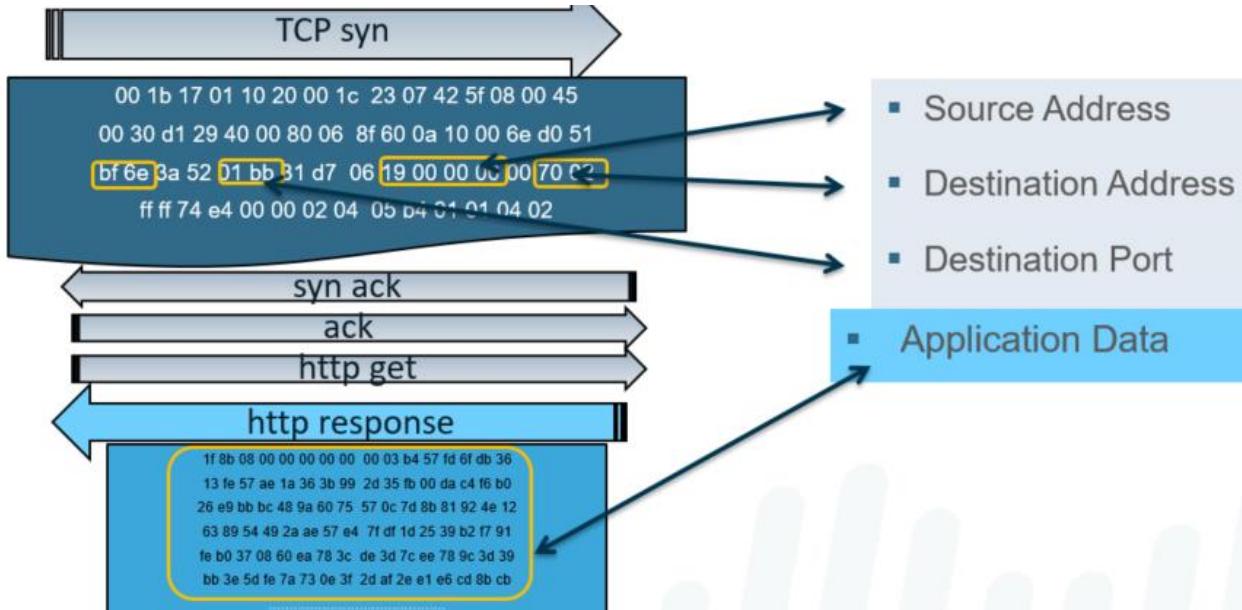


Examining TCP Packets:

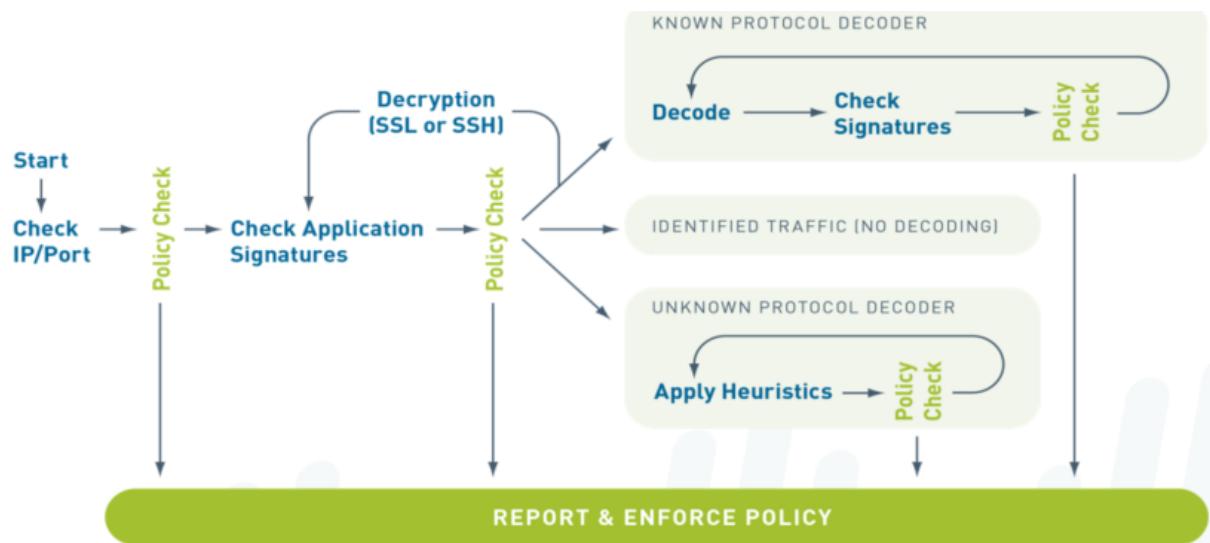
Applications that use TCP usually do not have all the required information in any single packet. This example shows a HTTP connection to www.sianets.com. The first packet is a TCP SYN packet. Though it does contain all the source and destination addresses, it contains no application data. In fact, the next two packets also do not contain any application data. They just complete the three-way handshake. The actual application data is either in the HTTP Get request or in the server reply.

Therefore, it is not until the firewall examines the fifth packet that it knows which application it's dealing with in regards to whether or not it is encrypted traffic, and if so, whether or not it should be decrypted, whether or not an “override policy” is applicable, or whether or not the

traffic should be considered part of a profile, and if so, what action should be taken based upon the policy it falls under.



App-ID Flow:



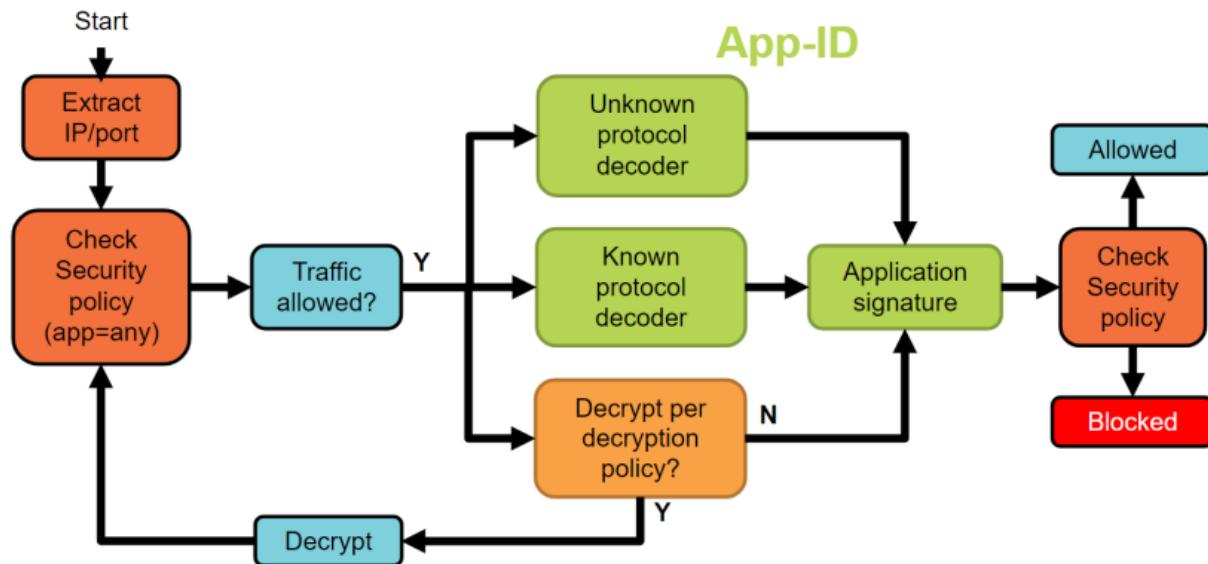
App-ID uses multiple identification mechanisms to determine the exact identity of applications traversing the network. The identification mechanisms are applied in this manner:

1. Traffic is first classified based on the IP address and port.

2. Signatures are then applied to the allowed traffic to identify the application based on unique application properties and related transaction characteristics.
3. If App-ID determines that encryption (SSL or SSH) is in use and a decryption policy is in place, the application is decrypted and application signatures are applied again on the decrypted flow.
4. Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics, or behavioral analysis may be used to determine the identity of the application.

After the application is identified, the policy check determines how to treat the application: block, allow and scan for threats/file transfers/data patters, or rate-limit them using QoS.

App-ID Operation



Identifying the Applications:

- The below App-ID (Application Identity) technologies are used during policy inspection.
- Uses multiple identification mechanism to determine the exact identity of applications.
- Accurate traffic classification, then it determine if it is going to allow or block the traffic.
-

App-ID Components:

The Palo Alto Networks solution utilizes four major technologies to identify applications:

- Protocol decoders
- Application signatures

- Protocol decryption
- Heuristics: When App-ID is unable to identify traffic by using application decoders and looking for signatures, the heuristics engine is used. This engine looks at patterns of communication and attempts to identify the application based on its network behavior. This type of detection is required for applications that use proprietary end-to-end encryption, such as Skype and encrypted BitTorrent.

Protocol Decoders
<ul style="list-style-type: none"> • Detect Protocol in Protocol within a session • Provide context for application signatures
Application Signatures
<ul style="list-style-type: none"> • Detect Layer 7 signatures within a session
Protocol Decryption
<ul style="list-style-type: none"> • SSL & SSH decryption
Heuristics
<ul style="list-style-type: none"> • Look for patterns of communication when no signature exists

Application Signature:

- Database of application signature updated weekly as part of firewall content updates.
- Application Signature can also be manually downloaded and installed in PA Firewall.

Unknown Protocol Decoder:

- An App-ID heuristic engine used to look up the pattern of the communication.
- It attempts to identify the application based on its network behavior.
- Example this type of detection required for proprietary end-to-end encryption like Skype.

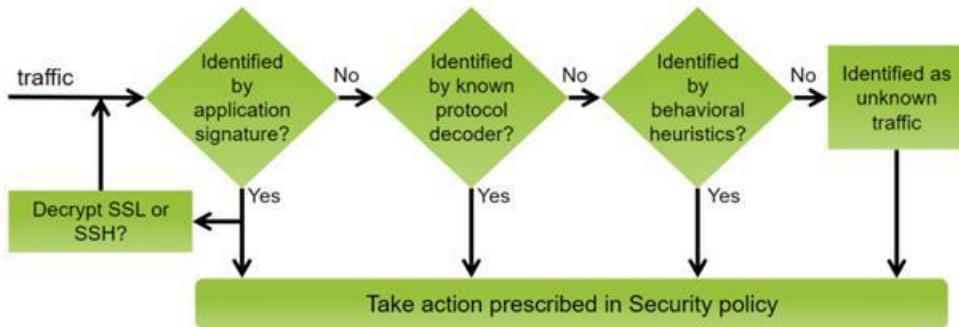
Known Protocol Decoder:

- Set of applications that coders understand syntax & commands of common applications.

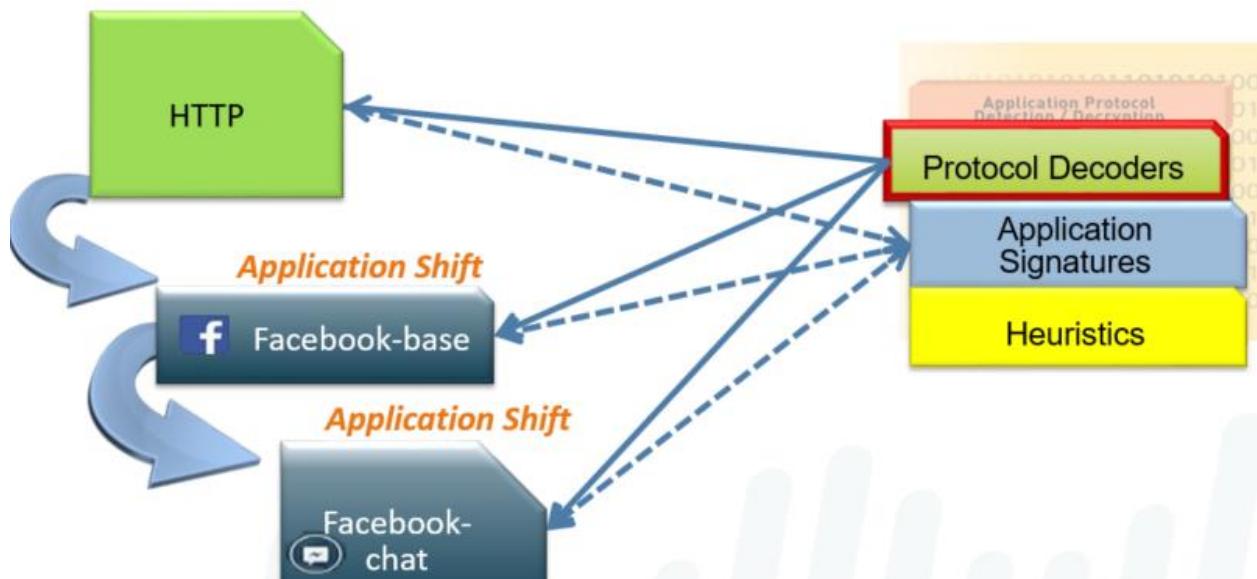
Protocol Decryption:

- Uses SSH (Secure Shell) and SSL (Secure Socket Layer) for encryption capabilities.

- App-ID™ identifies applications in traffic observed by the firewall.



Protocol Decoders:



These software constructs understand the application at the protocol level and provide contexts for the application. For example, the HTTP decoder understands that there will be a method and a version for each HTTP request. The decoders assist in detecting when a second protocol is tunneled within an existing session. This is called “Protocol in Protocol.”

Application Signatures:

Palo Alto Networks maintains a database of known application signatures for use in the App-ID engine. Updates to the database are issued weekly.

You can view the application signatures in three ways:

- In the WebUI under Objects > Applications
- On the Web at <http://apps.paloaltonetworks.com/applipedia/>
- On an Apple iOS device with the Applipedia app

Each signature covers multiple versions of an application.

In the information about the application, you may see the application identified as a SaaS. SaaS is a service where the software and infrastructure is owned and managed by the application service provider but where the customer retains full control of the data, including who can create, access, share, and transfer the data.

Objects > Applications

The screenshot shows the Palo Alto Networks management interface. On the left, a sidebar lists various objects like Addresses, Applications, Services, and Security Profiles. The 'Applications' section is highlighted and expanded, showing categories such as business-systems, auth-service, database, email, encrypted-tunnel, file-sharing, gaming, general-business, and peer-to-peer. A specific application, 'bitbucket', is selected in the main list, which then displays its detailed properties on the right. The properties pane includes fields for Name (BitTorrent), Description (BitTorrent is a peer-to-peer file sharing (P2P) communications protocol.), Standard Ports (http/https, udp/dns), Depends on (web-browsing), and Implicitly Used (bitbucket). A red arrow points from the sidebar's Applications section towards the detailed view of the BitTorrent application.

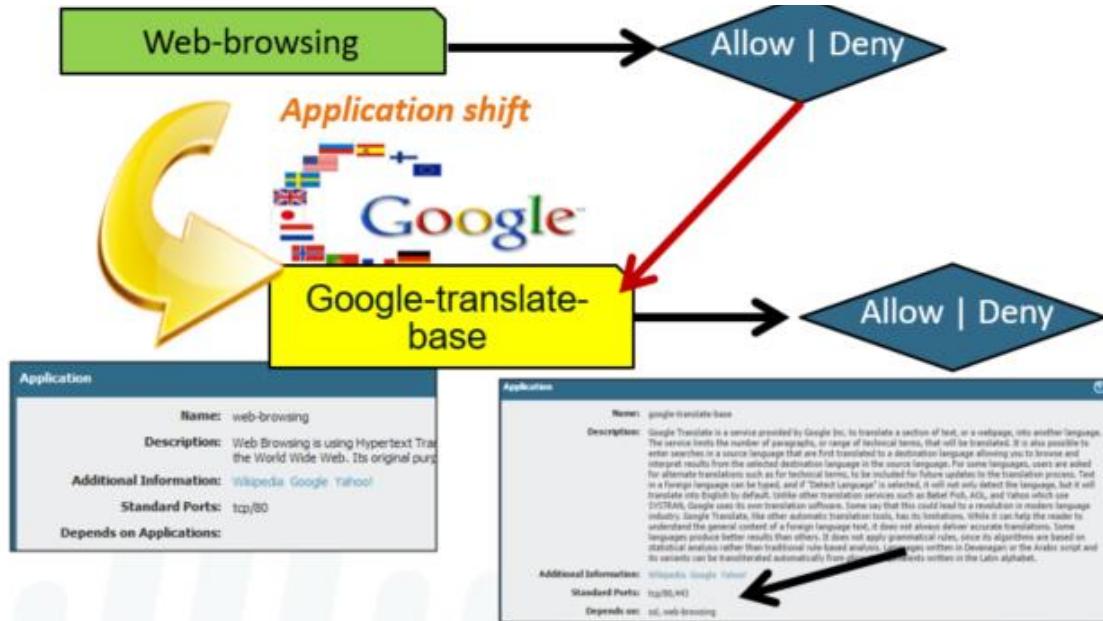
Application Dependencies:

Parent applications must also be allowed by security policy for the dependent applications to function.

When creating a policy to allow specific applications, you must also be sure that you are allowing any other applications on which the application depends. In many cases, you do not have to explicitly allow access to the dependent applications for the traffic to flow because the firewall is able to determine the dependencies and allow them implicitly. This implicit support also applies to custom applications that are based on HTTP, SSL, MS-RPC, or RTSP. Applications for which the firewall cannot determine dependent applications on time require that you explicitly allow the dependent applications when defining your policies. You can determine application dependencies in Applipedia.

In this example, a user wants to translate text using Google Translate. Before doing so, the user must first initiate an HTTP web-browsing session and so the security policy must account for this by enabling the web-browsing application in addition to allowing the google-translate-base application.

Application dependencies can be found by accessing App-ID in the WebUI. Select Objects > Applications to see application information. The App-ID listings are also available through Applipedia.



Applications with Implicitly Used Applications:

To use Facebook, the SSL and web-browsing applications are required. Therefore, the facebook-base application implicitly includes both of these applications, which means you do not need to take action to include either SSL or web-browsing when configuring your Facebook policy.

The screenshot shows the 'Objects > Applications' page in the Palo Alto Networks WebUI. A search bar at the top is set to 'facebook-base'. The left sidebar lists various object types, and the main pane displays a list of applications. A red circle highlights the search term 'facebook-base' in the search bar. A red box highlights the 'facebook-base' entry in the search results list. Another red box highlights the 'Implicitly Uses:' field in the detailed application view, which lists 'ssl, web-browsing'. The detailed view also shows the application's name, description, additional information, standard ports, and characteristics.

Characteristics		Classification	
Evasive: no	Category: collaboration	Excessive Bandwidth Use: no	Subcategory: social-networking
Used by Malware: yes	Technology: browser-based	Capable of File Transfer: yes	Risk: !! Customize...
Has Known Vulnerabilities: yes			
	collaboration	social-networking	browser-based
	collaboration	instant-messaging	browser-based
	general-internet	file-sharing	browser-based
	collaboration	email	browser-based
	collaboration	social-networking	browser-based
	collaboration	social-networking	browser-based

Applications that Depend on Applications:

Application dependencies: With the application Office-on-Demand, notice that four dependent applications must be allowed on the firewall to use Office-on-Demand. Therefore, you must account and allow for these dependent applications within your configurations.

The screenshot shows three windows from the Palo Alto Networks Firewall interface:

- Search Results:** Shows a search for "office-on-demand". A red circle highlights the search bar. Below it, a table lists applications, with one row for "ms-office365 (1 out of 1 chosen)" and another for "office-on-demand".
- Application Configuration:** A detailed view for "office-on-demand". It shows the name, description (Office-on-Demand allows subscribers of Microsoft Office 365 to stream Office (full versions of Word, Excel, PowerPoint, Access, and Publisher) to any Internet-connected Windows 7 or Windows 8 PC where it isn't installed. You can use Office on Demand to create documents or to keep working on documents you've saved to SkyDrive. Office on Demand: Google, Yahoo!), standard ports (tcp/80), and dependencies. A red box highlights the "Depends on" field, which lists "ms-office365-base, sharepoint-online, ssl, web-browsing".
- Job Status - Commit:** A window showing the commit status. It indicates "Operation Commit", "Status Completed", "Result Successful", and "Details Configuration committed successfully". A red box highlights the "Warnings" section, which lists several dependency warnings related to "ssl", "sharepoint-online", "ssl", and "web-browsing".

Implicit Applications:

- PAN-OS implicitly allows parent applications for a set of commonly used applications such as ssl and web-browsing.
- In this example, Facebook access will work even if the **Allow Web-browsing** policy rule were to be removed.

Name	Tags	Type	Source			Destination			Application	Service	URL Category	Action	Profile	Options
			Zone	Address	User	Zone	Addr...							
Allow Facebook	none	universal	Trust-L3	any	any	Untrust-L3	any		facebook-base facebook-chat facebook-mail	application-default	social-networking	Allow		
Allow web-browsing	none	universal	Trust-L3	any	any	Untrust-L3	any		web-browsing	application-default	any	Allow		

Requiring that dependencies be allowed in order to enable an application can often allow more traffic than intended. For example, enabling access to web-browsing just to allow facebook-base allows users to browse other sites, which means that the administrator must configure other policies to regulate this access. PAN-OS addresses this concern by implicitly allowing dependencies for a set of commonly used applications to streamline the security policy process. Implicit permissions of a parent application are only handled only if there is no match with an explicit rule.

When working with App-ID, it is important to understand that each App-ID signature may have dependencies that are needed to fully control an application. For example, with Facebook applications, the App-ID facebook-base is needed to access the Facebook website and to control other Facebook applications. Therefore, to configure the firewall to control Facebook

email, you must allow the App-IDs facebook-base and facebook-mail. To determine application dependencies for App-ID signatures, visit Applipedia, search for the given application, and then click the application for details.

Application Dependencies:

To successfully enable Office-on-Demand, the policy is configured to allow all of its dependent applications, services, and URL categories.

The screenshot shows two main parts. On the left is a table titled 'URL FILTERING' listing a policy named 'Allow Office-on-Demand'. The policy has 'any' for Source Address and User, and 'any' for Destination Zone. It includes services like ms-office365-base, office-on-demand, sql, and web-browsing. The 'Action' column shows 'Allow' with a green checkmark. A red arrow points from the 'Category' column of this row to the 'Category' field in the 'TEST A SITE' section on the right. On the right is a 'TEST A SITE' page where the URL 'https://login.microsoftonline.com' is entered, and the category 'Computer and Internet Info' is displayed.

Name	Tags	Type	Zone	Address	User	Zone	Addr...	Application	Service	URL Category	Action	Profile
Allow Office-on-Demand	none	universal	Trust-L3	any	any	Untrust-L3	any	ms-office365-base office-on-demand sql web-browsing	application-default	computer-and-in...	Allow	none

URL FILTERING

TEST A SITE

URL: https://login.microsoftonline.com

Category: Computer and Internet Info

Implicit Application Dependencies:

Application and Threat Research Center: <https://applipedia.paloaltonetworks.com/>

Allowed Application	Example Applications	Implicitly Allowed App Dependency
software-update apps business-systems apps web-mail apps, IMs, social-networking	erp-crm, storage-backup, sharepoint	web-browsing
Apps identified in rpc decoder	mount, nfs, portmapper, ibm-clearcase	rpc
Apps identified in msrpc decoder	ms-exchange, active-directory, arcserve msrpc ms-ds-smb	msrpc ms-ds-smb
Apps identified in rtsp decoder		rtsp
Apps identified in rtmp decoder	bbc-iplaye	rtmp, rtmpt
Media streaming apps	napster, megavideo	flash
Citrix ICA/Jedi	ms-rdp, msn-remote-desktop	t.120
IM apps	yahoo-voice, gtalk-voice, msn-voic, facetime gotomeeting, gotomypc, gotoassist	stun jabber
Apps identified based on SSL request and response SSH can remain in uses-apps and implicit-uses-apps		ssl

Using Port Numbers in Security Policies:

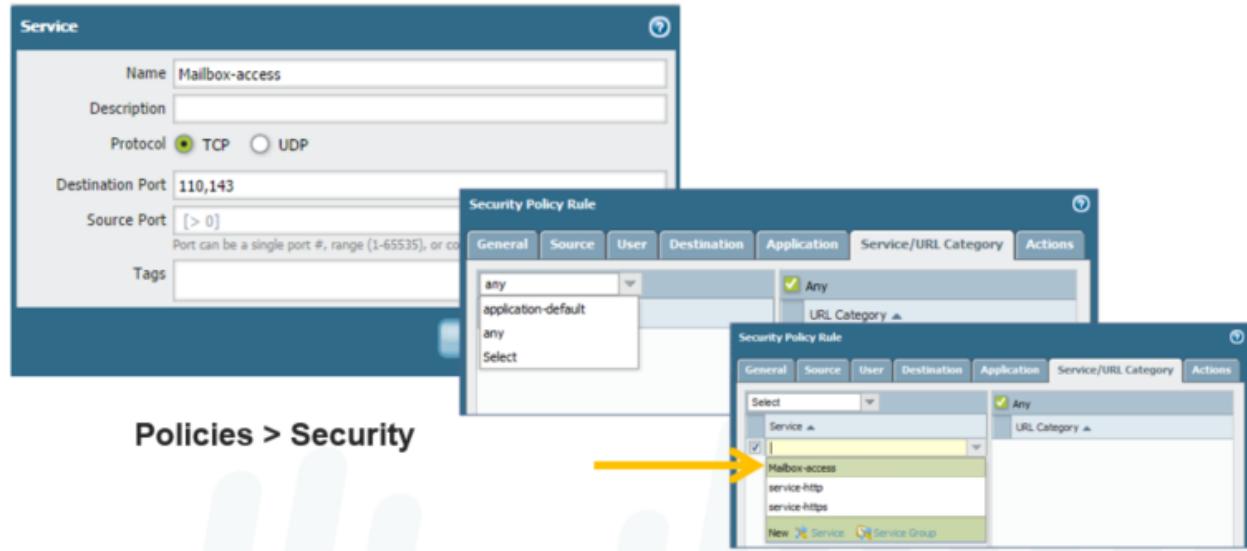
Security policies on a PAN-OS firewall match source, destination, application, and service. The application and service columns specify which applications can be identified on a defined set of

ports, or on all available ports. The service column allows administrator to select one of these options:

- Application-default: The service application-default option will set the security policy to allow the application on the standard ports associated with the application.
- service-http or service-https: The predefined services use TCP ports 80 and 8080 for HTTP, and TCP port 443 for HTTPS. Use this security policy setting if you want to restrict web browsing and HTTPS to these ports.
- Any: The predefined service Any matches any TCP/UDP port. This service is typically used to deny applications.
- Custom service: Administrators can create their own definition of TCP/UDP port numbers to restrict applications usage to specific ports.

Using the service application default is the recommended practice for configuring a security policy to allow the applications.

Objects > Services



The screenshot shows the 'Service' configuration interface. On the left, there's a form with fields for Name (Mailbox-access), Description, Protocol (TCP selected), Destination Port (110,143), Source Port (> 0), and Tags. A dropdown menu is open over the 'Application' tab of the 'Security Policy Rule' section. The menu contains options: 'any', 'application-default', 'any', and 'Select'. An arrow points from the 'Select' option in this menu to the 'Service' dropdown in the main 'Security Policy Rule' window. The 'Service' dropdown in the main window also has 'Select' and 'Mailbox-access' options. The 'Mailbox-access' option is highlighted in green, indicating it is selected.

Application Default:

- Application Default option is found in the Service column
- Example: Policy matches only if the application matches SSH and is using TCP port 22 as would be expected
- To limit services to their published default port values, policies can be configured with the application-default setting. With this setting configured, the policy matches only if the port number associated with the session matches the port listed in the matched

application's entry in the App-ID database. This feature is intended to limit port hopping and port spoofing.

Name	Type	Source			Destination			Application	Service	URL Category	Action
		Zone	Address	User	Zone	Address					
AllowSSH	universal	Trust-L3	any	any	Untrust-L3	any		ssh	application-default	any	

Application

Name: ssh

Description: Secure Shell is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer.

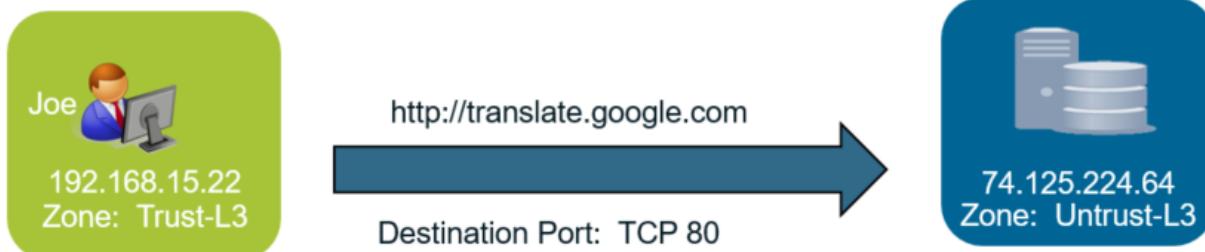
Additional Information: [Wikipedia](#) [Google](#) [Yahoo!](#)

Standard Ports: tcp/22

Depends on Applications:

Security Policy Example: http-get

Address Group:
"Local-Net" 192.168.0.0 /16



Name	Type	Source			Destination			Application	Service	Action
		Zone	Address	User	Zone	Address				
General Internet	universal	Trust-L3	any	any	Untrust-L3	any		dns fileserve flash ftp ping ssl web-browsing	application-default	✓
Google Translate	universal	Trust-L3	any	any	Untrust-L3	any		google-translate-base	application-default	✓

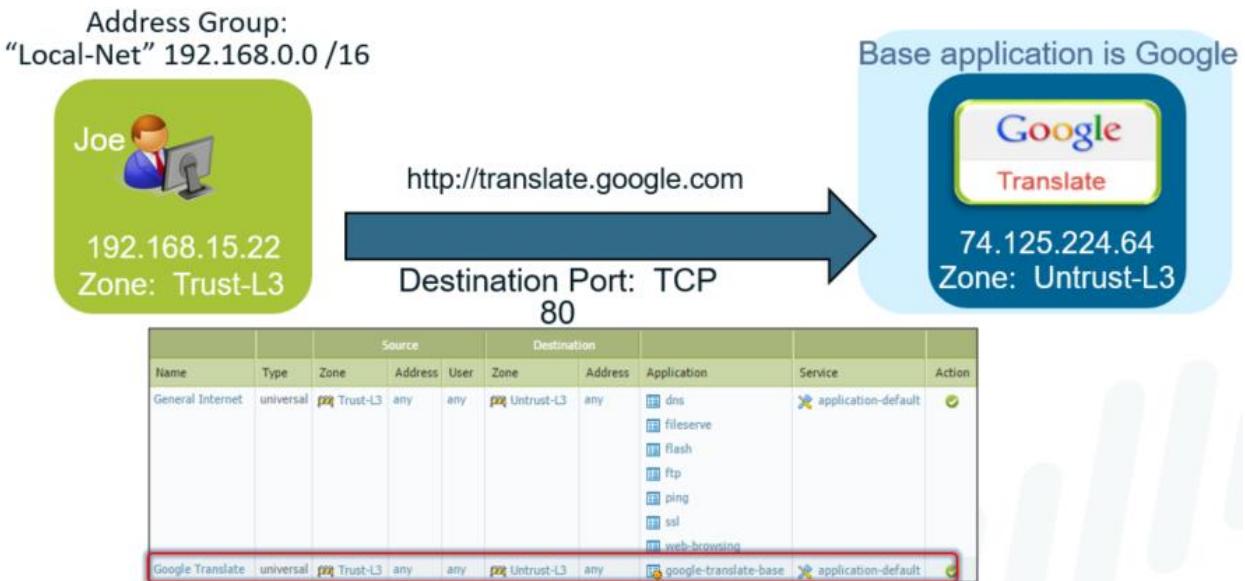
In this example, user Joe wants to access the website <http://translate.google.com> across the firewall. Joe's computer is in the Trust-L3 zone and the firewall interface connected to the public Internet is in the Untrust-L3 zone.

When Joe opens a browser connection to the website, a session is started. The firewall scans the traffic and finds the application signature for the http-get process, which matches the web-browsing application in App-ID. Based on the source and destination addresses, the firewall determines that the traffic is flowing from Trust-L3 (Source) to Untrust-L3 (Destination) zones.

Only these parameters are needed to match the General Internet policy, so the traffic is allowed. The Google Translate rule is not checked at this time because a match has already been found.

However, connecting to the website and actually using Google Translate are two different events. We evaluate that action in the next slide.

Security Policy Example: Google Translate



Security policy rules are examined for every packet that traverses the firewall in a session. The firewall can detect application shifts, or changes, within an established session.

For example, if a user to a website and tries to access Google Translate, this initiates an application shift in the current session. The App-ID engine detects the shift and finds the application signature for google-translate-base. The session still exists between Trust-L3 and Untrust-L3.

Using these three conditions (application, source zone, destination zone), the first rule is checked. There is no match because google-translate-base does not match the applications listed in the rule so the firewall moves on to the next rule. The second rule matches on all conditions, and google-translate-base is allowed to run.

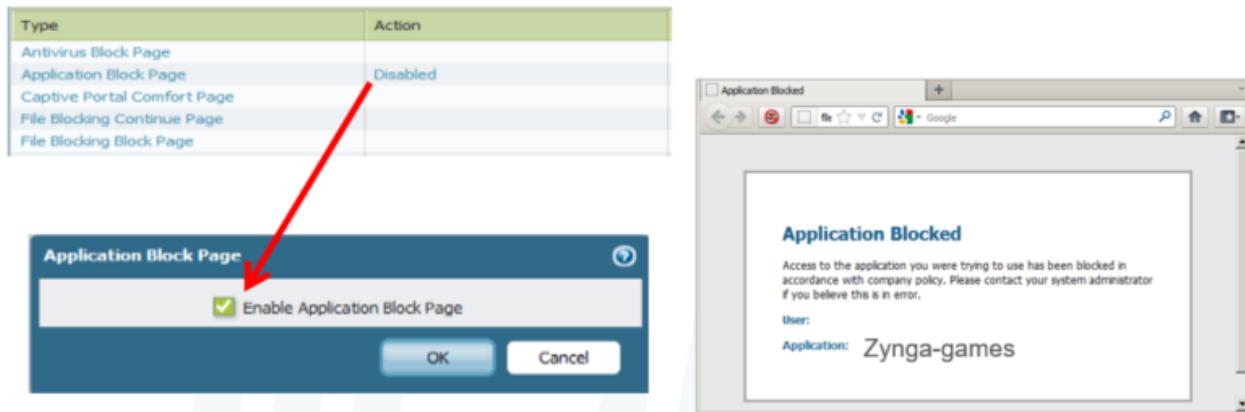
Does the order of the two rules matter in this example?

In this example, the order is not relevant. Traffic that matches one rule cannot match the other rule so neither rule prevents the other from being evaluated.

Application Block Response Pages:

When a security policy blocks a web-based application, a response page can be displayed on the user's browser.

Device > Response Pages > Application Block Page



By default, if a policy denies a Web-based application, in this case Zynga-games, the user simply gets generic browser-based error pages. In many cases, this results in additional support calls because users assume network problems rather than a policy violation. Therefore, custom response pages such as the one shown can be created to notify users when their action is blocked by a policy of the firewall.

The default response page includes the prohibited application name, as well as the username (if User-ID is enabled).

Application block response pages do not require an interface management profile to be set.

Application Filters and Application Groups:

- **Application Filters**
 - Dynamic grouping of individual App-IDs based on App-ID attributes:
 - Category
 - Subcategory
 - Technology
 - Risk
 - Characteristic
- **Application Groups**
 - Aggregates of:

- **Individual App-IDs**
- **Application Filters**
- **Nested Application Groups**

Security policies are based primarily on App-ID. The App-ID database is ever growing, so PAN-OS allows for the dynamic grouping of App-ID signatures through application filters. As new applications are added to the App-ID database and categorized, policies based on these filters automatically check for these new entries without any manual reconfiguration.

Application groups are static, user-defined sets of applications, application filters and other application groups. They allow the firewall administrator to create logical grouping of applications that can be applied to policies. Application groups are not updated with App-ID database changes.

Application Filters:

- Application filters are used to cover families of applications
- New application signatures are automatically included in the filter when released

Objects > Application Filters > Add

Name	Category	Subcategory	Technology	Risk	Characteristic
16 auth-service	business-systems	23 browser-based	8	1	14 Evasive
27 database		12 client-server	12	2	2 Excessive Bandwidth
32 erp-crm		1 peer-to-peer	8	3	3 Prone to Misuse
104 general-business			5	4	26 Transfers Files
187 management			3	5	2 Tunnels Other Apps
36 office-programs					6 Used by Malware
29 software-update					21 Vulnerability
46 storage-backup					20 Widely used

Name	Category	Subcategory	Risk	Technology	Standard Ports
google-calendar-base	business-syst	office-program	2	browser-base	443,80,tcp
google-calendar-enterprise	business-syst	office-program	5	browser-base	443,80,tcp
google-docs	business-syst	office-program	4	browser-base	443,80,tcp
google-docs-base	business-syst	office-program	5	browser-base	443,80,tcp
google-docs-editing	business-syst	office-program	5	browser-base	443,80,tcp
google-docs-enterprise	business-syst	office-program	5	browser-base	443,80,tcp
google-drive	business-syst	office-program	5	browser-base	443,80,tcp

An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and

characteristic. This feature is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, create an application filter that matches on the Category business-systems and the Subcategory office-programs as shown in this example.

As applications are added to the App-ID database during the weekly updates, they are classified by category, subcategory, technology, risk, and characteristic. So as the new office program applications emerge, and new App-IDs get created, these new applications automatically match the filter you defined; in this case, office program applications. The benefit is you need not make additional changes to your policy rule base to safely enable any application that matches the attributes you defined within the Office Programs filter.

Application Groups:

Application groups can contain applications, filters, or other application groups

The screenshot shows the Palo Alto Networks management interface. On the left, a sidebar lists various objects like Addresses, Applications, and Application Groups. The 'Applications' section is currently selected. In the main pane, there's a table titled 'social-networking' with columns for Name, Location, Members, Applications, and Filters. Under 'Applications', it lists youtube, facebook, and twitter. Below the table are buttons for Add, Delete, and Clone. A red arrow points from the text 'Application groups can contain applications, filters, or other application groups' to the 'Applications' section of the table. To the right, a detailed view of the 'social-networking' application group is shown in a separate window. It has a 'Name' field and a 'Applications' list containing many different application signatures such as wetpaint-editing, wikidot-editing, etc. At the bottom of this window, there are sections for 'Application Group' (containing 'social-networking') and 'Application Filter' (containing 'web-browsing-filter').

To group specific applications, application groups allow administrators to create custom lists of applications for policies to check. Application groups can combine applications, application filters, and application groups into a single entry that can be added to security policies.

Application groups are not automatically updated when new applications are added to App-ID database unless the group contains a filter that contains the new signature.

An application group is an object that contains applications that you want to treat similarly in a policy. Application groups are useful for enabling access to applications that you explicitly sanction for use within your organization. Grouping sanctioned applications simplifies administration of your rule bases: instead of updating individual policy rules when there is a change in the applications you support, instead you update only the affected application groups.

When deciding how to group applications, consider how you plan to enforce access to your sanctioned applications and create an application group that aligns with each of your policy goals. For example, you might have some applications that you allow only your IT administrators to access, and other applications that you want to make available for any known user in your organization. In this case, you create separate application groups for each of these policy goals. Although you generally want to enable access to applications on the default port only, you may want to group applications that are an exception to this and enforce access to those applications in a separate rule.

Application Groups Example:

In this example, the applications that the administrator wants to allow and deny do not fit into an application filter search. This administrator finds it more convenient to manually list the applications. However, any new applications added to the App-ID database do not automatically populate these groups.

Known_Good

- Static group of applications
 - DNS
 - Web-browsing
 - SSL
 - Flash

Known_Bad

- Static group of filters and applications
 - Games
 - P2P
 - Remote Access
 - Tunneling

Objects > Application Groups				
Name	Members	Applications	Filters	Groups
Known_Good	4	dns web-browsing ssl flash		
Known_Bad	4		Games P2P Remote Access Tunneling	

Displaying Application Information:

In a security policy rule, select the Objects tab to view information about application groups, filters, or individual applications in the rule.

PAN-OS allows viewing of the contents of these objects from the policy page. Click the name of the object to see information about the object and the contained components.

Address objects can also be expanded in the policy window for additional information.

Displays detailed information for:

Applications
Application Containers

Filters
Application Groups

Name	Source			Destination			Application	Service	Action
	Zone	Address	User	Zone	Address	Application			
Known_Good rule	Trust-L3	Internal Users	any	Untrust-L3	any	Known_Go	Edit...	✓	
Known_Bad rule	Trust-L3	Internal Users	any	Untrust-L3	any	Known_Ba	Filter	✗	
Unclassified_Traffic Rule	Trust-L3	any	any	Untrust-L3	any	any	Remove	✗	

Application Group
Name: Known_Good
Members: dns
web-browsing
ssl
flash

Identify Your Unknown, Unclassified Traffic:

Requirements:

- Process known good and known bad applications
- Determine what other applications are present within your network traffic for future classification

Name	Source			Destination			Application	Service	Action
	Zone	Address	User	Zone	Address	Application			
Known_Good rule	Trust-L3	Internal Users	any	Untrust-L3	any	Known_Go	Edit...	✓	
Known_Bad rule	Trust-L3	Internal Users	any	Untrust-L3	any	Known_Ba	Filter	✗	
Unclassified_Traffic Rule	Trust-L3	any	any	Untrust-L3	any	any	Remove	✗	

Application Group
Name: Known_Good
Members: dns
web-browsing
ssl
flash

In this example, the administrator was given a list of applications to allow and deny on the network. For instance, some of the known good applications include: dns, web-browsing, ssl, and flash.

However, the company acknowledges that they do not know all of the applications that the users are using. Therefore the administrator must set allow and deny policies and determine

what other applications are in use so they can be added to their respective rule. The three rules you see here enable the administrator to do just that.

Looking at the Actions column, the first “Known_Good rule” allows the known good applications to pass through the firewall, whereas the “Known_Bad rule” blocks those known bad applications that are disallowed by company policy.

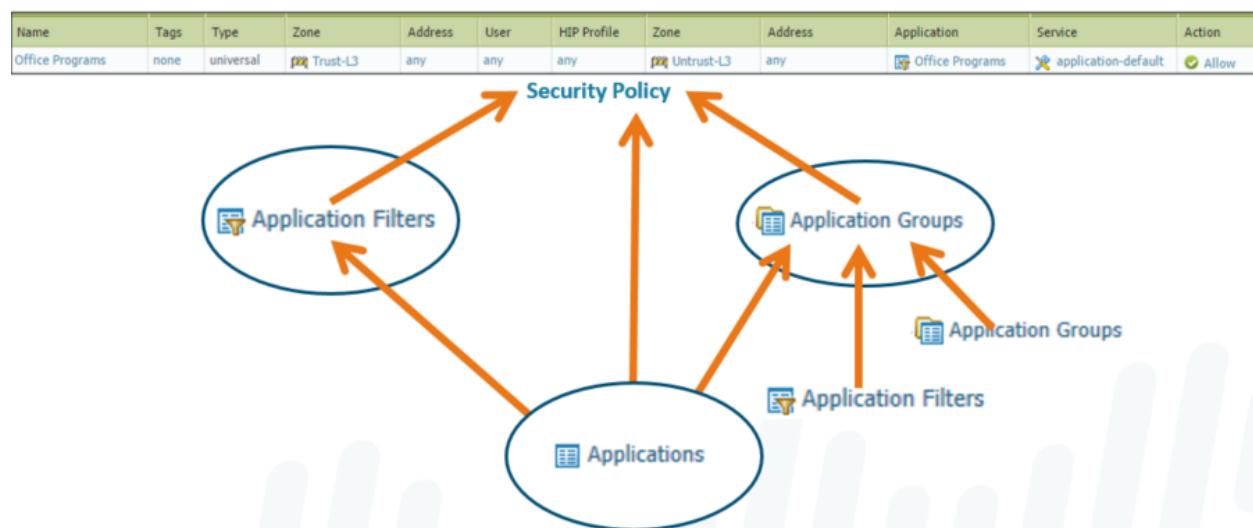
The last “Unclassified_Traffic Rule” is what enables the administrator to determine what other applications are hitting the firewall by matching traffic that is not caught by the first two rules. Whether this rule is set to allow or deny the traffic, in this case deny, any traffic matched by this rule is logged by the firewall. The administrator can then use the logs to identify applications in use on the network and add them to the appropriate application group as necessary. Hence, this last rule is an important one that should not be omitted. This last rule also helps you identify newly classified applications, or reclassified applications, that you want to allow or deny and can easily do so by adding them to the rule.

Application Filters and Groups Hierarchy

Applications are automatically added to matching application filters when they are added to the App-ID database.

Application groups are manually configured to include applications, application filters, and other applications groups.

Firewall policies can be configured to match newly discovered application signatures against applications, application filters, or application groups.



Application Window Details:

Application

Name: ssh	Description: Secure Shell is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer.										
Standard Ports: tcp/22											
Depends on:											
Implicitly Uses:											
Additional Information: Wikipedia Google Yahoo!											
Characteristics <table border="1"> <tr> <td>Evasive: no</td> <td>Tunnels Other Applications: yes</td> </tr> <tr> <td>Excessive Bandwidth Use: no</td> <td>Prone to Misuse: no</td> </tr> <tr> <td>Used by Malware: yes</td> <td>Widely Used: yes</td> </tr> <tr> <td>Capable of File Transfer: yes</td> <td></td> </tr> <tr> <td>Has Known Vulnerabilities: yes</td> <td></td> </tr> </table>		Evasive: no	Tunnels Other Applications: yes	Excessive Bandwidth Use: no	Prone to Misuse: no	Used by Malware: yes	Widely Used: yes	Capable of File Transfer: yes		Has Known Vulnerabilities: yes	
Evasive: no	Tunnels Other Applications: yes										
Excessive Bandwidth Use: no	Prone to Misuse: no										
Used by Malware: yes	Widely Used: yes										
Capable of File Transfer: yes											
Has Known Vulnerabilities: yes											
Options <table border="1"> <tr> <td>TCP Timeout (seconds): 3600</td> <td>Customize...</td> </tr> <tr> <td>TCP Half Closed (seconds): 120</td> <td>Customize...</td> </tr> <tr> <td>TCP Time Wait (seconds): 15</td> <td>Customize...</td> </tr> <tr> <td>App-ID Enabled: yes</td> <td></td> </tr> </table>		TCP Timeout (seconds): 3600	Customize...	TCP Half Closed (seconds): 120	Customize...	TCP Time Wait (seconds): 15	Customize...	App-ID Enabled: yes			
TCP Timeout (seconds): 3600	Customize...										
TCP Half Closed (seconds): 120	Customize...										
TCP Time Wait (seconds): 15	Customize...										
App-ID Enabled: yes											
Classification <table border="1"> <tr> <td>Category: networking</td> </tr> <tr> <td>Subcategory: encrypted-tunnel</td> </tr> <tr> <td>Technology: client-server</td> </tr> <tr> <td>Risk: 4 Customize...</td> </tr> </table>		Category: networking	Subcategory: encrypted-tunnel	Technology: client-server	Risk: 4 Customize...						
Category: networking											
Subcategory: encrypted-tunnel											
Technology: client-server											
Risk: 4 Customize...											

paloalto NETWORKS[®]

Dashboard ACC Monitor Policies Objects Network Device

To reset any filters, please click the Clear Filters button

Total Number of Applications: 3190 matching applications

Category	Subcategory	Technology	Risk	Characteristic
1238 business-systems	54 audio-streaming	1175 browser-based	1331 1	41 Data Breaches
633 collaboration	23 auth-service	1385 client-server	827 2	634 Evasive
501 general-internet	38 database	481 network-protocol	531 3	654 Excessive Bandwidth
320 media	85 email	147 peer-to-peer	359 4	36 FEDRAMP
496 networking	66 encrypted-tunnel		142 5	1 FINRA
2 unknown	45 erp-crm			98 HIPAA
	344 file-sharing			99 IP Based Restrictions
	68 gaming			23 New App-ID
	192 general-business			519 No Certifications

The Applications page lists various attributes of each application definition

Displaying 1-94 of 3419

Application Shifts:

Applications can change during lifetime of a session called an application shift.

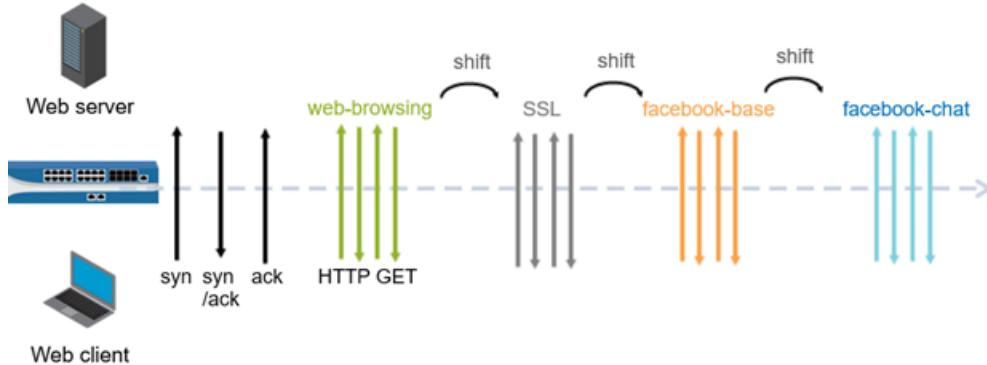
example, user types www.facebook.com into web browser to access Facebook-chat.

Initial request goes out as HTTP request, & application is recognized as web-browsing.

After the HTTP request is completed, the application is changed to Facebook-base.

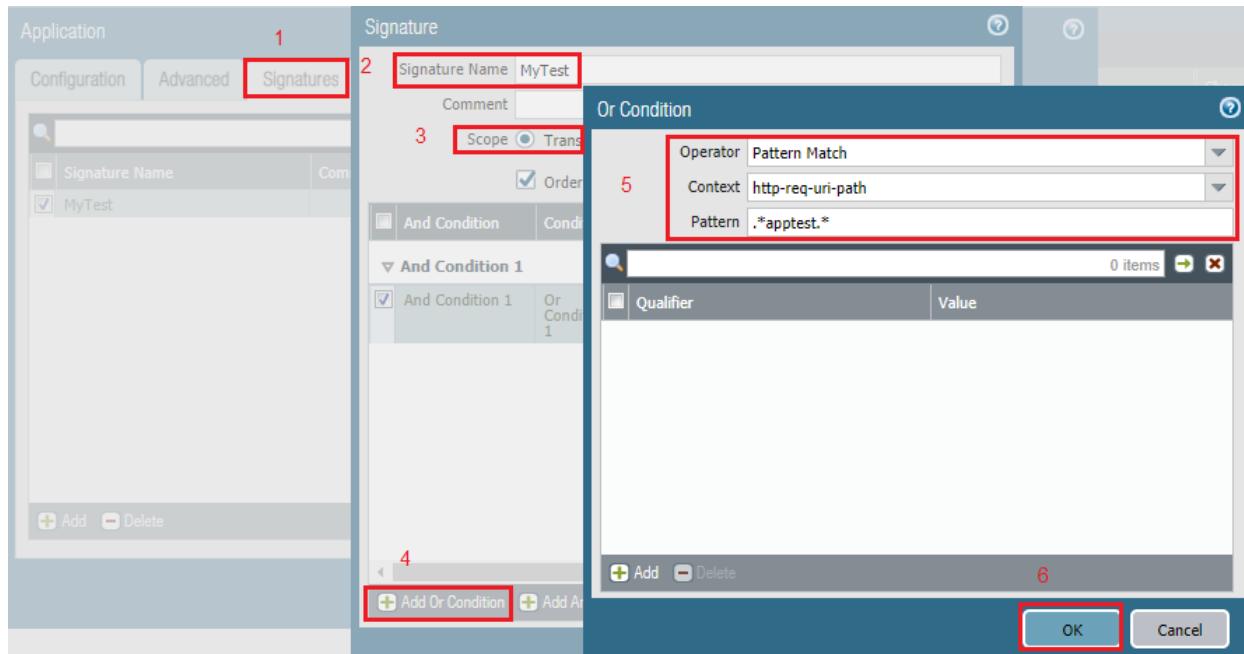
After Facebook-base application is processed, application changes to Facebook-chat.

Network traffic can shift from one application to another during a session.

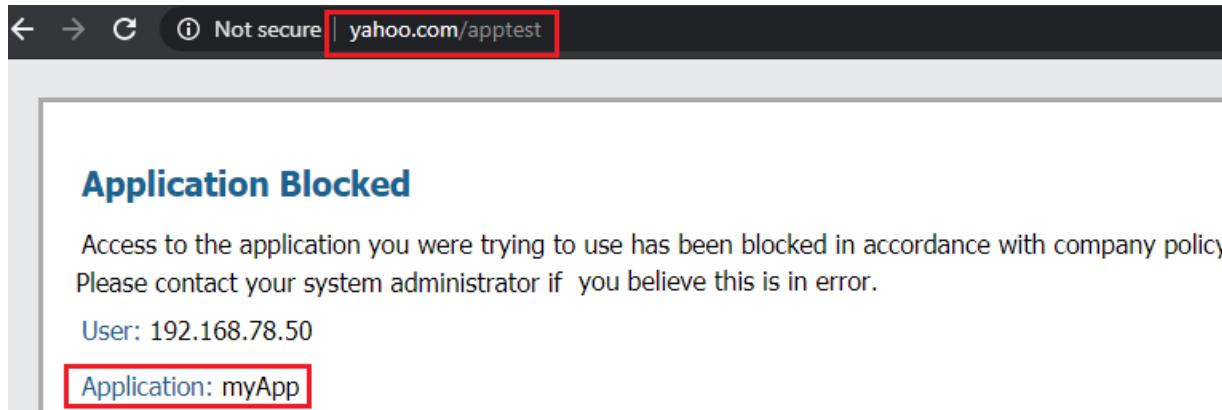


Custom Application:

Let's create custom Signature, on the same our create Filter category. On the Signatures tab, click Add and define a Signature Name. Specify the Scope of the signature: whether it matches to a full Session or a single Transaction. Specify conditions to define signatures by clicking Add And Condition or Add Or Condition. Select an Operator to define the type of match conditions.



Lets tested go to Inside-PC and type yahoo.com/apptest it will show block page because our custom created app is under social networking category, which is block in our filter, so it dynamically added to that Filter and blocked by Palo Alto Network Firewall.



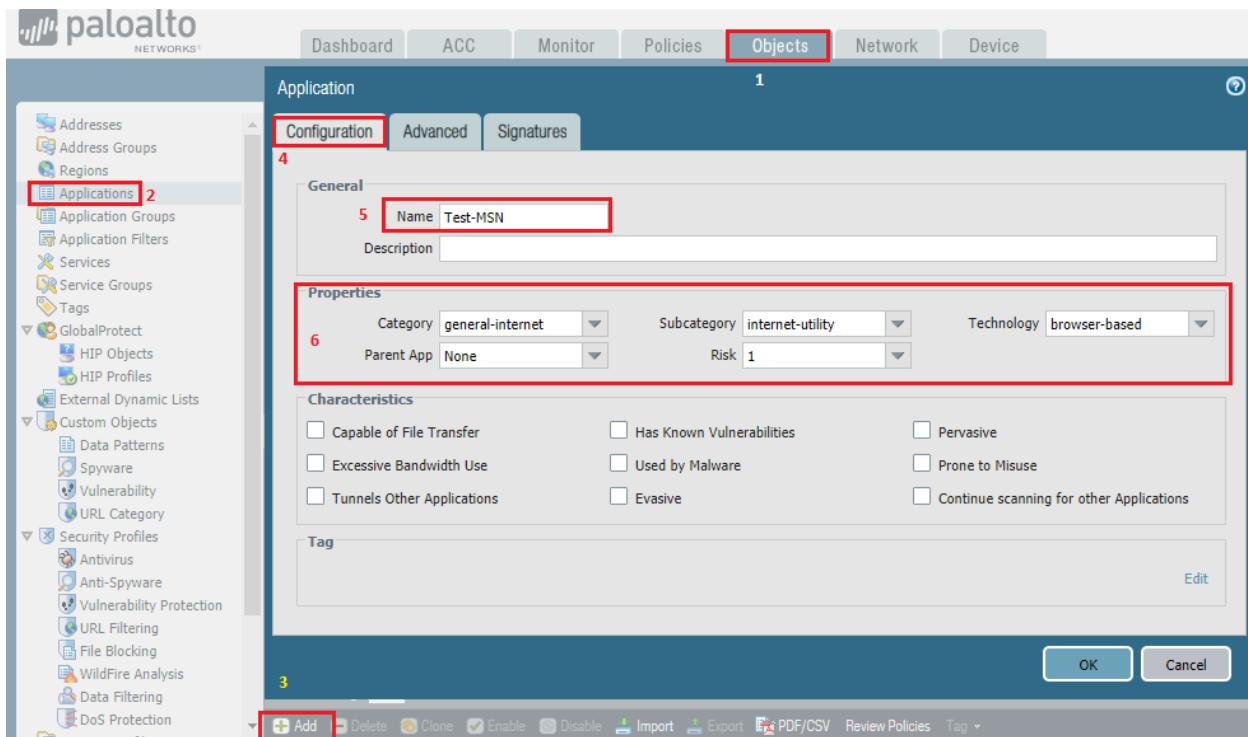
Application Override:

Firewall is configured to override normal App-ID of specific traffic passing through firewall.
Application Override policy takes effect, all further App-ID inspection of traffic is stopped.
Change the firewall classifies network traffic into apps, specify application override policies.
Application override with custom application will prevent session from being processed.
Application override prevent session to process by App-ID engine, which is L7 inspection.

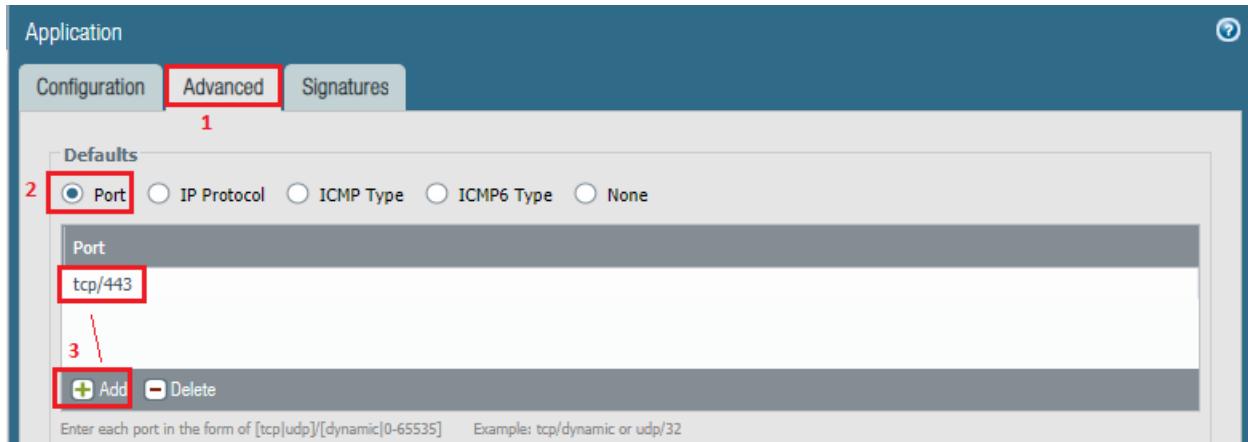
In simple words, with Application Override Policy, Firewall stops doing Layer 7 processing.
Instead it forces firewall to handle the session as regular stateful inspection firewall at L4.

So, in other words application override policy thereby saves application processing time.
Customers build own custom applications to address specific needs unique to the company.
May not have signatures to properly identify expected behavior and identify traffic & app.
Creating application override to allow easier identification & reporting & prevent confusion.
Network applications that are classified as unknown can create new application definitions.

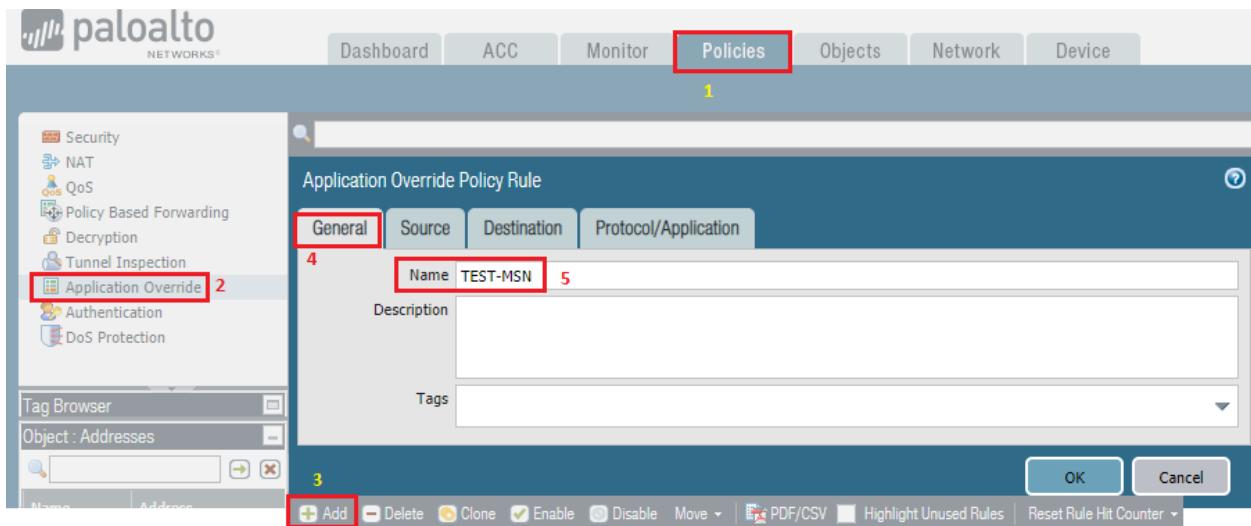
Let's create custom application go to Objects>Applications then click Add in lower left corner name application in our case Test-MSN select values for Category, Subcategory & Technology. Go to Advanced > Defaults and select Port to list the ports in the application. click Add type the port tcp/443 and press OK. We don't need a signature, so go ahead and click OK to complete this custom application.



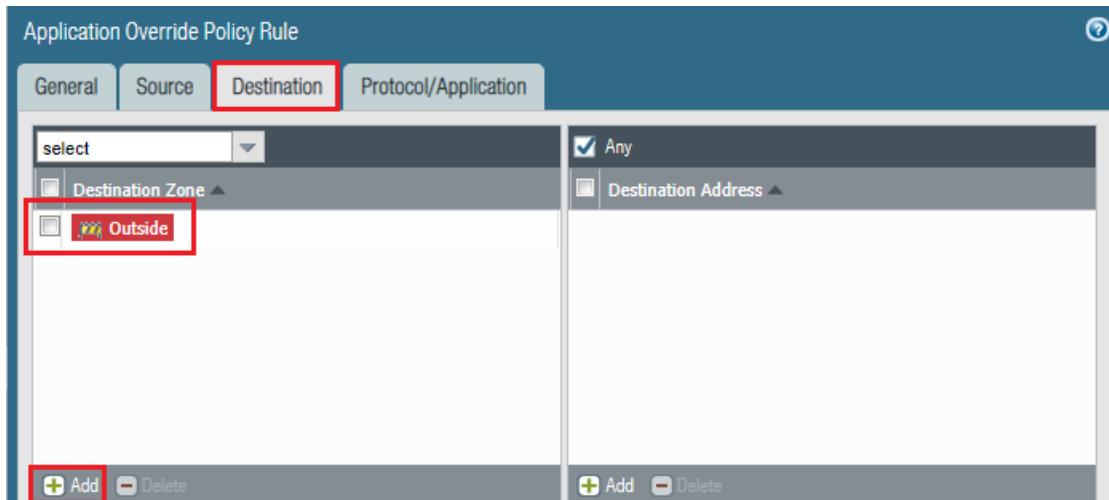
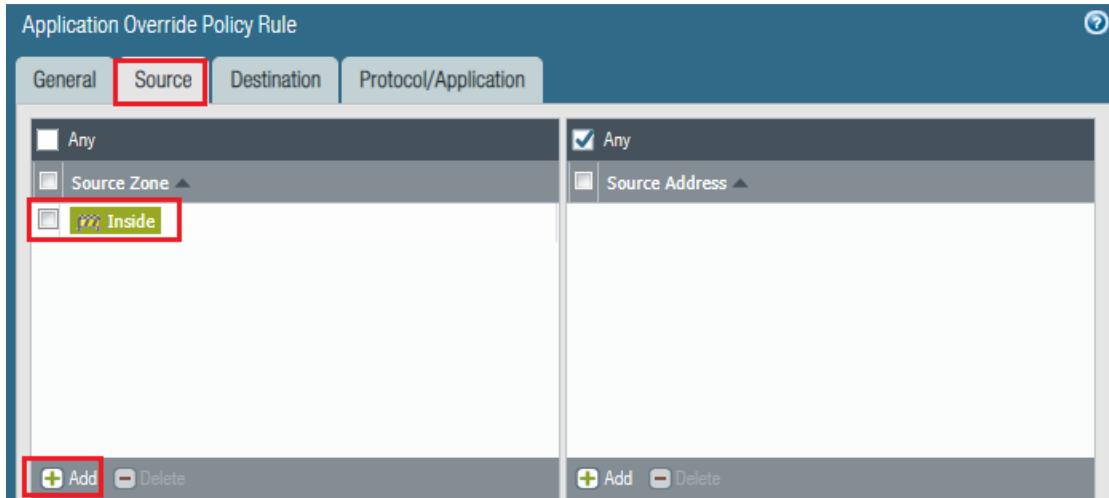
Go to Advanced > Defaults and select Port to list the ports in the application. click Add type the port tcp/443 and press OK. We don't need a signature, so go ahead and click OK to complete this custom application.



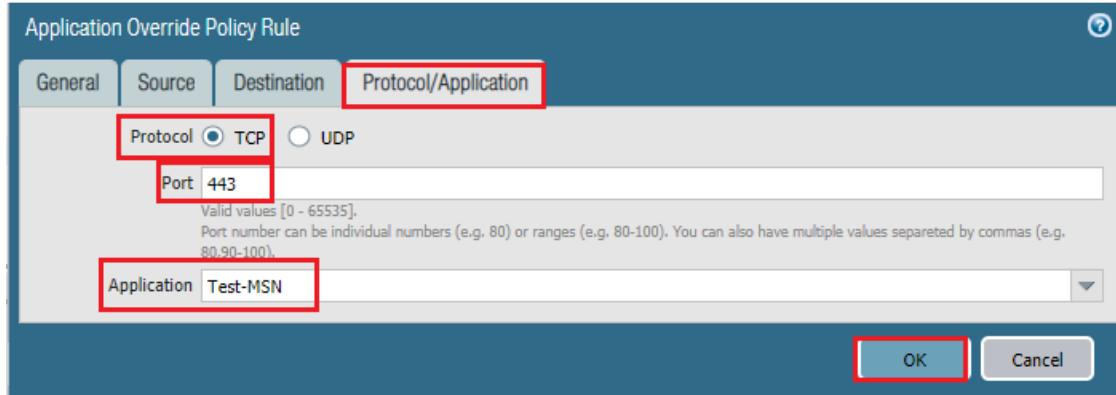
To create an Application Override policy, go to Policies > Application Override, then click Add: Under the General tab, enter a name for the policy. In our case TEST-MSN.



Go to Source and add the Source Zone. Specify a Source/Destination Address if the source is a static address; otherwise, leave as Any.



Go to Protocol/Application and select the Protocol, enter the Port number in our case 443, and select the custom application created in our case Test-MSN.



Note: Create Security Policy to allow this new application through firewall or modify an existing rule.

Now commit all the changes and lets test the new created Application Override policy.

	Receive Time	Type	Decr...	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
🕒	02/13 23:53:26	end	no	Inside	Outside	Inside-PC	a-0003.a-msedge.net	443	Test-MSN	allow	Inside-to-Outside1	tcp-rst-from-server	15.0k
🕒	02/13 23:48:33	end	no	Inside	Outside	Inside-PC	69.172.200.235	443	Test-MSN	allow	Inside-to-Outside1	tcp-rst-from-client	7.3k
🕒	02/13 23:48:22	end	no	Inside	Outside	Inside-PC	a-0003.a-msedge.net	443	Test-MSN	allow	Inside-to-Outside1	tcp-rst-from-server	15.0k
🕒	02/13 23:48:17	end	no	Inside	Outside	Inside-PC	ham02s12-in-f42.1e100.net	443	Test-MSN	allow	Inside-to-Outside1	tcp-rst-from-client	7.7k

Application Updates:

From the WebGUI, go to Device > Dynamic Updates

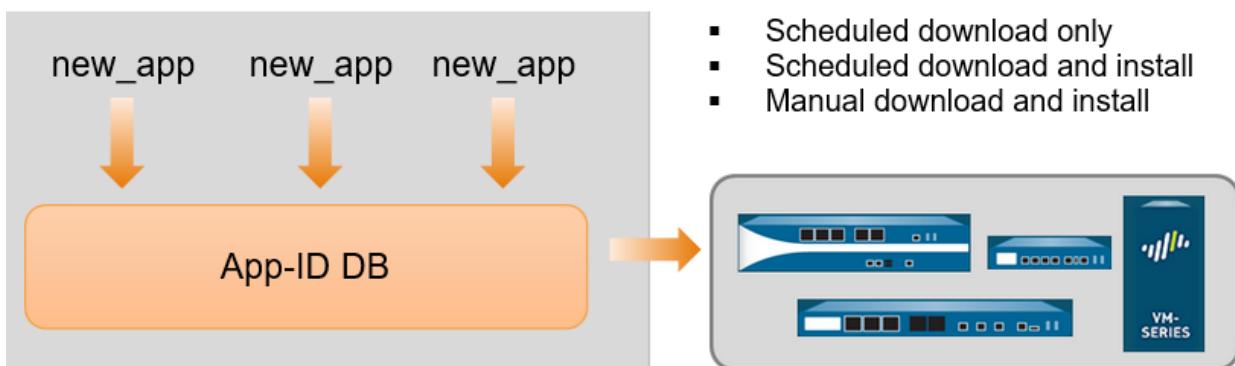
Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Documentation				
8226-5859	panuvp2-all-apps-8226-5859	Apps	Full	37 MB	2020/01/14 10:25:48 PST			Download	Release Notes				
8227-5876	panuvp2-all-apps-8227-5876	Apps	Full	42 MB	2020/01/17 17:03:29 PST			Download	Release Notes				
8228-5880	panuvp2-all-apps-8228-5880	Apps	Full	42 MB	2020/01/20 10:00:49 PST			Review Policies	Release Notes				
8229-5889	panuvp2-all-apps-8229-5889	Apps	Full	42 MB	2020/01/22 20:08:48 PST			Download	Release Notes				
8230-5894	panuvp2-all-apps-8230-5894	Apps	Full	42 MB	2020/01/24 16:25:16 PST			Download	Release Notes				
8231-5919	panuvp2-all-apps-8231-5919	Apps	Full	42 MB	2020/01/29 20:25:38 PST			Review Policies	Release Notes				
8232-5926	panuvp2-all-apps-8232-5926	Apps	Full	43 MB	2020/01/31 21:18:52 PST			Download	Release Notes				
8233-5931	panuvp2-all-apps-8233-5931	Apps	Full	43 MB	2020/02/04 20:24:09 PST			Download	Release Notes				
8234-5935	panuvp2-all-apps-8234-5935	Apps	Full	43 MB	2020/02/06 18:36:31 PST			Install	Release Notes				
8235-5938	panuvp2-all-apps-8235-5938	Apps	Full	43 MB	2020/02/11 10:30:09 PST			Download	Release Notes				
8236-5939	panuvp2-all-apps-8236-5939	Apps	Full	43 MB	2020/02/12 13:25:22 PST			Download	Release Notes				
8237-5941	panuvp2-all-apps-8237-5941	Apps	Full	43 MB	2020/02/13 17:05:24 PST			Download	Release Notes				
▼ GlobalProtect Clientless VPN										Last checked: 2020/02/08 11:22:44 PST	Schedule: None		
82-175	panup-all-gp-82-175	GlobalProtectCle...	Full	73 KB	2019/12/19 13:52:49 PST			Download	Release Notes				
84-177	panup-all-gp-84-177	GlobalProtectCle...	Full	73 KB	2020/01/31 14:26:13 PST			Download	Release Notes				

Palo Alto Networks regularly posts updates for application detection.

Application can be updated manually download and install or schedule.

Screenshot of the Palo Alto Networks Device configuration interface. The 'Device' tab is selected. On the left, the navigation pane shows 'Dynamic Updates' highlighted with a red box. The main table lists 'Applications and Threats' with a schedule of 'Every Wednesday at 01:02 (Download)'. A modal window titled 'Applications and Threats Update Schedule' is open, showing the schedule details: Recurrence (Weekly), Day (Wednesday), Time (01:02), Action (download-only), and Threshold (hours) set to [1 - 336]. The 'OK' button is also highlighted with a red box.

Version	File Name	Features	Type	Size	Release Date
8226-5859	panupv2-all-apps-8226-5859	Apps	Full	32 MB	2020/01/14 10:25:48 PST
8227-5876	panupv2-all-apps-8227-5876				
8228-5880	panupv2-all-apps-8228-5880				
8229-5889	panupv2-all-apps-8229-5889				
8230-5894	panupv2-all-apps-8230-5894				
8231-5919	panupv2-all-apps-8231-5919				
8232-5926	panupv2-all-apps-8232-5926				
8233-5931	panupv2-all-apps-8233-5931				
8234-5935	panupv2-all-apps-8234-5935				
8235-5938	panupv2-all-apps-8235-5938				
8236-5939	panupv2-all-apps-8236-5939				
8237-5941	panupv2-all-apps-8237-5941				
82-175	panup-all-gp-82-175				
84-177	panup-all-gp-84-177				



Decryption Concepts

- Encrypted traffic is growing every year
- PAN's can decrypt SSHv2 and SSL/TLS inbound and outbound traffic
- SSL Establishment includes:
 - Client – requests SSL connection
 - Server – sends server public cert
 - Client – Verifies Cert
 - Client – sends encrypted session key
 - Server – begins encrypted communications session
- When an SSL session is first established or needs to re-establish a session and rekey, this is known as PFS (Perfect Forward Secrecy)

- The FW can act as an Outbound SSL Proxy:
 - A client initiates a session to an external server
 - The FW intercepts the connection, decrypts it, applies any security policies, re-encrypts the traffic and sends to the external server
- The FW can perform Inbound SSL decryption (does not act as a proxy, just decrypts and inspects)
 - The internal server's certificate and private key need to be added to the PAN firewall for this to function properly
- The FW can perform SSHv2 Proxy for both inbound and outbound SSH traffic
 - If SSH Tunneling of another application is found, the session is blocked to prevent apps from bypassing firewall rules.
- Public Key Infrastructure (PKI) solves issue of secure identification of public keys
 - Uses digital certificates to verify public key owners (x.509 format)
 - Typical PKI components include:
 - Root CA: Provides service that confirm identity and public keys to people and companies.
 - Intermediate CA: Certified by a Root CA, and will issue certificates; has a DB that will issue, revoke certs and stores CSR's
 - Device has the certificate and private keys. They maintain a list of trusted CA's, and can be updated by admins or by system updates.
 - Certificate Chain starts with the device and ends with the Root CA. As long as there is a Root CA in the chain, the certificate can be checked as valid (or revoked).
 - Certificate Hashes can be validated to confirm that it hasn't been intercepted and altered.
- Firewalls can use for many purposes:
 - SSL/TLS
 - MGT Interface User Auth
 - Global Protect: Portal Auth, Gateway Auth, Mobile Security Manager Auth
 - Captive Portal User Auth
 - IPSec VPN IKE Auth
 - HA Auth
 - Secure Syslog Auth
- All Certificates in a chain must be checked and validated before an SSL session is permitted
- Checking a Certificate includes:
 - Is the signature valid

- Is the date range valid
- is it intact/not malformed?
- Has the certificate been revoked?
 - CRL (certificate revocation list) has a list of revoked certificates
 - OCSP (online cert status protocol) can check revocation status
 - Certs can be revoked for: Private key compromised, Hostname/username changed, counterfeit key found
- Certificate signing request (CSR) is generated by the device. This is used by a certificate issuing authority to generate the device. The private key generated with this CSR never leaves the device.

Certificate Management

- Devices are managed under Device > Certificate Management > Certificates
 - Operations supported include:
 - Generate CSR's
 - View Certificates
 - Modify Certificate Use
 - Import/Export Certificates
 - Delete Certificates
 - Revoke Certificates
 - Different certificates have different features
 - A signing certificate is required for SSL Forward Proxy and Global Protect
 - There are 3 methods of getting a certificate on the FW
 - Generate a self-signed CA Certificate from the FW
 - Generate a CA Cert using CSR
 - Import a CA Certificate
- The FW will sort the certificates in a hierarchy in order of the CA chain, root to intermediate to device.

SSL Forward Proxy Decryption

- An SSL Forward Proxy decryption is used to intercept and decrypt SSL session in order to inspect the traffic for nefarious contents
- Steps in this process are:
 - Client sends request to external server through firewall
 - Firewall intercepts the SSL request
 - Firewall then contacts the external server and sends that server the FW cert
 - External server responds with its server certificate; firewall validates certificate
 - The SSL session is then established between the server and the firewall

- The firewall then sends a copy of the remote server cert, signed with the FW SSL certificate
 - The client validates the certificates and the session continues
- The firewall will sign the certificate sent to the client with its firewall trust cert if the external servers cert is signed by a CA it trusts. If it doesn't have a CA the FW knows/trusts, the FW will send back its firewall untrust certificate, and the client is shown an untrusted warning page in their browser.
- To configure Forward Proxy: (see PAN Docs for more details and instructions)
 - Configure a Forward Trust Certificate
 - Configure a Forward Untrust Certificate
 - Generate a new cert on FW; cert should not be trusted by SSL clients, but ability to sign other server certs.
 - Do not copy; this should be untrusted and unknown to any CA.
 - Select 'CA' checkbox on this cert
 - Configure as forward untrust cert in properties
 - Configure SSL Forward Proxy
 - Under Policies > Decryption (be sure to know what traffic is protected by local/state/national laws and cannot be decrypted).
 - A decryption profile allows check on both decrypted traffic and traffic excluded from decryption
 - Allows to block sessions unsupported protocols, cypher suites, or SSL client auth.
 - Block sessions based on certificate status: revoked, unknown, expired, etc
 - After creating a profile, it can be applied to a decryption policy.
 - A default profile is provided that can be used/cloned/modified.
 - Rules for the decrypted traffic will need to be present. For example, if traffic is web-browsing, google docs, or another encrypted application setting, security policies allowing that traffic must be present or the traffic will be dropped as matching no FW rules.

SSL Inbound Inspection

- FW Can inspect inbound SSL traffic
- The internal server's cert and private key must be loaded on the firewall.
- The firewall will decrypt and read the traffic, and then forwards the original encrypted traffic to the server
 - Note that the traffic will be forwarded only if it is not blocked/dropped by a security policy on the firewall.
- To create an SSL inbound inspection policy:

- Import the server certificate and private key into the firewall (PEM and PKCS12 formats supported)
- Create a decryption policy under Policies > Decryption > Add – under Options, select ‘Decrypt’
- (Optional) Create a decryption profile that can be added to the decryption policy

Other Decryption Topics

- Some applications may not work with SSL Forward Proxy
 - Application with client-side certs
 - Non-RFC compliant apps
 - Servers using unsupported cryptographic settings
- If an application fails, the site is added to the excluded cache list for 12 hours
- Decryption Exclusion are apps that encryption is known to break
 - The prepopulated list is under Device > Certificate Management > SSL Decryption Exclusion
 - Custom domains can be added to this list, and wildcards are supported.
- If the decryption policy is set to an action of ‘no-decrypt’, the profile attached to the rule can still check for expired or untrusted certificates. This can be done under ‘No Decryption’ tab in the profile.
- Decryption Mirroring can mirror decrypted traffic to a capture device for DLP and/or network forensics
 - Requires a (free) licence to activate; contact TAC support to get the license key. Key is perpetual, does not need renewal.
 - Only available on the PA-3000, PA-5000 and PA-7000 series firewall.
- Hardware Security Module (HSM) are a hardware storage for keys for additional security features (FIPS)
 - PA-3000, PA-5000, PA-7000, and PA-VM series; Panorama VM, and M100e
- The traffic log can be used to determine if the traffic is being decrypted by the firewall
 - Also can be done by setting a log filter for Flags, Has, SSL Proxy.
- Troubleshooting SSL sessions
 - Using the log filter to search for ‘session end reason’ ‘equal’ ‘decrypt error’, you can see what sessions are not being decrypted.

Application ID Overview

- An application is a specific program or feature whose communication can be labeled, monitored and controlled
- App-ID does additional work beyond just port
- Port-based rules use ‘Service’

- Application-based rules use 'application'
- Application rules will allow only the application traffic that is allowed (ex: FTP) and not other traffic using that port.
- Zero-day or unknown traffic trying to pass on an application policy is also blocked, because it doesn't match the application traffic.
- App-ID for UDP can generally identify the application on the first packet
- App-ID for TCP will take several packets to identify, as the 3-way handshake needs to be done, and then the app data will need to be examined, depending on the app data.
- Application DB is updated weekly with new and updated application identifiers.
- Unknown protocol decoder will attempt to identify unknown appid traffic
- Known protocol decoder will match traffic with a known app
- Decryption to ID traffic will check if decrypt is configured.
- App-ID steps:
 - Packet comes in – IP/Port identified
 - Check if allowed by Security policy
 - If allowed, App-ID will attempt to identify – Known, Unknown or Decrypt (if configured)
 - Does it match?
 - Security policy applied to allow or block.

Using App-ID in a Security Policy

- Traffic can shift from one app to another during a session lifetime
- As more traffic is received, it can also refine what the traffic it sees is.
- This is why several applications are sometimes needed; web browsing, Facebook base and facebook chat could all be in the same session.
- Signatures contain data on several versions of applications
- Application dependence can be seen in the applications section under objects
- Some objects have dependencies built in – example, facebook has web-browsing as a needed dependence
- Under Objects > Applications, you can find what applications have what implicit use of other applications.
 - Search for an application
 - Click the application
 - Look for the 'implicitly uses' to see what apps it will implicitly use.
- Application Filters can be used to allow access to a series of applications, such as Office application systems, or online streaming audio and video.

- Application Groups can be used to group together several applications for easier deployment to firewall security policy rules. They also can be used for QoS and Policy Based Forwarding (PBF) Policies.
- Applications, Filters and groups can be nested to several levels and added to policies.
- Application groups are added to security policy rules just like single applications.
- Under Objects > Services can be used to build custom services on specific ports. This can be used to narrow access on applications
- Application Block Page can be configured to block access to specific applications. If User ID is in use, it will use the name of the user. If not, it will use their IP address.

Identifying Unknown Application Traffic

- Traffic known to the PAN FW will be shown in the traffic log with the app identified.
- When it's not able to be identified, if it is http, it is identified as web browsing, if it is not http, it is 'unknown tcp' or 'unknown udp'.
- In initial deployments in TAP mode, in the Policies > Security section, you can create a policy to block 'known good' or 'known bad' apps, and add known applications on your network to the appropriate rule. A third rule set for 'any/any/allow' will let you see the other applications not identified to help pinpoint what they are and their source/destination.
- To control unknown applications:
 - Create a custom application after identifying the traffic via packet captures.
 - Configure an application override policy. This will disable the application ID for this traffic,
 - Block unknown-tcp, unknown-udp * be cautious if in production, this could block legitimate traffic. This isn't recommended unless you are confident the traffic will have no production impact.

Updating App-ID

- App-ID DB is updated weekly, and can be added to the application/threat auto update. It can also be manually downloaded and installed.
- A check can be done on the updated App-ID under Object > Applications, and clicking on the 'review policies' on the bottom of the page.
- On the Application > Review policies page, you can see what rules will be impacted by the new application matches.

----- END -----

Day 10 Content ID

Zone Protection and Dos Protection

Security Profiles

-> Types of security profiles include:

1. **Antivirus:** Detects infected files being transferred with the application
2. **Anti-Spyware:** Detects spyware downloads and traffic from already installed spyware
3. **Vulnerability Protection:** Detects attempts to exploit known software vulnerabilities
4. **URL Filtering:** Classifies and controls web browsing based on content
5. **File Blocking:** Tracks and blocks file uploads and downloads based upon file type and application
6. **WildFire Analysis:** Forwards files to the WildFire Public Cloud, the WF-500 Private Appliance, or both.
7. **Data Filtering:** Looks for specific patterns of data in the traffic

-> URL Filtering

-> What is URL Filtering ?

-> URL Filtering Security Profile

-> URL Category vs. URL Filtering Security Profile

-> URL Filtering Sequence

 1. Block List

 2. Allow List

 3. Custom Categories

 4. URL Categories

-> URL Filtering Actions

-> URL Filtering Log

-> URL Filtering Service: Pan-DB

-> Configure to Access the PAN-DB Private Cloud

-> Recategorization Requests

WildFire

-> WildFire Public Cloud

-> WF-500 Private Appliance

-> WildFire Hybrid Cloud

WildFire Operation

WildFire Analysis Verdicts

- 1. Benign**
- 2. Grayware**
- 3. Malware (viruses, worms, Trojans, remote access tools (RATs), rootkits, and botnets)**
- 4. Fishing**

WildFire Analysis Profile

Threat Log

IP Exemption from the Threat Log

DoS Protection Profile:

- > DoS attack attempts to make network devices unreachable by disrupting services.
- > It attempt to disrupt network services by overloading network with unwanted traffic.
- > PAN-OS DoS protection features protect your firewall from all type of flooding attacks.
- > Its turn your network resources and devices from being exhausted or overwhelmed.
- > In the event of network floods, host sweeps, port scans and packet-based attacks.
- > Create DoS Protection profiles and policies to protect critical individual inside devices.
- > Or small groups of devices, internet-facing devices such as web and database servers.
- > The DoS protection profiles can be used to mitigate several types of DoS attacks.
- > Palo Alto Networks Firewalls provide Zone Protection and DoS Protection profiles.
- > Help to mitigate against flood attacks, reconnaissance activity & packet-based attacks.

Zone Protection Profiles:

- > In Palo Alto Network Firewall Zone protection policies allow use of flood protection.
- > Have the ability to protect against port scanning, sweeps and packet-based attacks.
- > In Palo Alto Firewall the Zone protection profiles may have less performance impact.
- > Zone Protection Profile are applied pre-session and don't engage the policy engine.
- > Apply only to new sessions in ingress zones & provide broad protection against flood.
- > Zone Protection Profile limiting the connections-Per-Second (CPS) to the PA Firewall.

- > Protection against reconnaissance, packet-based attacks & L2 protocol-based attacks.
- > It offers protection against floods, reconnaissance attacks & other packet-based attacks.
- > Zone protection is broad-based protection & is not designed to protect specific end host.
- > Zone protection profiles consist of five types of floods SYN, UDP, ICMP, ICMPv6, Other IP.
- > Zone protection policies can be aggregate only, but DoS Protection Profile can be both.

DoS Protection Profiles & Policy Rules:

- > Provide granular protection of specific, critical devices for the new sessions.
- > A major difference is a DoS policy can be classified policy or aggregate policy.
- > Classified policies protect individual devices by limiting the CPS for specific device.
- > Aggregate profile allows creation of max session rate for all packets matching policy.
- > The threshold applies to new session rate for all IPs combined for group of devices.
- > Once the threshold is triggered it would affect ALL the traffic matching the policy.

Aggregate:

- Apply DoS thresholds configured in profile to all packets that match rule criteria.
- Aggregate profile allows creation of a max session rate for all packets matching policy.
- Example, aggregate rule with a SYN flood threshold of 10000 pps counts all packets.

Classified:

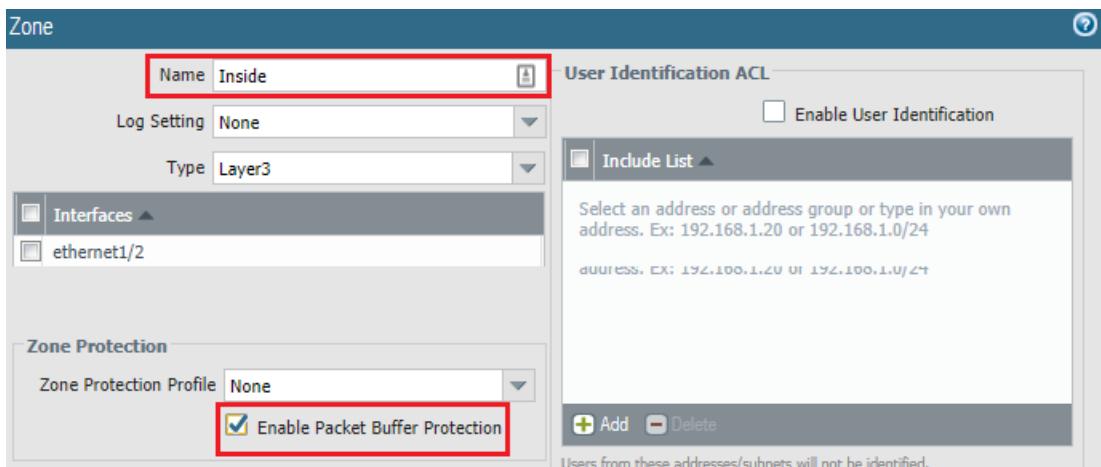
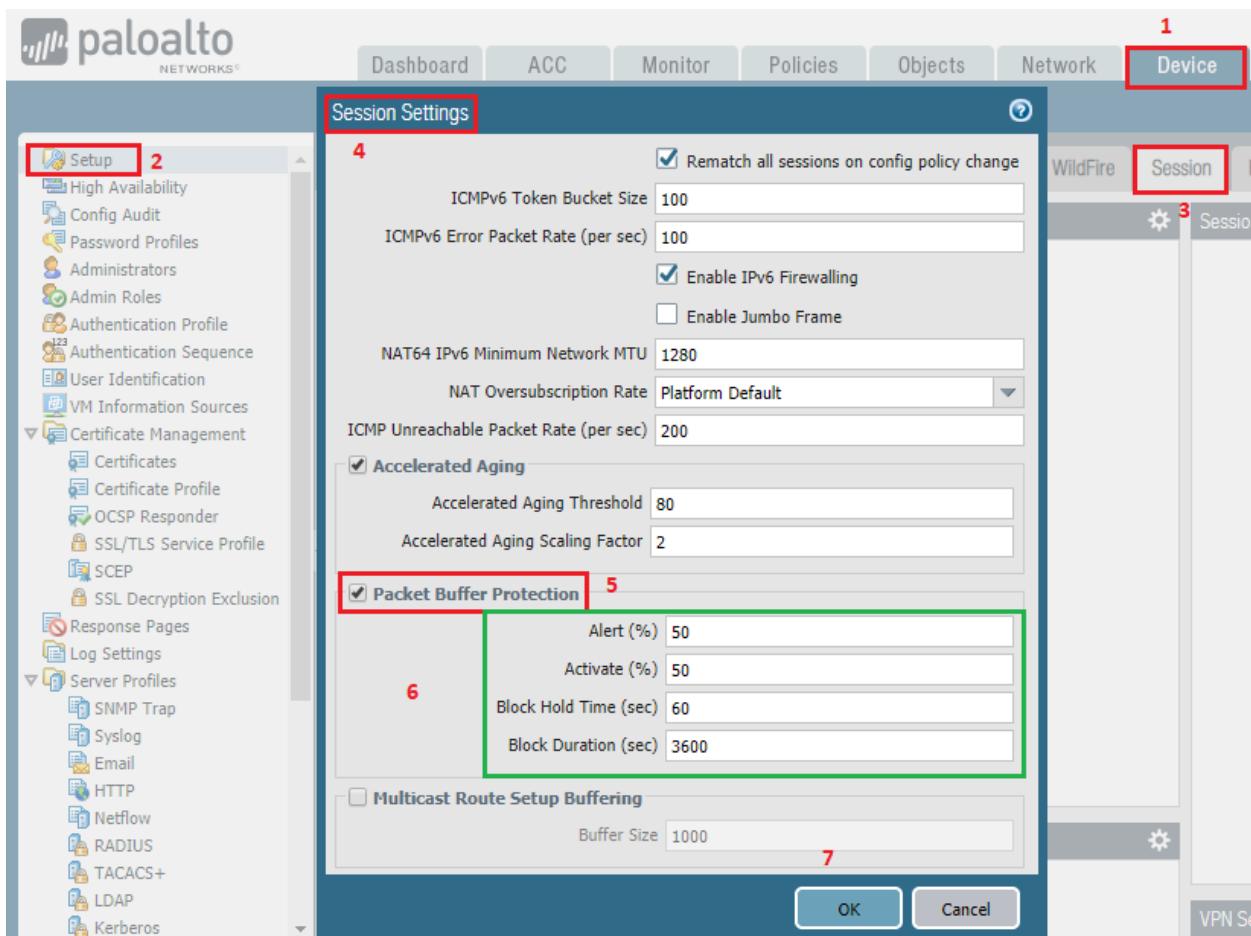
- Apply DoS thresholds configured in profile to all packets satisfying classification criteria.
- Classified example is such as the source IP, destination IP or source-and-destination IP.
- Classified profile allows the creation of a threshold that applies to a single source IP.

Packet Buffer Protection:

- A single session on a Firewall can consume packet buffers at a high volume.
- It defends your Firewall and network from the single session DoS attacks.
- It defends the Firewall from single session denial-of-service DoS attacks.
- That can overwhelm Firewall's packet buffer & cause legitimate traffic to drop.
- If zone protection on packet buffer is enabled, firewall monitor high buffer utilization.

Go to Device > Setup > Session : Session Settings enable Packet Buffer Protection & set values.

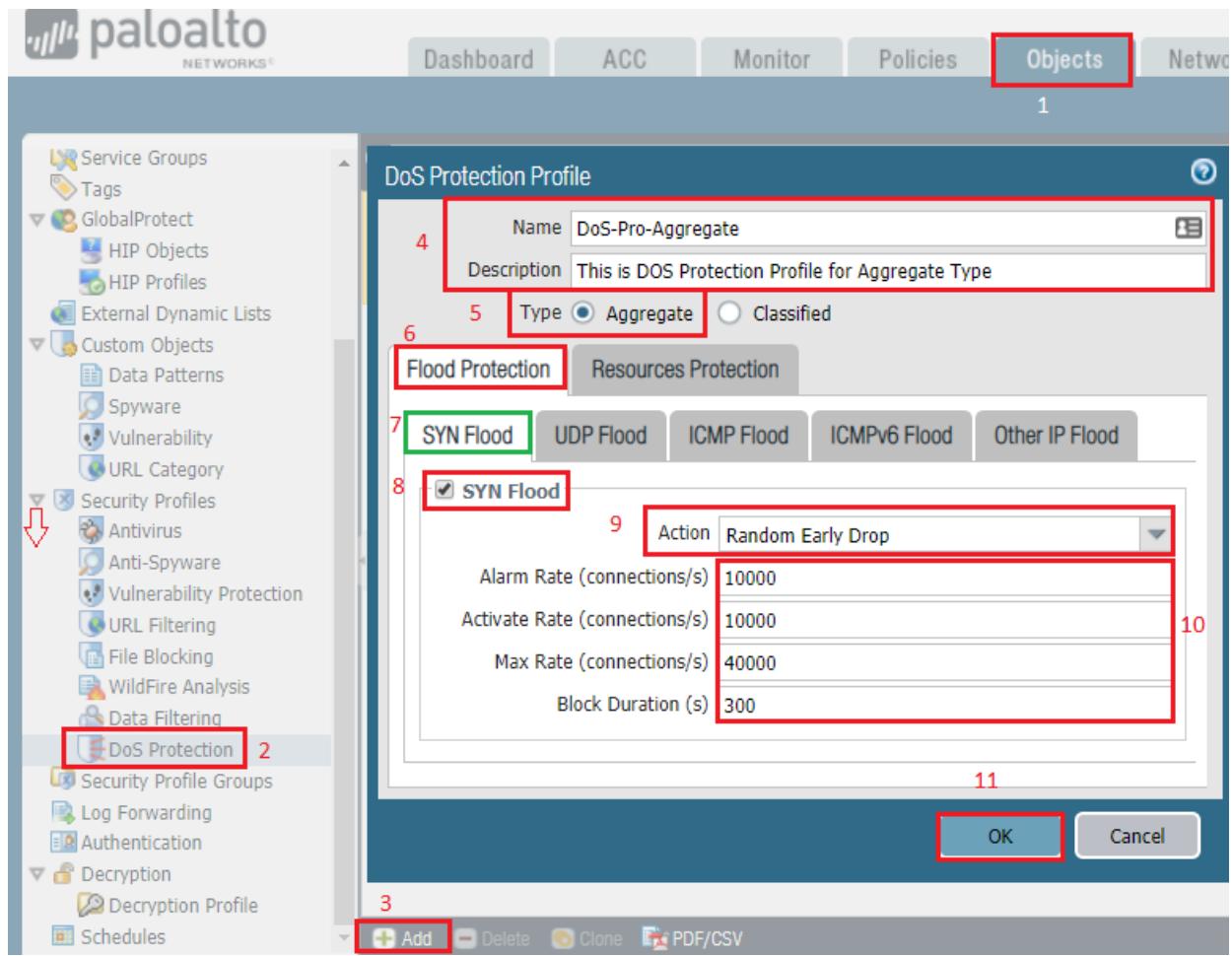
Go to Network > Zones tick Enable Packet Buffer Protection on every zone Inside, Outside etc.



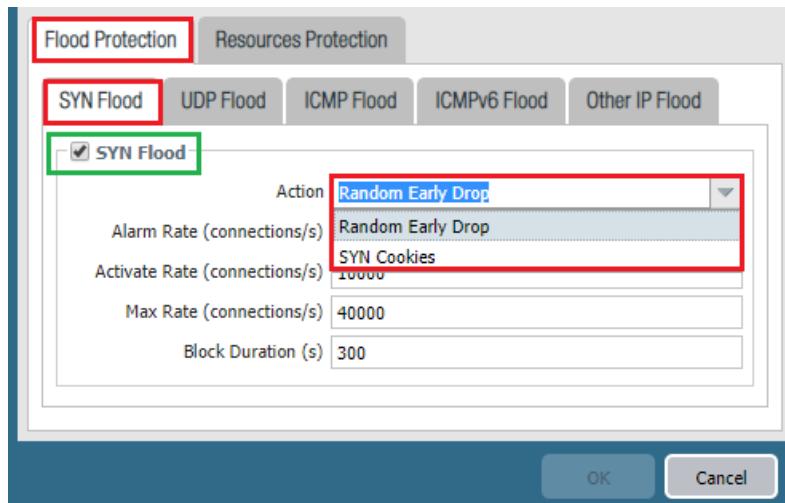
DoS Protection Profile:

Using DoS protection profiles, you can create DoS rules much like security policies, allowing traffic based on the configured criteria. These profiles are configured under the

Objects tab > Security Profiles > DoS Protection. Enter name, description and choose type of profile.



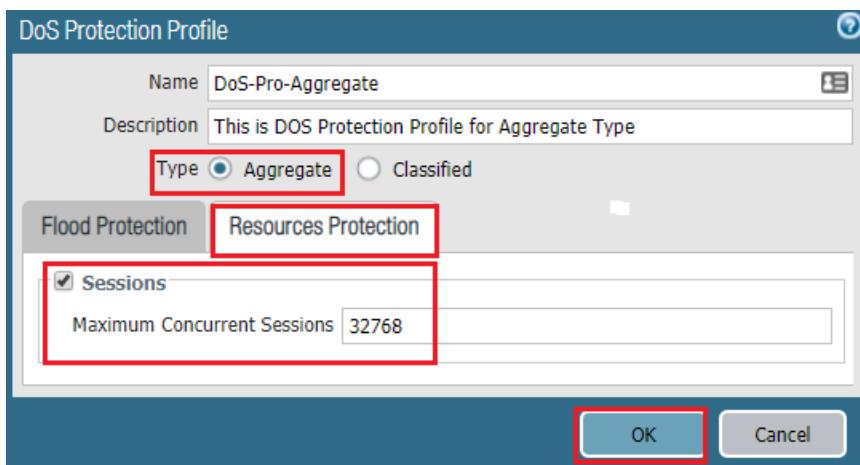
Go to Objects > Security Profiles > DoS Protection Flood Protection Tab.



Flood Protection Tab

SYN Flood tab	Enable type of flood protection indicated on the tab and specify settings: Action —(SYN Flood only) Action that the firewall performs. Random Early Drop —Drop packets randomly when connections per second reach the Activate Rate threshold.
UDP Flood tab	SYN cookies —Use SYN cookies to generate acknowledgments so that it is not necessary to drop connections during a SYN flood attack. Alarm Rate —Specify the threshold rate (CPS) to generate a DoS alarm (range is 0 to 2,000,000 cps; default is 10,000 CPS).
ICMP Flood tab	Activate Rate —Specify the threshold rate (cps) at which a DoS response is activated. Activate Rate range is 0 to 2,000,000 cps; default is 10,000 cps. Max Rate —Specify the threshold rate of incoming connections per second the firewall allows. At the Max Rate threshold, the firewall drops 100% of new connections (range is 2 to 2,000,000 cps; default is 40,000 cps.)
ICMPv6 tab	Block Duration —Specify the length of time (seconds) during which the offending IP address remains on the Block IP list and connections with IP address are blocked. Rate thresholds (range is 1 to 21,600 seconds; default is 300 seconds).
Other IP tab	

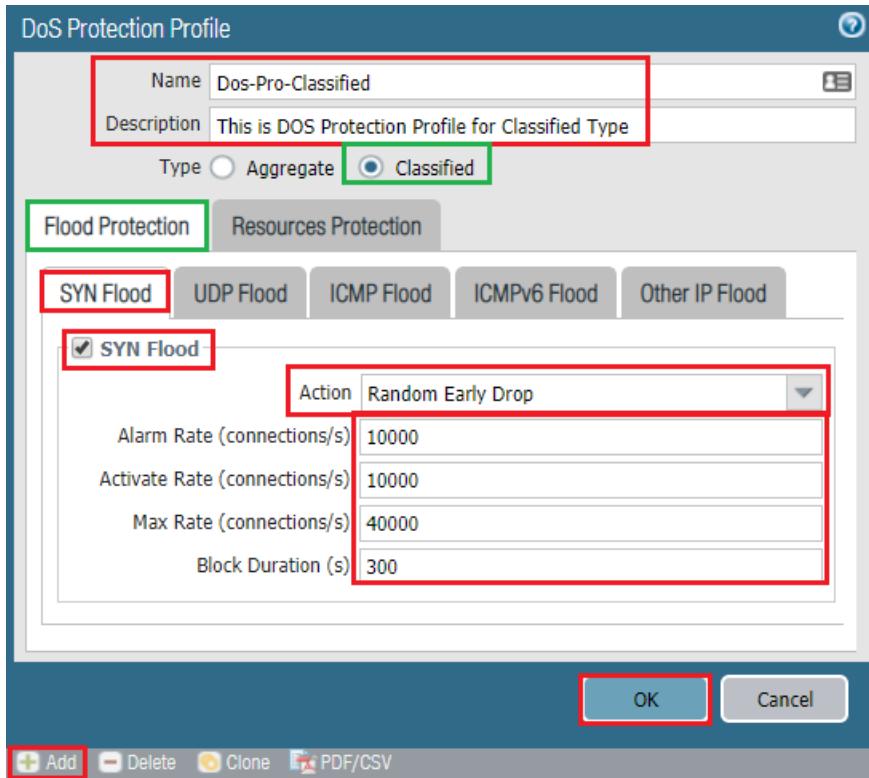
Go to Objects > Security Profiles > DoS Protection Resources Protection Tab.



Resources Protection Tab

Sessions	Select this option to enable resources protection.
Max Concurrent Limit	Specify the maximum number of concurrent sessions.

Go to Objects > Security Profiles > DoS Protection choose type Classified this time.

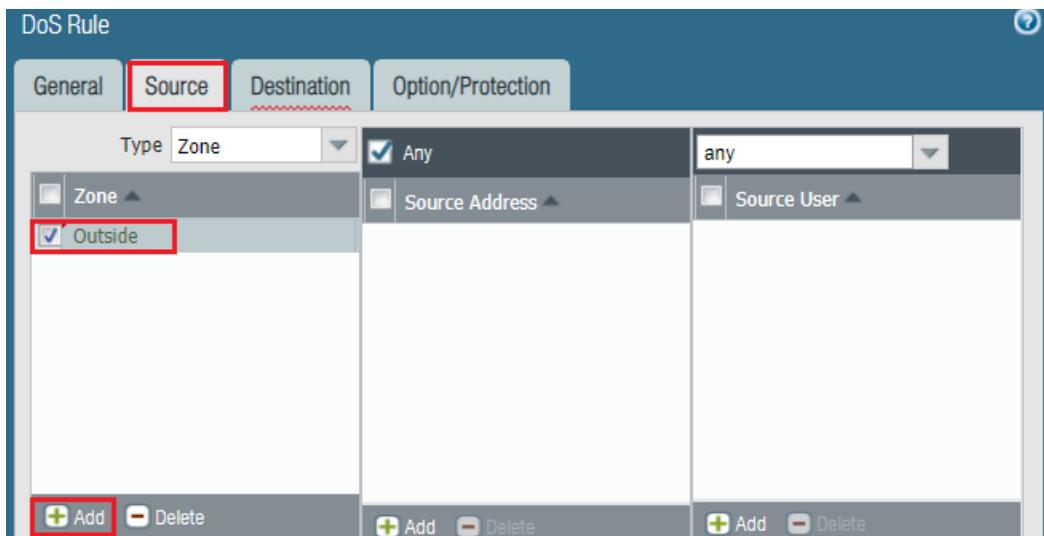
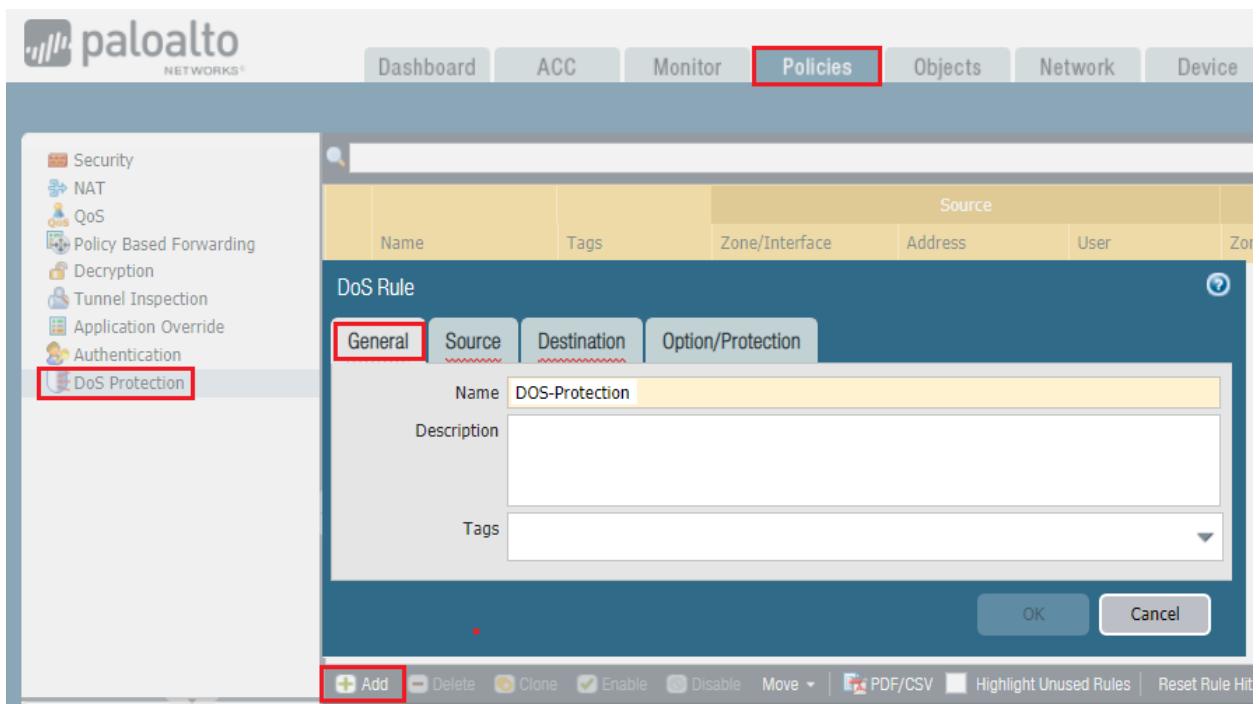


Finally, we created two different type of DoS protection Profiles, Aggregate & Classified.

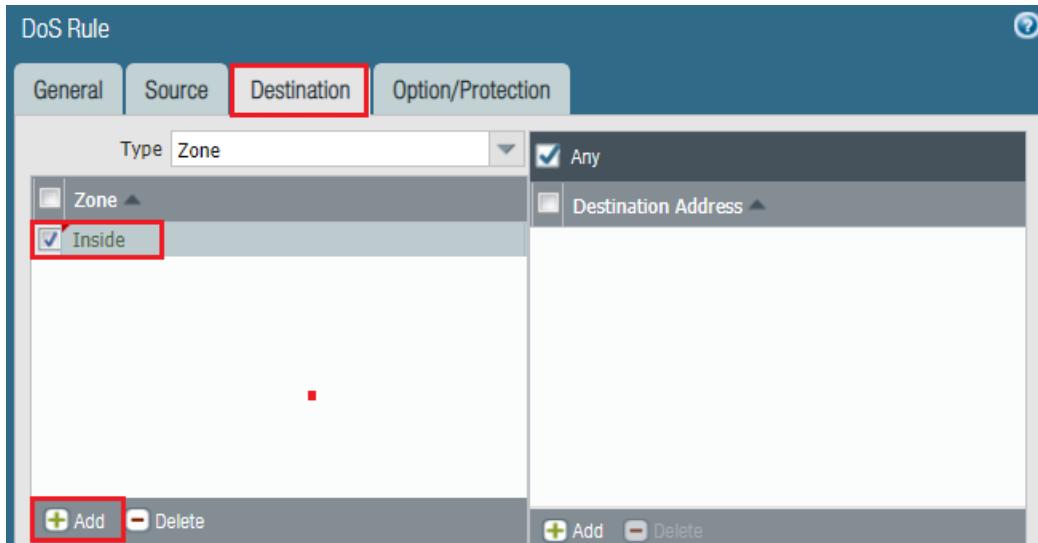
Name	Type	Flood Protection					Resources Protection	
		SYN Flood	UDP Flood	ICMP Flood	ICMPv6 Flood	Other IP Flood	Sessions	
<input type="checkbox"/> Dos-Pro-Aggregate	aggregate	<input checked="" type="checkbox"/>						
<input checked="" type="checkbox"/> Dos-Pro-Classified	classified	<input checked="" type="checkbox"/>						

Next we'll go to Policies > DoS Protection to create a DoS policy similar to the way we create a security rule. Enter a name to identify the rule.

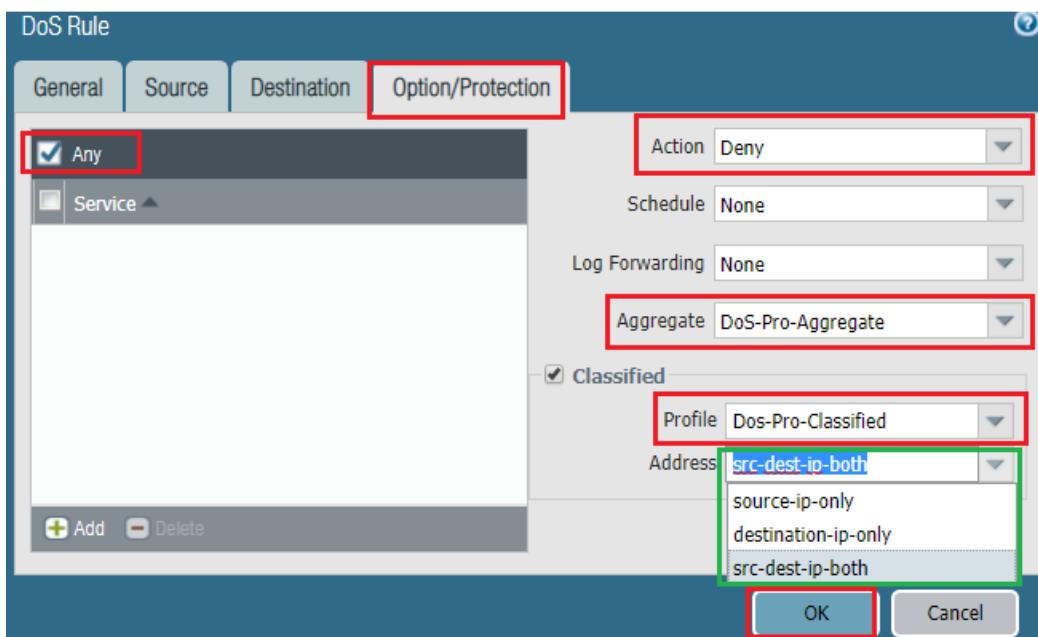
Select the Source tab to define the source interface(s) or source zone(s), & optionally source address(es) & source user(s) that define incoming traffic to which DoS policy rule applies.



Select the Destination tab to define the destination zone or interface and destination address that define the destination traffic to which the policy applies.

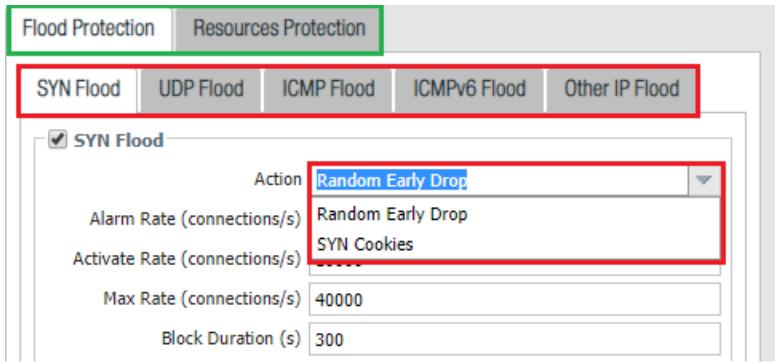


Select the Option/Protection tab to configure options for the DoS Protection policy rule.



Finally, the DoS Protection Policy rule look like below.

Name	Tags	Source			Destination	
		Zone/Interface	Address	User	Zone/Interface	Address
1 DOS-Protection	none	Outside	any	any	Inside	any



SYN Random Early Drop:

- This feature causes SYN packets to be dropped to mitigate a flood attack early.
- When flow exceeds Activate rate threshold, Firewall drops SYN packets randomly.
- When flow exceeds Maximum rate threshold, 100% of incoming SYN packets dropped.

SYN Cookies:

- The PA Network Firewall acts as man-in-the-middle for the TCP handshake.
- Firewall does sequence number translation for active legitimate session.
- SYN Cookies alarms can be viewed in the threat logs or dashboard in PA.

UDP Flood:

- UDP is activated when number of UDP packets zone receives per second is reached.
- Firewall uses an algorithm to progressively drop more packets as attack rate increase.
- The Palo Alto Network Firewall drop packets until the rate reaches the Maximum rate.
- Firewall stops dropping UDP packets if incoming rate drops below Activate threshold.

ICMP Flood:

- ICMP is activated when number of ICMP packets zone receives per second is reached.
- Firewall uses an algorithm to progressively drop more packets as attack rate increases.
- The Palo Alto Network Firewall drop packets until the rate reaches the Maximum rate.
- Firewall stops dropping ICMP packets if incoming rate drops below Activate threshold.

Other IP Flood:

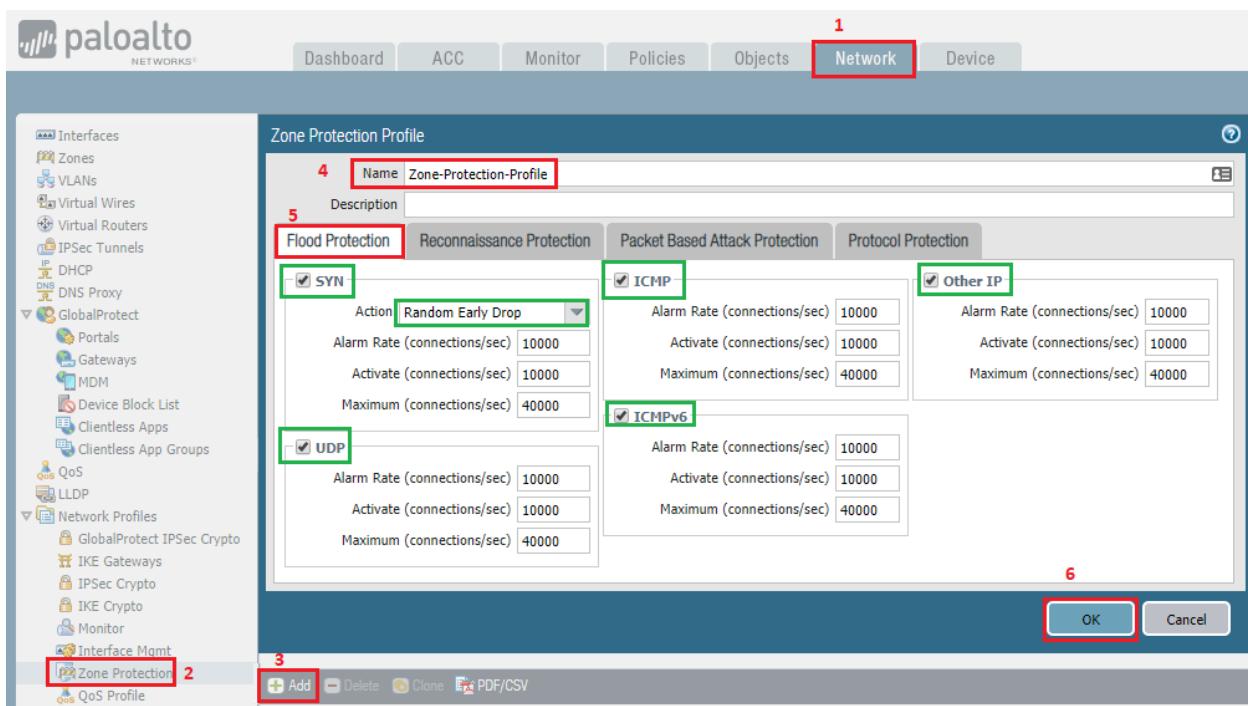
- Other IP is activated when number of other IP packets non-TCP, ICMP & UDP packets.
- Firewall uses an algorithm to progressively drop more packets as attack rate increases.
- The Palo Alto Network Firewall drop packets until the rate reaches the Maximum rate.
- Firewall stops dropping ICMP packets if incoming rate drops below Activate threshold.

Reconnaissance Protection:

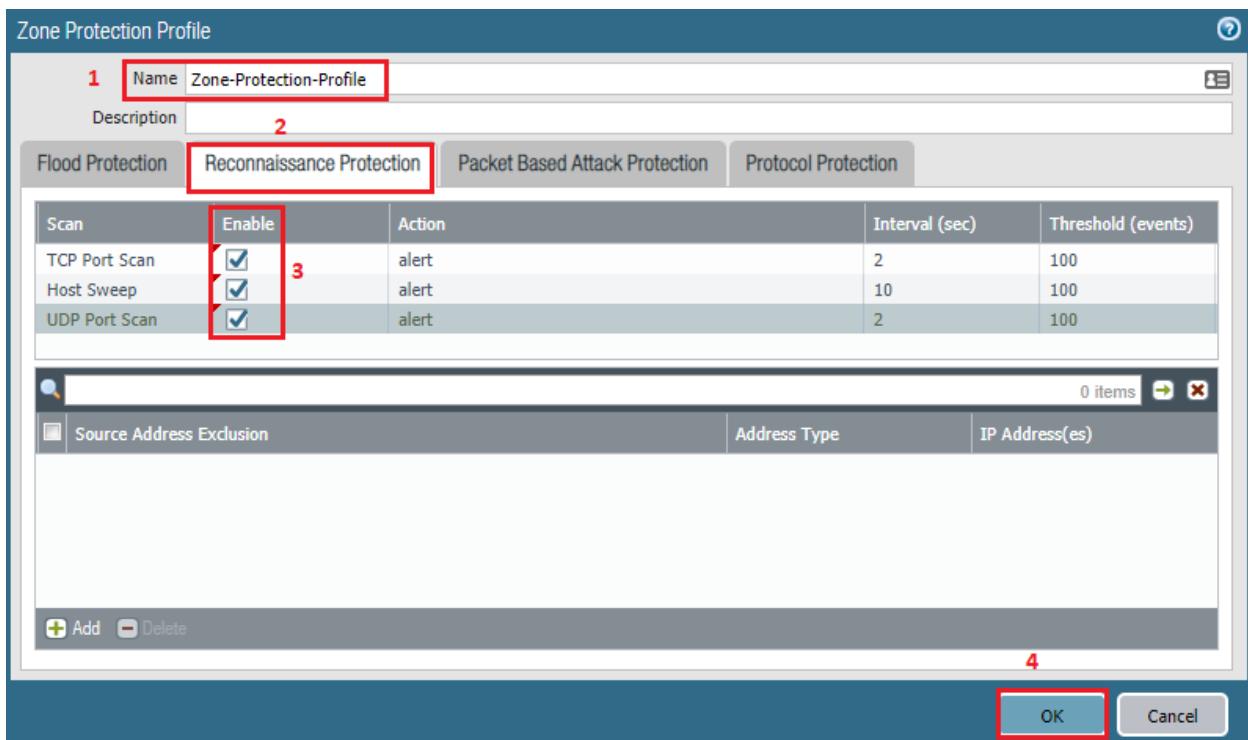
- Palo Alto Firewall reconnaissance protection protects against reconnaissance attacks.
- Reconnaissance attack is the first type of attacks within a Cyber-Attack Lifecycle.

Zone Protection:

Go to Network > Network Profiles > Zone Protection Enter a profile name.



Network > Network Profiles > Zone Protection > Reconnaissance Protection tab.



Settings	Description
TCP Port Scan	Enable configures profile to enable protection against TCP port scans.
UDP Port Scan	Enable configures profile to enable protection against UDP port scans.
Host Sweep	Enable configures profile to enable protection against host sweeps.

Action	Action system take in response to corresponding reconnaissance attempt: Allow —Permits the port scan or host sweep reconnaissance. Alert —Generates an alert for each port scan or host sweep that matches the threshold within the specified time interval (the default action). Block —Drops all subsequent packets from the source to the destination for the remainder of the specified time interval. Block IP —Drops all subsequent packets for specified Duration, in seconds.
Interval (sec)	Time interval, in seconds, for TCP or UDP port scan detection (range is 2-65,535; default is 2). Time interval, in seconds, for host sweep detection (range is 2-65,535; default is 10).
Threshold (events)	Number of scanned port events or host sweep events within the specified time interval that triggers the Action (range is 2-65,535; default is 100).
Source Address Exclusion	IP addresses whitelisted from the reconnaissance protection.

Network > Network Profiles > Zone Protection > Packet Based Attack Protection.

Zone Protection Profile

1 Name: Zone-Protection-Profile

2 Description:

Flood Protection Reconnaissance Protection **Packet Based Attack Protection** Protocol Protection

IP Drop TCP Drop ICMP Drop IPv6 Drop ICMPv6 Drop

3 Spoofed IP address
 Strict IP Address Check
 Fragmented traffic

IP Option Drop

<input type="checkbox"/> Strict Source Routing	<input type="checkbox"/> Security
<input type="checkbox"/> Loose Source Routing	<input type="checkbox"/> Stream ID
<input type="checkbox"/> Timestamp	<input type="checkbox"/> Unknown
<input type="checkbox"/> Record Route	<input type="checkbox"/> Malformed

4

5

OK Cancel

Settings	Description
Spoofed IP address	Discard packets with a spoofed IP address.
Strict IP Address Check	Discard packets with malformed source or destination IP addresses.
Fragmented traffic	Discard fragmented IP packets.
IP Option Drop	Select the settings in this group to enable the firewall to drop packets containing these IP Options.
Strict Source Routing	Discard packets with the Strict Source Routing IP option set.
Loose Source Routing	Discard packets with the Loose Source Routing IP option set.
Timestamp	Discard packets with the Timestamp IP option set.
Record Route	Discard packets with the Record Route IP option set.
Security	Discard packets if the security option is defined.
Stream ID	Discard packets if the Stream ID option is defined.
Unknown	Discard packets if the class and number are unknown.
Malformed	Discard packets if they have incorrect combinations of class, number, and length based on Discard malformed packets.

Network > Network Profiles > Zone Protection > Packet Based Attack Protection > TCP Drop Tab.

The screenshot shows the 'Zone Protection Profile' dialog box. The 'Name' field is set to 'Zone-Protection-Profile'. The 'Description' field contains the number '1'. The tabs at the top are 'Flood Protection', 'Reconnaissance Protection', 'Packet Based Attack Protection' (which is highlighted with a red box), and 'Protocol Protection'. Below these tabs, there are five sub-tabs: 'IP Drop', 'TCP Drop' (which is highlighted with a red box), 'ICMP Drop', 'IPv6 Drop', and 'ICMPv6 Drop'. A large green box encloses the 'TCP Drop' sub-tab area. Inside this green box, the 'TCP Drop' tab has several options listed with checkboxes: 'Mismatched overlapping TCP segment' (unchecked), 'Split Handshake' (unchecked), 'TCP SYN with Data' (checked), and 'TCP SYNACK with Data' (checked). Below these are two dropdown menus: 'Reject Non-SYN TCP' set to 'global' and 'Asymmetric Path' set to 'global'. Another green box encloses the 'Strip TCP Options' section, which contains 'TCP Timestamp' and 'TCP Fast Open' checkboxes (both unchecked) and a 'Multipath TCP (MPTCP) Options' dropdown set to 'global'. The bottom right of the dialog box has 'OK' and 'Cancel' buttons, with the 'OK' button highlighted with a red box. Red numbers 2, 3, and 4 are overlaid on the image to point to specific sections: 2 points to the 'TCP Drop' sub-tab, 3 points to the 'Reject Non-SYN TCP' dropdown, and 4 points to the 'OK' button.

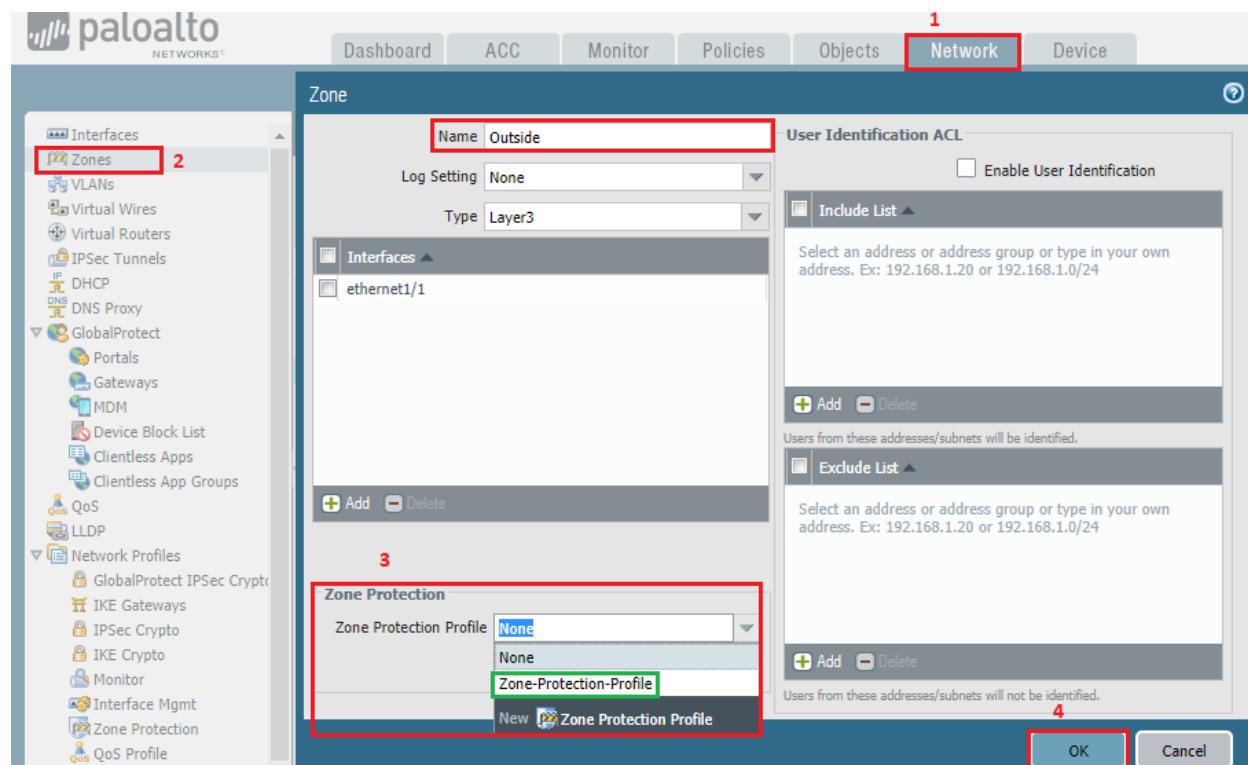
Settings	Description
Mismatched overlapping TCP segment	Attackers construct connections with overlapping but different data in them to cause misinterpretation of the connection. Attackers can use IP spoofing & sequence number prediction to intercept a user's connection.
Split Handshake	Prevent TCP session from being established if the session establishment procedure does not use well-known three-way handshake.
TCP SYN with Data	Prevent a TCP session from being established if the TCP SYN packet contains data during a three-way handshake. Enabled by default.
TCP SYNACK with Data	Prevent a TCP session from being established if the TCP SYN-ACK packet contains data during a three-way handshake. Enabled by default.
Reject Non-SYN TCP	Determine whether to reject the packet if the first packet for the TCP session setup is not a SYN packet.
Asymmetric Path	Determine whether to drop or bypass packets that contain out-of-sync ACKs or out-of-window sequence numbers
Strip TCP Options	Determine whether to strip the TCP Timestamp or TCP Fast Open option from TCP packets.
TCP Timestamp	Determine whether the packet has a TCP timestamp in the header and, if it does, strip the timestamp from the header.
TCP Fast Open	Strip the TCP Fast Open option (and data payload, if any) from the TCP SYN or SYN-ACK packet during a TCP three-way handshake
Multipath TCP (MPTCP) Options	MPTCP is an extension of TCP that allows a client to maintain a connection by simultaneously using multiple paths to connect to the destination host. By default, Disable.

Network > Network Profiles > Zone Protection > Packet Based Attack Protection > ICMP Drop.

The screenshot shows the 'Zone Protection Profile' configuration window. The 'Name' field is set to 'Zone-Protection-Profile'. The 'Description' field is empty. The 'Packet Based Attack Protection' tab is selected, indicated by a red box and the number '1' above it. Below this tab, the 'ICMP Drop' sub-tab is also selected, indicated by a red box and the number '2' above it. A green box highlights the list of ICMP drop options under the 'ICMP Drop' tab, with the number '3' to its left. The options listed are: 'ICMP Ping ID 0', 'ICMP Fragment', 'ICMP Large Packet(>1024)', 'Discard ICMP embedded with error message', 'Suppress ICMP TTL Expired Error', and 'Suppress ICMP Frag Needed'. At the bottom right, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted by a red box and the number '4' above it.

Setting	Description
ICMP Ping ID 0	Discard packets if the ICMP ping packet has an identifier value of 0.
ICMP Fragment	Discard packets that consist of ICMP fragments.
ICMP Large Packet (>1024)	Discard ICMP packets that are larger than 1024 bytes.
Discard ICMP embedded with error message	Discard ICMP packets that are embedded with an error message.
Suppress ICMP TTL Expired Error	Stop sending ICMP TTL expired messages.
Suppress ICMP Frag Needed	Stop sending ICMP fragmentation needed messages in response to packets that exceed interface MTU & have do not fragment bit set.

Apply the Zone protection Profile to the Zone wanted by going to Network > Zones. Click the Zone, for example "Outside," to add the Zone Protection Profile and select it from the drop-down menu in the Zone Protection Profile. Once has been selected, click OK.



Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection
DMZ	layer3	ethernet1/2	Zone-Protection-Profile	<input checked="" type="checkbox"/>
Inside	layer3	vlan.1 vlan.2	Zone-Protection-Profile	<input checked="" type="checkbox"/>
Outside	layer3	ethernet1/1	Zone-Protection-Profile	<input checked="" type="checkbox"/>

Now Let's check ICMP Flood logs, go to Monitor > Logs>Threat

The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor (which is highlighted with a red box), Policies, Objects, Network, and Device. On the left, there's a sidebar with categories like Logs, Traffic, Threat (highlighted with a red box), URL Filtering, WildFire Submissions, Data Filtering, HIP Match, User-ID, Tunnel Inspection, Configuration, System, and Alarms. The main content area displays a table of logs. The columns are: Receive Time, Type, Name, From Zone, To Zone, Source address, Destination address, To Port, Application, Action, and Severity. The logs show multiple entries for 'flood' type events named 'ICMP Flood' occurring at various times on the same day, all categorized as 'critical' severity.

	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity
	01/28 10:45:32	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical
	01/28 10:45:22	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical
	01/28 10:45:11	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical
	01/28 10:45:00	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical
	01/28 10:44:51	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical
	01/28 10:44:41	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical

Go back to Network > Network Profiles > Zone Protection>>Reconnaissance Protection tab.

The screenshot shows the 'Zone Protection Profile' configuration screen. The 'Name' field is set to 'Zone-Protection-Profile' (highlighted with a red box). The 'Description' field is empty. Below these, there are four tabs: Flood Protection, Reconnaissance Protection (highlighted with a red box), Packet Based Attack Protection, and Protocol Protection. Under the 'Reconnaissance Protection' tab, there is a table for 'Scan' types. It lists three items: 'TCP Port Scan' (checked), 'Host Sweep' (checked), and 'UDP Port Scan' (checked). The 'Action' column for all three is 'alert'. The 'Interval (sec)' and 'Threshold (events)' columns are also visible. At the bottom right, there are 'OK' and 'Cancel' buttons, with 'OK' highlighted with a red box.

Now Let's check TCP/UDP Port Scan logs, go to Monitor > Logs>Threat

The screenshots show three separate log tables under the 'Threat' category in the 'Logs' section. The first table shows UDP Port Scan logs. The second table shows TCP Port Scan logs. The third table shows a mix of ICMP Flood and Host Sweep logs. All logs are categorized as 'medium' severity.

	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity
	01/28 10:55:51	scan	SCAN: UDP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	24921	not-applicable	alert	medium
	01/28 10:55:39	scan	SCAN: UDP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	26987	not-applicable	alert	medium
	01/28 10:55:24	scan	SCAN: UDP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	19197	not-applicable	alert	medium
	01/28 10:54:54	scan	SCAN: UDP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	27473	not-applicable	alert	medium

	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity
	01/28 11:02:37	scan	SCAN: TCP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	1187	not-applicable	alert	medium
	01/28 11:00:38	scan	SCAN: TCP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	2718	not-applicable	alert	medium
	01/28 10:59:36	scan	SCAN: TCP Port Scan	Inside	Outside	192.168.78....	192.168.17.150	6580	not-applicable	alert	medium

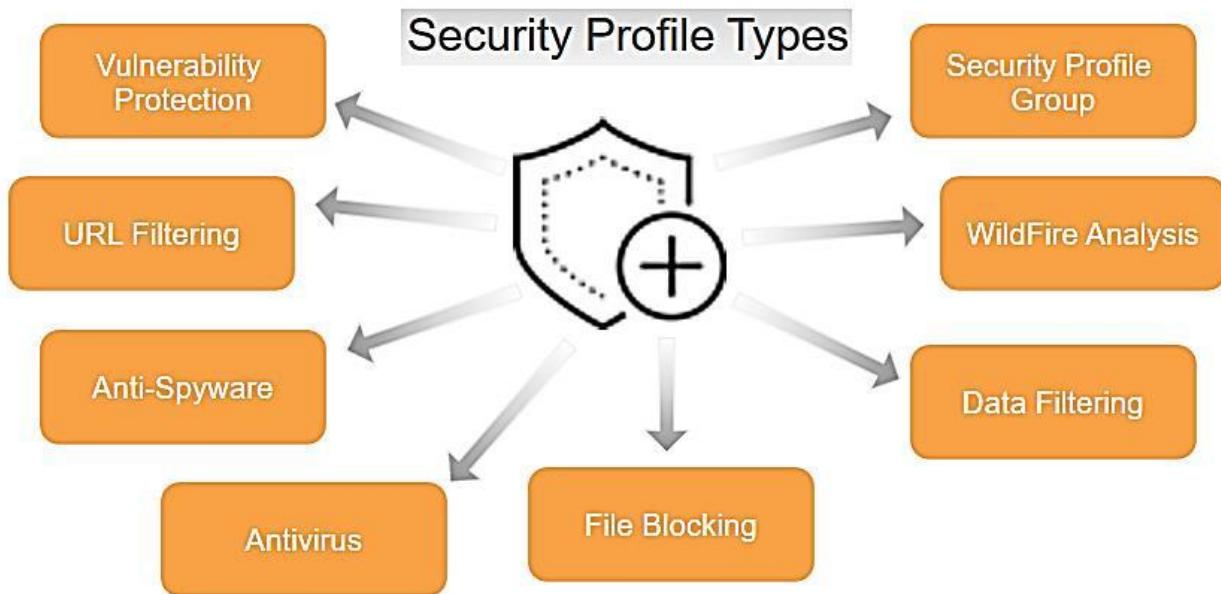
	Receive Time	Type	Name	From Zone	To Zone	Source address	Destination address	To Port	Application	Action	Severity
	01/28 11:17:12	flood	ICMP Flood	Inside	Inside	0.0.0.0	0.0.0.0	0	not-applicable	drop	critical
	01/28 11:17:07	scan	SCAN: Host Sweep	Inside	Outside	192.168.78....	192.168.17.106	0	not-applicable	alert	medium
	01/28 11:17:05	scan	SCAN: Host Sweep	Inside	Outside	192.168.78....	192.168.17.99	443	not-applicable	alert	medium

Security Profile Groups:

Security Profile Group Simplified use of security profiles within security policies. Security Profile Group placing our different security profiles into the groups. By creating Security Profile Group Security Policies call single security profile group. The Palo Alto Network Firewall supports the ability to create Security Profile groups. Specify sets of Security Profiles that treated as unit & then added to security policies.

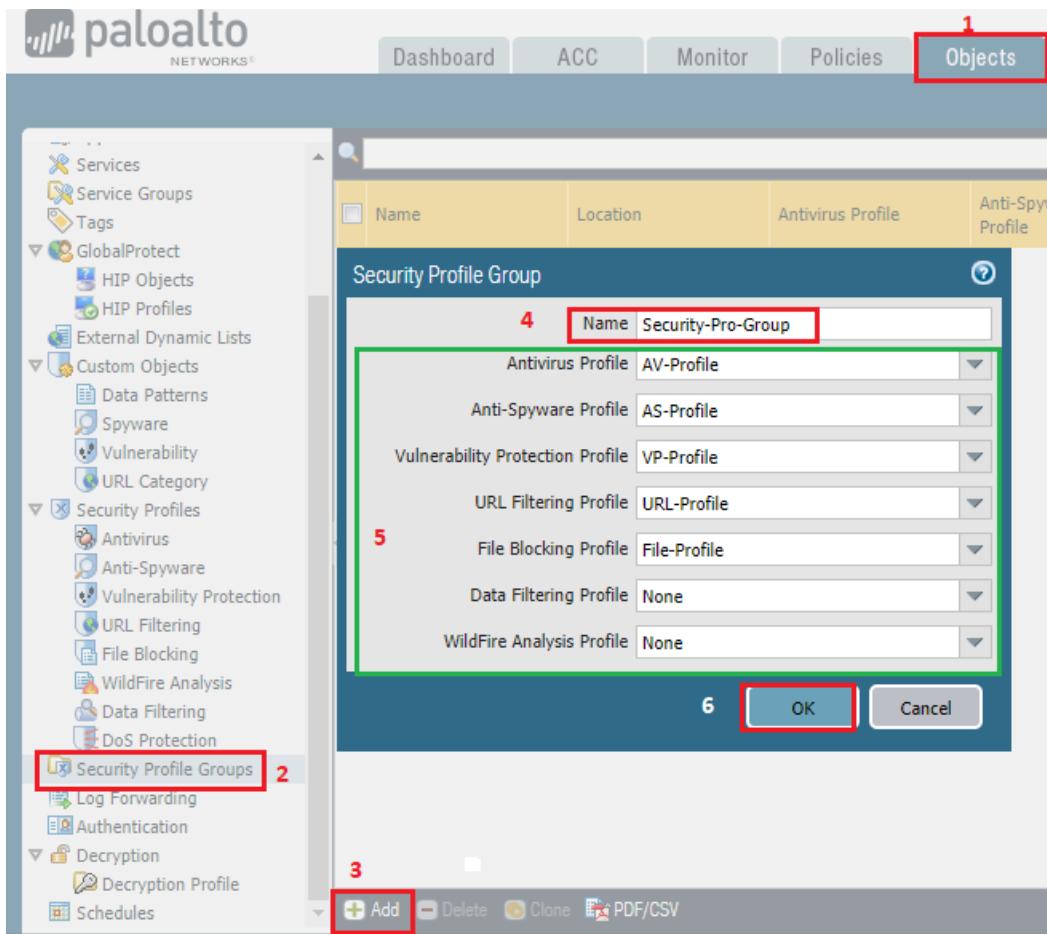
Navigate to Objects > Security Profile Groups, click Add at bottom of window to make.

Security Profile Group can be created includes one or more security profiles. Which simplifies the task of adding security profiles to a security policy rule. Security profiles scan security policies that have an action set to Allow only. The most commonly used security profiles are Antivirus, and Anti-Spyware. Also, most commonly used Vulnerability Protection, URL Filtering, and WildFire.



Select Objects>Security Profile Groups and Add a new security profile group.

Give the profile group a descriptive Name , for example, in my case Security-Pro-Group. Add existing profiles to the group. Click OK to save the profile group.



Finally, after created Security Profile Groups will look like below.

Name	Location	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile	URL Filtering Profile	File Blocking Profile
<input checked="" type="checkbox"/> Security-Pro-Group		AV-Profile	AS-Profile	VP-Profile	URL-Profile	File-Profile

Select Policies>Security and Add or modify a security policy rule. Select the Actions tab. In the Profile Setting section, select Group for the Profile Type. In the Group Profile drop-down, select the group you created. Click OK to save the policy and Commit your changes.

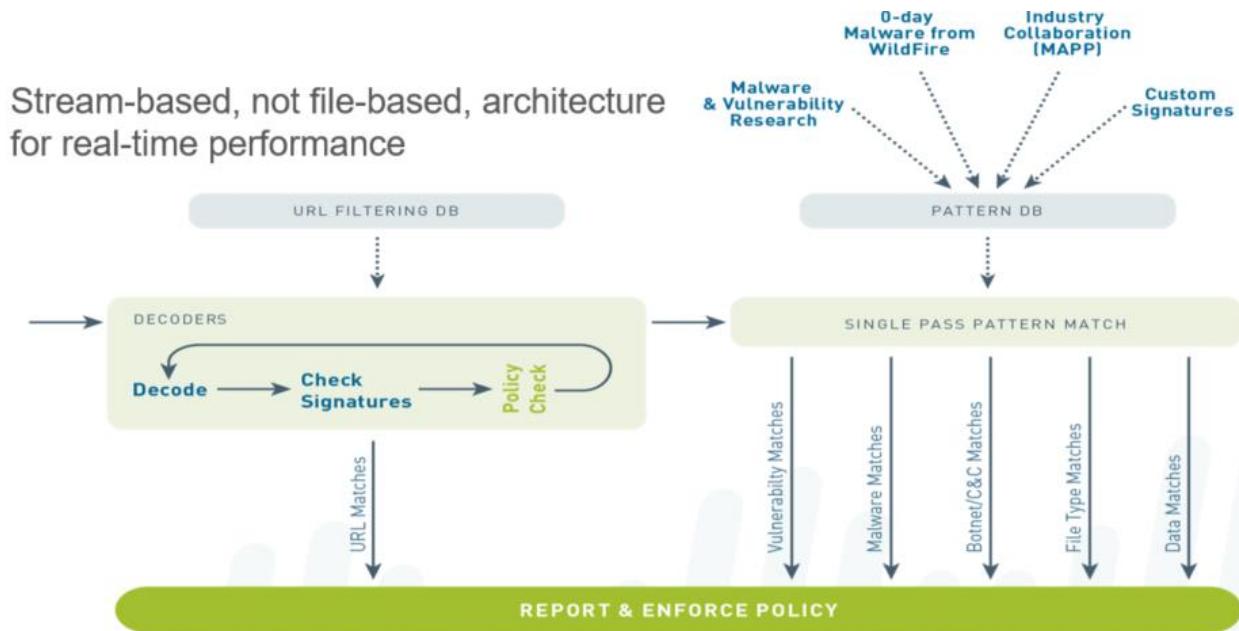
Security Policy Rule

General	Source	User	Destination	Application	Service/URL Category	Actions
Action Setting 2 Action Allow <input type="checkbox"/> Send ICMP Unreachable						Log Setting 1 <input checked="" type="checkbox"/> Log at Session Start <input type="checkbox"/> Log at Session End Log Forwarding None
Profile Setting Profile Type Group Group Profile Security-Pro-Group						Other Settings 3 Schedule None QoS Marking None <input type="checkbox"/> Disable Server Response Inspection
4 <input type="button" value="OK"/> <input type="button" value="Cancel"/>						

Finally, it shows like below Security Profile Group is attached to Allow Policy rule.

	Name	Type	Source		Destination	Rule Usage	Application	Service	Action	Profile
1	Inside-to-Outside	universal	Inside Outside		Inside Outside	25097576	any		Allow	
2	Inside-To-Outside	universal	Inside		Outside	0	any		Allow	none

Content-ID:



Content-ID combines a real-time threat prevention engine with a comprehensive URL database. Content-ID uses some of the same elements of App-ID to limit unauthorized data and file transfers, detect and block a wide range of threats, and control non-work-related web surfing.

Advantages of Content-ID include:

- A stream-based (not file-based) architecture for real-time performance
- The ability to block transfer of sensitive data and file transfers by type
- URL filtering capability enabled via a fully-integrated URL Database
- The ability to detect zero-day attacks with WildFire

Note: The first arrow on the left side in the diagram refers to traffic that has been matched to a security policy with an action of allow that has one or more security profiles attached to it.

For additional information about threat prevention in PAN-OS, refer to the Threat Prevention Deployment Tech Note available on the support website.

Security Profiles:

Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile
RestrictYouTube	universal	Trust-L3	any	any	Untrust-L3	any	youtube	application-default	✓	
Disable-FB	universal	Trust-L3	any	...	Untrust-L3	any	facebook-base	application-default	✗	none
General Access	universal	Trust-L3	any	any	Untrust-L3	any	any	any	✓	

Threat License Required

Antivirus

URL Filtering
URL Filtering License Required

Anti-Spyware

File Blocking

Vulnerability

WildFire Analysis
WildFire License Required

Security Profile Group

Data Filtering

Security profiles are objects that are added to security policies with the “allow” action. Profiles are not necessary for security policies with the “deny” action because no further processing is needed if the packet is to be dropped. As with policies, profiles are applied to all packets over the life of a session.

The profiles represent additional security checks to be performed on the allowed traffic. They look for improper or malicious use of applications that are allowed in the environment. For example, web browsing may be allowed, but there is still worry that users can download a virus from a website. The security policy allows web browsing, and an antivirus profile is added to detect and react to viruses.

Types of security profiles include:

- **Antivirus:** Detects infected files being transferred with the application

- **Anti-Spyware:** Detects spyware downloads and traffic from already installed spyware
- **Vulnerability Protection:** Detects attempts to exploit known software vulnerabilities
- **URL Filtering:** Classifies and controls web browsing based on content
- **File Blocking:** Tracks and blocks file uploads and downloads based upon file type and application
- **WildFire Analysis:** Forwards files to the WildFire Public Cloud, the WF-500 Private Appliance, or both.
- **Data Filtering:** Looks for specific patterns of data in the traffic

Antivirus Security Profile:

Objects > Security Profiles > Antivirus

Decoder	Action	WildFire Action
imap	default (alert)	default (alert)
pop3	default (alert)	default (alert)
smtp	default (alert)	default (alert)
ftp	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)
smb	default (reset-both)	default (reset-both)

The Antivirus security profile defines actions to be taken if an infected file is detected as part of an application. The listed applications represent the wide variety of vectors that modern viruses can take in infecting a system. For each application type an action can be defined.

If a virus is detected, the default action is to “reset-both”, which equals a drop action if UDP. If TCP, the action resets the server and the client.

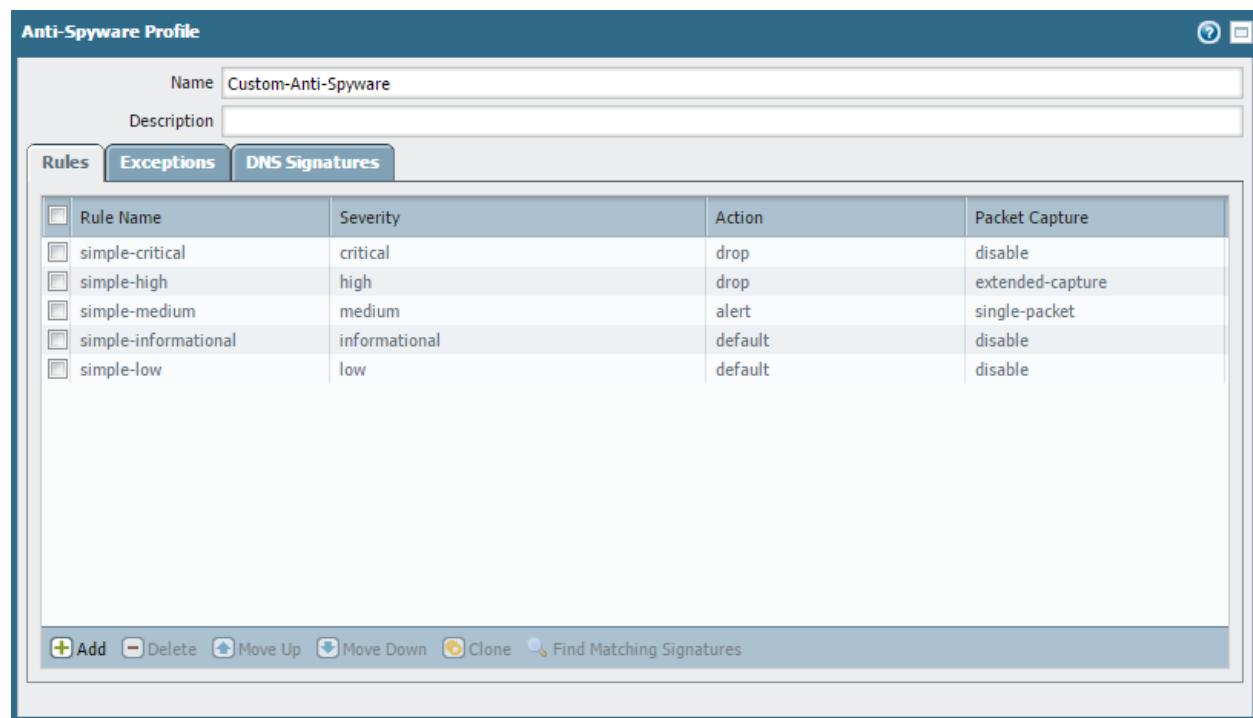
If the decoder is either IMAP or POP3, the default action is to “alert”. These protocols are store-and-forward protocols: if an intermediate device drops the packets, POP3 and IMAP are designed to continually resend until the data is ultimately delivered. For these kinds of applications, the infected file needs to be removed at either the server or the client, not on the wire.

If the decoder is SMTP the default action is also to “alert”, however, an SMTP 541 error message is sent as part of the reset action when a virus is detected. This message tells the mail server not to retry sending the message, which allows the firewall to drop the mail without the mail server trying to resend.

The Actions column configures the action taken if the infected file is identified by the firewall antivirus definitions file. The WildFire Action column defines the action taken if the infected file is matched against the threat list maintained by the WildFire subscription feature, which is discussed later in this module. When the action is set to “alert”, no traffic is blocked. The only action taken is to generate an entry in the threat log. By selecting the Packet Capture check box, any alert is also accompanied by a packet capture of the portion of the file that triggered the virus signature. This capture can be used to verify the presence of the virus and rule out false positives.

Anti-Spyware Security Profile:

Objects > Security Profiles > Anti-Spyware



The screenshot shows the 'Anti-Spyware Profile' configuration window. At the top, there are fields for 'Name' (set to 'Custom-Anti-Spyware') and 'Description'. Below these are three tabs: 'Rules' (selected), 'Exceptions', and 'DNS Signatures'. The 'Rules' tab displays a table of five rules:

Rule Name	Severity	Action	Packet Capture
simple-critical	critical	drop	disable
simple-high	high	drop	extended-capture
simple-medium	medium	alert	single-packet
simple-informational	informational	default	disable
simple-low	low	default	disable

At the bottom of the table are buttons for 'Add', 'Delete', 'Move Up', 'Move Down', 'Clone', and 'Find Matching Signatures'.

A security policy can include specification of an anti-spyware profile for “phone home” detection (detection of traffic from installed spyware). The firewall includes two predefined anti-spyware security profiles:

- **Default:** The profile applies the default action to all client and server critical, high, and medium severity spyware events. This profile is typically used for Proof of Concept (POC) or first-phase deployments.
- **Strict:** The profile applies the block response to all client and server critical-, high-, and medium-severity spyware events and uses the default action for low and informational spyware events. Strict profiles are used for out-of-the-box protection with recommended block of critical, high, and medium threats.

These predefined profiles cannot be modified or deleted.

DNS Sinkhole Configuration:

Object > Anti-Spyware > DNS Signature

The screenshot shows the 'Anti-Spyware Profile' configuration window. The 'Name' field is set to 'sinkhole dns'. The 'Rules' tab is selected, showing a table with one row: 'test url list 2' under 'External Dynamic List Domains' and 'sinkhole' under 'Action on DNS Queries'. The 'Exceptions' tab is visible but empty. The 'DNS Signatures' tab is selected, showing a 'Threat ID Exceptions' list with 0 items. Below the table are configuration fields for 'Sinkhole IPv4' (set to 'PAN Sinkhole Default IPv4 Address (pan-sink)'), 'Sinkhole IPv6' (set to '::1'), 'Packet Capture' (set to 'disable'), and a checkbox for 'Enable Passive DNS Monitoring' which is unchecked. A 'Threat ID' search bar and 'Add/Delete' buttons are also present.

The sinkhole action provides administrators with an easy way to quickly identify infected hosts on the protected network using DNS traffic. When an anti-spyware profile is enabled in a security profile, the anti-spyware signatures and DNS-based signatures will trigger on DNS queries directed at threat domains.

These signatures can identify a network's local DNS resolver as the source of the traffic rather than the infected host. Then the firewall is unable to determine the originator of the query.

Sinkholing DNS queries involves the forging of responses to DNS queries which are directed at malicious domains. The clients on the network attempt to connect to the sinkhole address rather than the actual host pointed to by DNS. Infected hosts can then be identified in the traffic logs because any host that attempts to connect to the sinkhole address is assumed to be an infected host.

After selecting the sinkhole action, specify an IPv4 and/or IPv6 address that will be used as the sinkhole (the default IPv4 address is a public address owned by Palo Alto Networks, which can be used if you do not wish to redirect the DNS traffic internally). When a sinkhole IP address is configured, the infected clients can be identified by filtering the traffic logs, or by building a custom report that checks for sessions to the specified IP address.

Vulnerability Protection Security Profile:

Objects > Security Profiles > Vulnerability Protection

The screenshot shows the Palo Alto Networks Management Console interface. On the left, there's a navigation sidebar with various icons and sections like Services, Service Groups, Tags, GlobalProtect, Dynamic Block Lists, Custom Objects, Data Patterns, Spyware, Vulnerability, URL Category, Security Profiles (which is currently selected), Antivirus, Anti-Spyware, Vulnerability Protection (which is also selected), URL Filtering, File Blocking, Data Filtering, DoS Protection, Security Profile Groups, Log Forwarding, Decryption Profile, and Schedules. Below the sidebar is a search bar and a 'panedu | Logout' button. The main area has tabs for Dashboard, ACC, Monitor, Policies, and Other. The 'Other' tab is active. In the center, there's a table listing security profiles: 'strict' (Predefined, Rules: 10) and 'default' (Predefined, Rules: 6). A red arrow points from the 'Vulnerability Protection' link in the sidebar to the 'Rules' tab of the 'Vulnerability Protection Profile' configuration window on the right. This window shows a table of rules for the 'Simple-Server-Medium' profile, with the 'Exceptions' tab selected. The table includes columns for Rule Name, Threat Name, CVE, Host Type, Severity, Action, and Packet Capture. The 'simple-client-critical' rule is highlighted.

Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
simple-client-critical				high	default	enable
simple-client-high				medium	default	enable
simple-client-medium				medium	default	enable
simple-client-informational				informational	default	enable
simple-client-low				low	default	enable
simple-server-critical				high	default	enable
simple-server-high	any	server	host	high	default	enable
simple-server-medium	any	server	host	medium	default	enable

A security policy can include specification of a vulnerability protection profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

The firewall includes two predefined vulnerability protection security profiles:

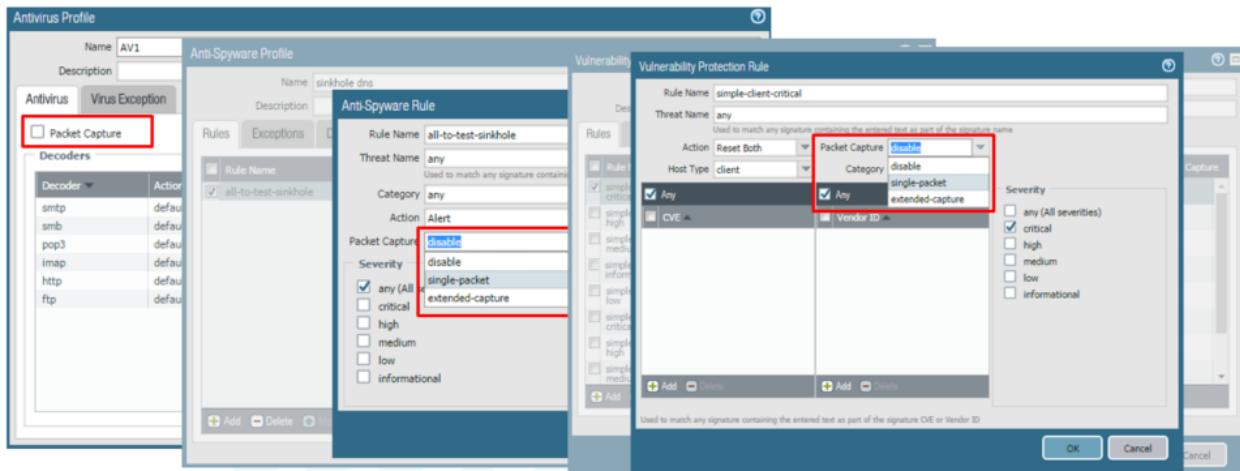
- Default:** The profile applies the default action to all client and server critical-, high-, and medium-severity vulnerability protection events. This profile is typically used for Proof of Concept (POC) or first-phase deployments.

- Strict:** The profile applies the block response to all client and server critical-, high-, and medium-severity vulnerability protection events and uses the default action for low and informational vulnerability protection events. Strict profiles are used for out-of-the-box protection with recommended block of critical, high, and medium threats.

The predefined profiles cannot be modified or deleted.

Enable Packet Captures on other Security Profiles:

Select the check box or appropriate pull down if you want to capture identified packets



One security feature that is sometimes overlooked by security professionals is the Packet Capture option inside of the Security Profiles. This option is available in the event you need to report any False Positives or in the event you would like to troubleshoot other suspect behaviors found in result of the Security Profiles. This may be especially true for Antivirus, Anti-Spyware and Vulnerability Protection profiles. Enabling this option will capture the data that the inspection engine tags as a threat.

Threat Log:

Anything logged from antivirus, anti-spyware ,or vulnerability protection profiles is viewed in the threat log.

Monitor > Logs > Threat

The threat log records each security alarm generated by the firewall. Each entry includes the date and time, the threat type, such as a virus or spyware/vulnerability filtering violation, the source and destination zones, addresses, and ports, the application name, and the action and severity.

Threat log entries can be logged remotely by severity level by defining log forwarding profiles, and then assigning the profiles to security rules. Threats are logged remotely only for the traffic that matches the security rules where the logging profile is assigned.

Threat logs are used in generating reports and in the Application Command Center.

	Receive Time	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
FTP	03/05 22:11:31	FTP Login Failed	untrust	untrust	61.136.188.83		10.154.2.26	21	ftp	alert	informational
FTP	03/05 22:11:30	HTTP response data URI scheme evasion attempt	untrust	untrust	198.189.255.74		10.154.14.14	59539	web-browsing	alert	informational
FTP	03/05 22:11:30	FTP: login brute force attempt	untrust	untrust	61.136.188.83		10.154.2.26	21	ftp	alert	high
FTP	03/05 22:11:29	HTTP WWW-Authentication Failed	untrust	untrust	10.154.7.210	pancademo\john...	17.250.248.77	80	web-browsing	alert	informational
FTP	03/05 22:11:25	FTP Login Failed	untrust	untrust	61.136.188.83		10.154.2.26	21	ftp	alert	informational
FTP	03/05 22:11:20	HTTP WWW-Authentication Failed	untrust	untrust	10.154.12.92	pancademo\kevi...	17.250.248.77	80	web-browsing	alert	informational
FTP	03/05 22:11:17	FTP Login Failed	untrust	untrust	61.136.188.83		10.154.2.26	21	ftp	alert	informational
FTP	03/05 22:11:08	FTP Login Failed	untrust	untrust	61.136.188.83		10.154.2.26	21	ftp	alert	informational
FTP	03/05 22:11:02	SIP Register Request Attempt	untrust	untrust	10.154.1.96	pancademo\bern...	68.142.233.164	443	sip	alert	low
FTP	03/05 22:11:02	HTTP WWW-Authentication Failed	untrust	untrust	10.154.4.2	pancademo\willia...	17.250.248.77	80	web-browsing	alert	informational
FTP	03/05 22:10:59	HTTP WWW-Authentication Failed	untrust	untrust	10.154.7.210	pancademo\john...	17.250.248.77	80	web-browsing	alert	informational

Creating an IP Exemption from the Threat Log:

Click the threat name in the threat log to add IP exemptions to multiple profiles at the same time

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
FTP	05/15 13:19:13	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 13:19:13	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 13:14:41	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 13:14:41	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 12:59:02	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 12:59:02	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 10:01:03	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 10:01:03	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 09:35:28	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 09:35:28	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 09:31:03	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						
FTP	05/15 09:31:03	vulnerability	Mozilla Firefox GeckoActiveXObject Method Denial of Service Vulnerability	Untrust-L3	Trust-L3	184.87.146.110						

Often, the need for exceptions to the vulnerability and anti-spyware profiles are not known until a user complains that they have lost functionality. The situation is further complicated by the fact that multiple profiles may need to have the same exception defined.

Check the box next to the profiles that should have an exemption for this threat and, optionally, specify the IP address exemptions in the adjacent panel.

Note: The Threat Details Interface is exclusively for adding functionality. The values shown do not reflect the current state of the listed profile exemption lists. Check the individual profiles to verify whether or not an exemption already exists.

URL Filtering Security Profile:

Objects > Security Profiles > URL Filtering > Add

The screenshot shows the 'URL Filtering Profile' configuration screen. At the top, there are fields for 'Name' (Branch Office) and 'Description' (For use in all branch offices). Below these are two tabs: 'Categories' (selected) and 'Settings'. Under 'Categories', there are sections for 'Block List' and 'Allow List'. In the 'Block List' section, the 'Action' dropdown is set to 'block'. To the right of these sections is a table listing predefined URL categories and their actions. A note below the table specifies the format for entering entries in the list. A link to 'Check URL Category' is also present.

Category	Action
abortion	allow
abused-drugs	allow
adult	allow
alcohol-and-tobacco	allow
auctions	allow
business-and-economy	allow
computer-and-internet-info	allow
content-delivery-networks	allow
dating	allow
educational-institutions	allow

* indicates a custom URL category
[Check URL Category](#)

URL Filtering security profiles enable you to monitor and control how users access the web over HTTP and HTTPS. The firewall comes with a default profile that is configured to block websites such as known malware sites, phishing sites, and adult content sites. You can use the default profile in a security policy, clone it to be used as a starting point for new URL Filtering profiles, or add a new URL profile that will have all categories set to allow for visibility into the traffic on your network. You can then customize the newly added URL profiles and add lists of specific websites that should always be blocked or allowed, which provides more granular control over URL categories.

A security policy can include specification of a URL Filtering security profile that blocks access to specific web sites and web site categories, or generates an alert when the specified web sites are accessed (a URL Filtering license is required). It is possible to define a block list of websites that are always blocked (or generate alerts) and an allow list of websites that are always allowed.

Predefined sets of web categories can be downloaded from Palo Alto Networks.

Administrators can also define custom URL categories to customize the behavior of the URL Filtering security profiles.

URL Category vs. URL Filtering Security Profile:

Policies > Security

Name	Source	Destination			Application	URL Category	Action	Profile
RestrictSocialMedia	Trust-L3	any	Untrust-L3	any	any	social-networking		

URL Category	URL Filtering Security Profile
Used as a match condition in policies	Applied to traffic allowed by security policy
Matches only predefined or custom categories	Matches predefined or custom categories, as well as Block/Allow Lists
Action is determined by policy	Action can be configured differently for individual categories or URLs
Logged as part of the entry for a policy in the traffic log	Logged in the URL Filtering log

The URL Filtering feature can be used by placing categories directly into policies or attaching a URL Filtering profile to a security rule. URL Filtering affects only HTTP and HTTPS traffic.

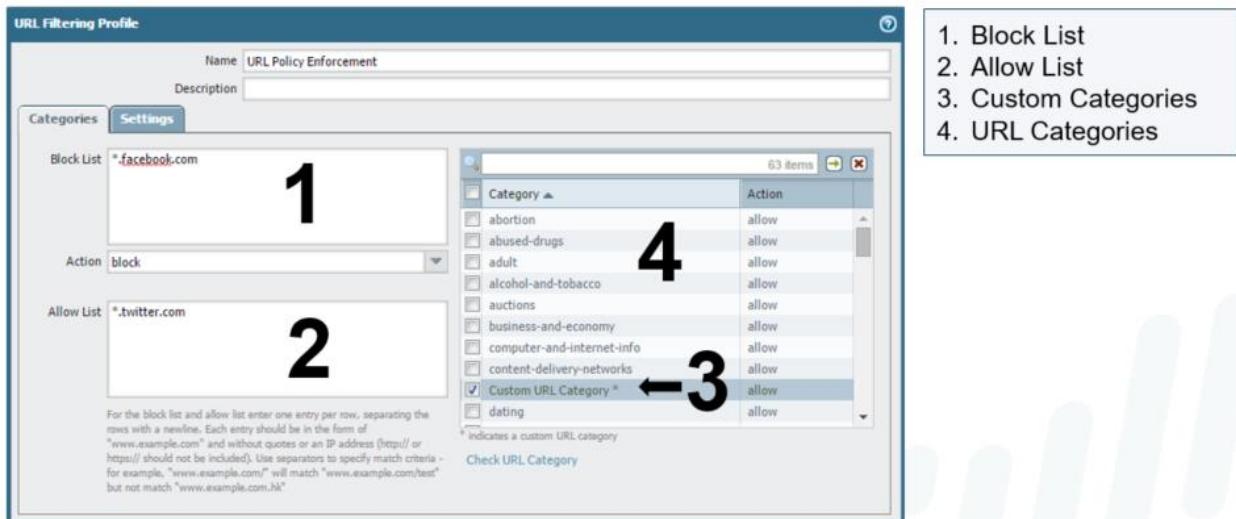
The URL Category field can be used as a match condition for security, QoS, decryption, and captive portal policies. Predefined and custom categories can be matched when using the URL Category field. The URL Category itself does not have an associated action; traffic behavior is controlled by the policy.

The URL Filtering security profile provides granular control for traffic allowed by a security policy.

As with other profiles, the URL Filtering profile is applied only if the associated policy allows traffic. The profile can match URL categories, as well as individual URLs. Each category can be assigned a different action for more focused management. For example, a security policy can be created to allow all web browsing, but has a policy that blocks all access to file sharing websites and logs all access to social networks.

URL Filtering Sequence:

The Order a URL Filtering Profile is Checked



Each URL Filtering profile can be configured with an explicit block list and allow list, which take precedence over URL categories. Omit the http[s]:// portion of the URLs when populating these lists. Entries in the block list and allow list are case-insensitive and must match exactly. For example, www.ebay.com is different from ebay.com.

The block list, allow list, and custom categories support wildcard patterns. A token is a string of characters that begins or ends with a valid separator character (./ ? & = ; +). For example, the following patterns are valid:

***.yahoo.com (Tokens are: "*", "yahoo" and "com")**

www.*.com (Tokens are: "www", "*" and "com")

www.yahoo.com/search=* (Tokens are: "www", "yahoo", "com", "search", "*")

It is recommended to enter the firewall administrator's domain in the allow list to avoid possible miscategorization.

For additional reading on this topic, refer to the document URL Categorization Components and Process on the Support website.

Note: * Depending on which URL Filtering database you are using, subsequent actions will vary. More details on each database, and their respective actions, are covered later in this module.

URL Filtering Actions:

Objects > Security Profiles > URL Filtering > Add

URL Filtering Profile

Name: Branch Office
Description: For use in all branch offices.

Categories **Settings**

Action: block

Allow List:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (<http://> or <https://> should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk".

Change actions for all categories

Change action for an individual category

Category	Action
A Custom URL Category *	override
abortion	allow
computer-and-internet-info	allow
content-delivery-networks	allow
Custom URL Cat *	allow

* Indicates a custom URL category

Check URL Category

Sort Ascending **Sort Descending**

Columns

Set All Actions **Set Selected Actions** **Adjust Columns**

allow
alert
block
continue
override

Actions can be set for the block list and the URL categories. The available actions are:

- **Allow:** Allows the user to access the website; no log or user message is generated.
 - **Block:** Traffic is blocked, a block log entry is generated and a response page is sent to the user's browser.
 - **Alert:** Allows the user to access the website but adds an alert to the URL log.
 - **Continue:** Sends a response page that prompts the user to click Continue to proceed, and logs the action.
 - **Override:** Sends a response page and allows the user to access the blocked page after entering a password, and logs the action.

If a user successfully Continues or Overrides, they have access to the category associated with the URL that generated the event for 15 minutes, without having to Continue or Override again. This timeout time is configurable. The override password is set in Device > Setup > Content ID > URL Admin Override. A firewall can have only one URL Admin Override password.

URL Filtering Log:

Actions that trigger a log are recorded in the URL Filtering log

(Alert, Block, Continue, Override)

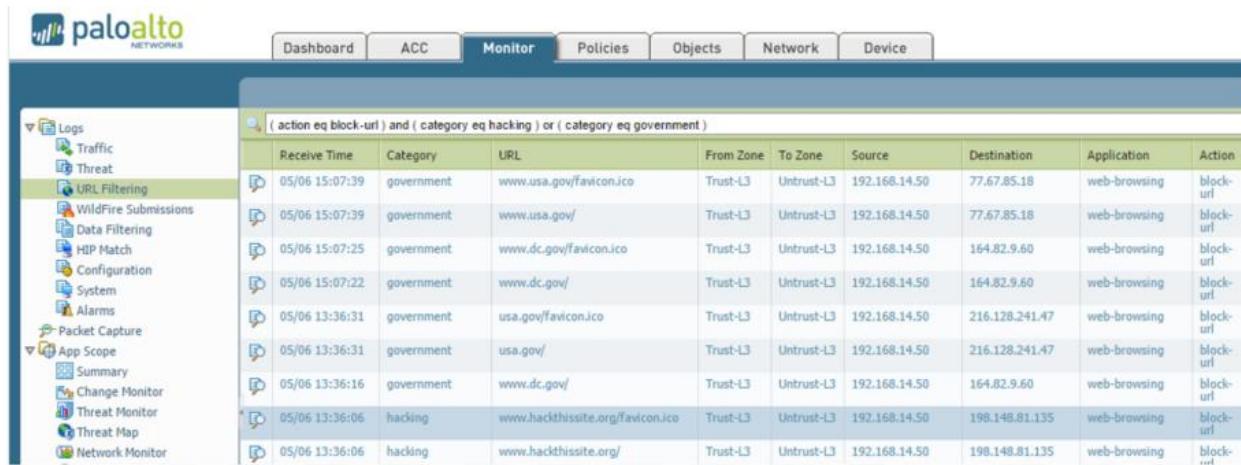
Monitor > Logs > URL Filtering

The URL Filtering log contains log entries for URLs that have action alert, continue, override, and block.

The action taken by the URL Filtering profiles are listed in the Action column.

Actions that require user interaction log the initial blocking action and the successful user interaction.

For example, if a user is presented with a Continue response page and then clicks the Continue button, the block-continue and continue entries are recorded.



A screenshot of the Palo Alto Networks UI. The top navigation bar includes Dashboard, ACC, Monitor (which is selected), Policies, Objects, Network, and Device. On the left, a sidebar menu shows Logs, Traffic, Threat, URL Filtering (selected), WildFire Submissions, Data Filtering, HIP Match, Configuration, System, Alarms, Packet Capture, App Scope, Summary, Change Monitor, Threat Monitor, Threat Map, and Network Monitor. The main content area displays a table of logs with the following columns: Receive Time, Category, URL, From Zone, To Zone, Source, Destination, Application, and Action. A search bar at the top of the table area contains the query: '(action eq block-uri) and (category eq hacking) or (category eq government)'. The table data is as follows:

Receive Time	Category	URL	From Zone	To Zone	Source	Destination	Application	Action
05/06 15:07:39	government	www.usa.gov/favicon.ico	Trust-L3	Untrust-L3	192.168.14.50	77.67.85.18	web-browsing	block-uri
05/06 15:07:39	government	www.usa.gov/	Trust-L3	Untrust-L3	192.168.14.50	77.67.85.18	web-browsing	block-uri
05/06 15:07:25	government	www.dc.gov/favicon.ico	Trust-L3	Untrust-L3	192.168.14.50	164.82.9.60	web-browsing	block-uri
05/06 15:07:22	government	www.dc.gov/	Trust-L3	Untrust-L3	192.168.14.50	164.82.9.60	web-browsing	block-uri
05/06 13:36:31	government	usa.gov/favicon.ico	Trust-L3	Untrust-L3	192.168.14.50	216.128.241.47	web-browsing	block-uri
05/06 13:36:31	government	usa.gov/	Trust-L3	Untrust-L3	192.168.14.50	216.128.241.47	web-browsing	block-uri
05/06 13:36:16	government	www.dc.gov/	Trust-L3	Untrust-L3	192.168.14.50	164.82.9.60	web-browsing	block-uri
05/06 13:36:06	hacking	www.hackthissite.org/favicon.ico	Trust-L3	Untrust-L3	192.168.14.50	198.148.81.135	web-browsing	block-uri
05/06 13:36:06	hacking	www.hackthissite.org/	Trust-L3	Untrust-L3	192.168.14.50	198.148.81.135	web-browsing	block-uri

URL Filtering Service: Pan-DB

PAN-DB

Two offerings: Public Online or Private Offline.

PAN-DB URL Filtering license required.

Uses a seed database for initial configuration, then the device stays in sync with cloud servers.

Attempts lookups from:

1. Caches
2. PAN-DB cloud servers or an M-500 (offline, private server)

Online option requires an Internet connection to the cloud servers.

Private, offline PAN-DB server option requires the Palo Alto Networks M-500.

The Palo Alto Networks URL Filtering solution complements App-ID by enabling you to configure the firewall to identify and control access to web (HTTP and HTTPS) traffic and to protect your network from advanced attacks in the cyber kill chain.

A URL Filtering database categorizes millions of websites into approximately 60-80 categories. You can use these URL categories as a match criteria in policies (captive portal, decryption, security, and QoS) or attach them as URL Filtering profiles within a security policy to safely enable web access and control the traffic that traverses your network.

The PAN-DB URL Filtering solution allows you to choose between the PAN-DB public cloud and the PAN-DB private cloud. Use the public cloud solution if the firewalls on your network can access the Internet directly. If the network security requirements in your enterprise prohibit the firewalls from directly accessing the Internet, you can deploy a PAN-DB private cloud on one or more M-500 appliances that function as PAN-DB servers within your network. The PAN-DB public cloud solution is the default.

A URL Filtering database developed by Palo Alto Networks that is tightly integrated into PAN-OS and the Palo Alto Networks threat intelligence cloud. PAN-DB provides high-performance local caching for maximum inline performance on URL lookups, and offers coverage against malicious URLs and IP addresses. As WildFire, which is a part of the Palo Alto Networks threat intelligence cloud, identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs), the PAN-DB database is updated with information on malicious URLs so that you can block malware downloads, and disable Command and Control (C&C) communications to protect your network from cyber threats. To view a list of PAN-DB URL Filtering categories, refer to <https://urlfiltering.paloaltonetworks.com/CategoryList.aspx>.

URL Filtering Cache: PAN-DB

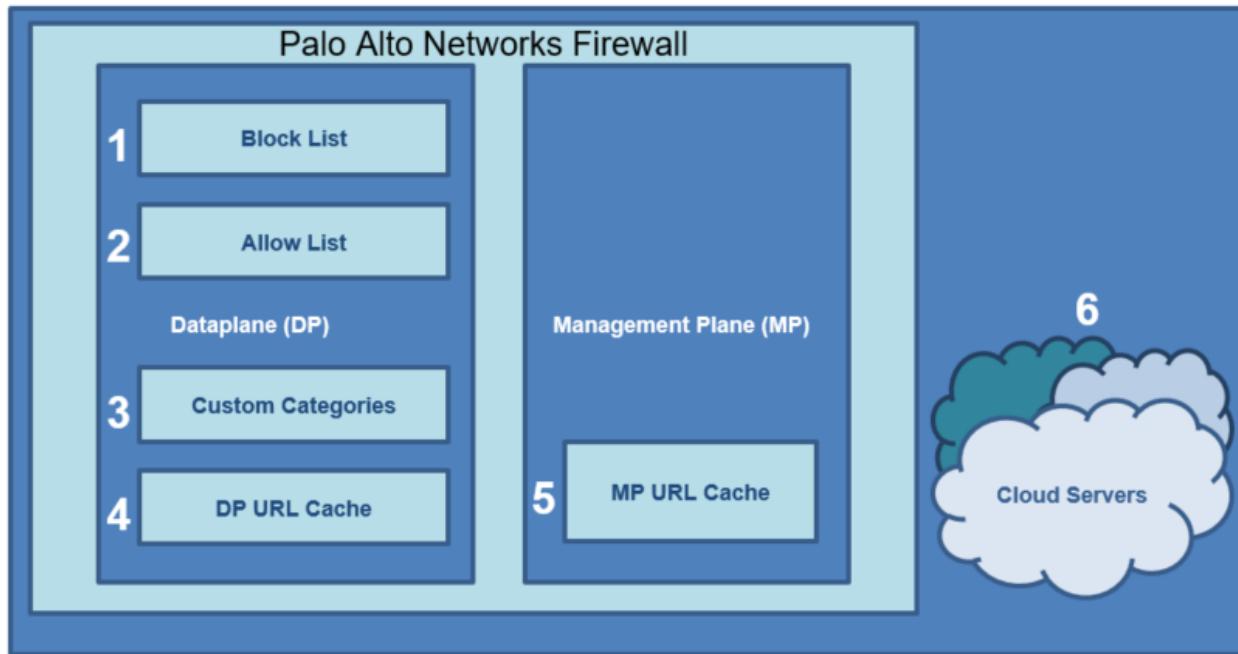
The Palo Alto Networks URL Filtering solution in combination with App-ID provides unprecedented protection against a full spectrum of cyber attacks, legal, regulatory, productivity, and resource utilization risks. While App-ID gives you control over what applications users can access, URL Filtering provides control over related web activity. When combined with User-ID, you can enforce controls based on users and groups. Firewalls using PAN-DB will cache URL lookups to expedite future lookups.

The Management Plane Cache is initially created from a seed database file downloaded from the cloud server. The size of this cache depends on the firewall model and ranges from 300K to 3.5M URLs. The cache is backed up on disk every eight hours and when a reboot is requested by the administrator. Entries expire based on timeouts included for each URL in the database. These timeouts are not configurable.

Like the management plane cache, the dataplane cache expires entries based on values set in the database for each URL. The size of the dataplane cache ranges from 100K to 250K URLs, based on the firewall model.

If a URL is not found in the caches, the firewall contacts the cloud servers for the lookup. PAN-DB does not require a nightly download of a URL Filtering file; all updates are downloaded dynamically from the cloud as needed.

PAN-DB supports full-path categorization of URLs categorizing content down to the page level instead of just at the directory level. The pages within a domain can belong to multiple categories, so this capability provides increased accuracy in filtering content and prevents potential over-blocking of web content. If, for example, you block malware and allow access to business/news content for users on your network, they can access <http://www.acme.com/c/news.html> because it is categorized as news/business, but be denied access to <http://www.acme.com/c/malware.exe> because PAN-DB categorizes the full-path for this web page as malware. To test the category for a full path of a valid URL, use <http://urlfiltering.paloaltonetworks.com/testASite.aspx>.



Configuring a URL Filtering Profile | PAN-DB

Objects > Security Profiles > URL Filtering

Dynamic URL Filtering is enabled by default and is not configurable if the firewall is using PAN-DB.

URL Filtering Profile

Name	Student URL Profile
Description	
Categories	Settings
Block List	<input type="checkbox"/> adult <input type="checkbox"/> alcohol-and-tobacco <input type="checkbox"/> auctions <input type="checkbox"/> business-and-economy <input type="checkbox"/> computer-and-internet-info <input type="checkbox"/> content-delivery-networks <input type="checkbox"/> dating <input type="checkbox"/> dynamic-dns
Action	block
Allow List	

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of:

Category	Action
adult	block

Configure to Access the PAN-DB Private Cloud

Device > Setup > Content-ID

The screenshot shows the Palo Alto Networks Device setup interface under the Content-ID tab. A modal window titled "URL Filtering" is open, showing configuration details for a specific URL filtering profile. The modal includes fields for Dynamic URL Cache Timeout, URL Continue Timeout, URL Admin Override Timeout, and URL Admin Lockout Timeout. It also lists a "PAN-DB Server" IP address (10.10.20.1, 10.10.30.2). Red arrows point from the "PAN-DB Server" field in the main Content-ID window to the same field in the modal window.

Each firewall accesses the PAN-DB servers in the cloud to download the list of eligible servers to which it can connect for URL lookups. With the PAN-DB private cloud, configure the firewalls with a static list of PAN-DB servers that will be used for URL lookups.

- URL Continue Timeout:** Specifies the interval in minutes following a user's continue action before the user must press Continue again for URLs in the same category (range is 1-86400 seconds with a default of 900 seconds or 15 minutes).
- URL Admin Override Timeout:** Specifies the interval in minutes after the user enters the admin override password before the user must re-enter the admin override password for URLs in the same category. (Range is 1-86400 seconds with a default of 900 seconds or 15 minutes.)

- URL Admin Lockout Timeout:** Specifies the period of time in minutes that a user is locked out from attempting to use the URL Admin Override password after three unsuccessful attempts. (Range is 1-86400 seconds with a default of 1800 seconds or 30 minutes.)
- PAN-DB-Server:** Required for connecting to a private PAN-DB server. Specify the IPv4 address, IPv6 address, or FQDN for the private PAN-DB server(s) on your network. You can enter up to 20 entries. The firewall connects to the public PAN-DB cloud, by default. The private PAN-DB solution is for enterprises that disallow the firewall(s) from directly accessing the PAN-DB servers in the public cloud. The firewalls access the servers included in this PAN-DB server(s) list for the URL database, URL updates, and URL lookups for categorizing web pages.

Recategorization Requests:

Sometimes URLs are miscategorized by the database providers, which causes users to be unable to access sites that should be allowed.

Requests for recategorization can be submitted through the Request Categorization Change link in the details window of a log entry. The link redirects the browser to a change request form that is submitted to the database vendor.

The screenshot illustrates the process of requesting URL recategorization. On the left, a table shows two log entries. The second entry's 'Log Details' pane is expanded, highlighting the 'Request Categorization Change' link at the bottom. A red arrow points from this link to a separate 'Request Categorization Change' dialog box on the right. This dialog box contains fields for 'URL', 'Log Category', 'Suggested Category', 'Email', 'Confirm Email', and 'Comments'. A red circle highlights the 'Request Categorization Change' link in the Log Details interface, and another red arrow points from it to the dialog box.

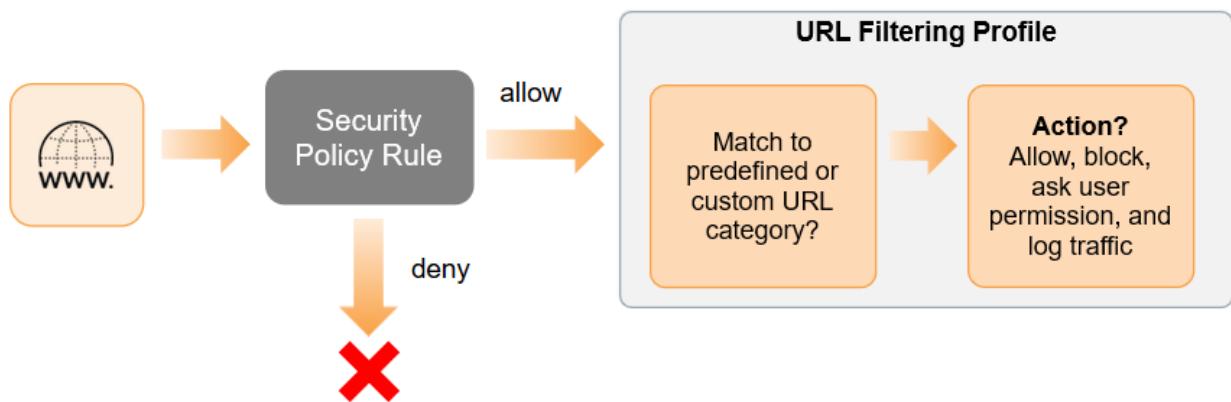
Adjust URL categorization is sent directly from the Log Details interface

PAN-DB

Dashboard > General Information to check URL Filtering Version.

Application Version	8218-5815 (12/16/19)
Threat Version	8218-5815 (12/16/19)
WildFire Version	419650-422432 (01/16/20)
URL Filtering Version	20200117.20158
GlobalProtect Clientless VPN Version	82-175 (12/19/19)

URL Filtering Operation:



Check that Valid Licensing either PAN-DB or BrightCloud URL Filtering is installed.

PAN-DB URL Filtering	
Date Issued	January 16, 2020
Date Expires	February 16, 2020
Description	Palo Alto Networks URL Filtering License
Active	Yes
Download Status	2020-01-16 02:24:45 PAN-DB download: Finished successfully. Re-Download
BrightCloud URL Filtering	
Date Issued	January 16, 2020
Date Expires	February 16, 2020
Description	BrightCloud URL Filtering
Active	No
Download Status	2020-01-16 02:24:04.411 -0800 Error downloading latest URL database

Site Access Column:

Action	Description
Alert	Allows access to web site but adds alert to URL log each time user accesses URL.
Allow	Allows access to the web site but doesn't log traffic.
Block	Blocks access to the web site.
Continue	Displays page to users that warn them against continuing to access the page.
Override	Displays a response page that prompts the user to enter a valid password in order to gain access to the site.

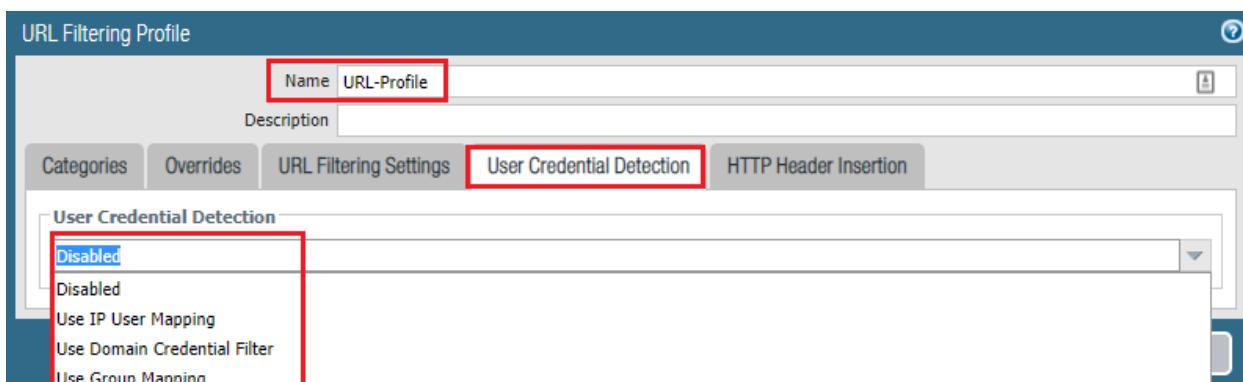
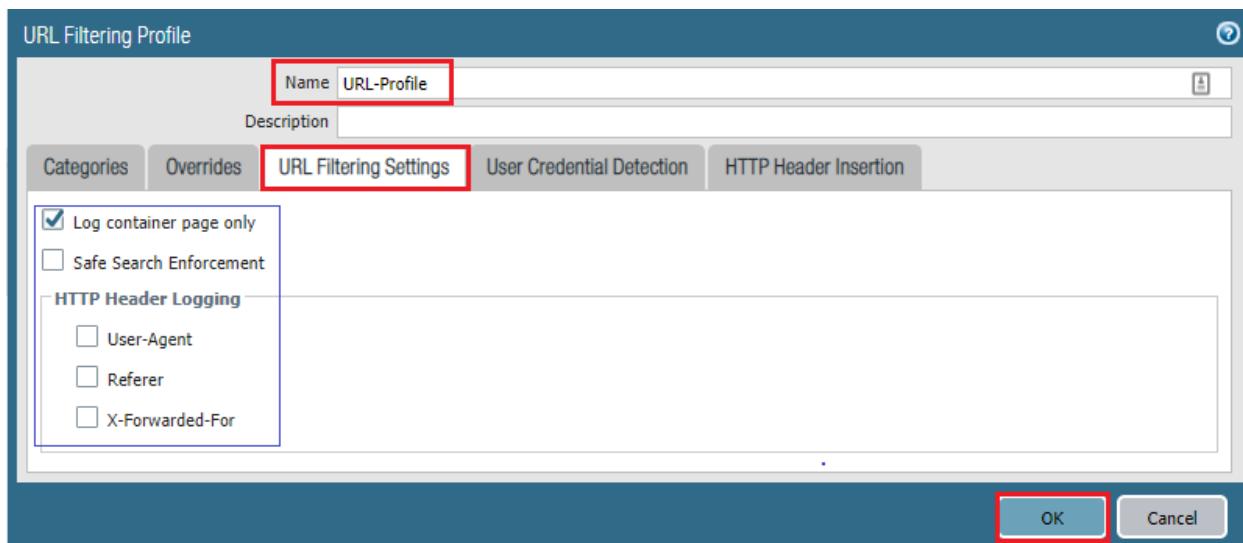
URL Filtering Profile Overrides Tab:

Allow List	Exclude specific websites from URL category enforcement in order to enforce that website separately from the associated URL category. Add sites you want to always allow to the Allow List.
Block List	Add sites to the Block List that you block, alert on, password protect, or warn users against accessing.
Action	Select the action to take when a web site in the block list is accessed.

Block List Action:	
Action	Description
Alert	Allow the user to access the web site but add an alert to the URL log.
Block	Block access to the web site.
Continue	Allow user to access the blocked page by clicking Continue on block page.
Override	Allow the user to access the blocked page after entering a password.

URL Filtering Settings	Descriptions
Log container page only	Select this option to log only the URLs that match the content type that is specified. Default: Enabled
Safe Search Enforcement	Select this option to enforce strict safe search filtering.
HTTP Header Logging	Enabling HTTP Header Logging provides visibility into the attributes included in the HTTP request sent to a server. User-Agent —Web browser that the user used to access the URL. Referer —URL of web page that linked user to another web page; X-Forwarded-For —The header field option that preserves the IP address of the user who requested the web page.

Select Objects > Security Profiles > URL Filtering > User Credential Detection to enable the firewall to detect when users submit corporate credentials.

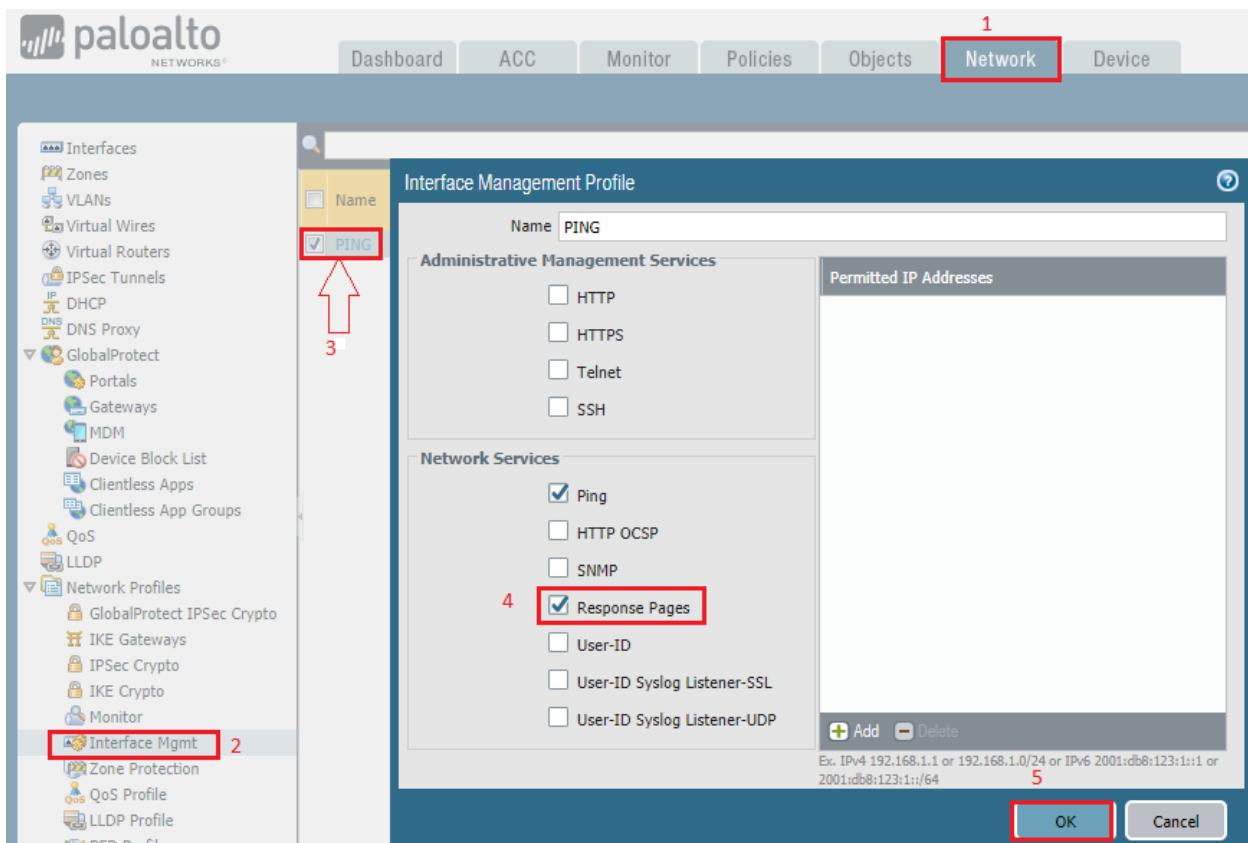


Settings	Description
IP User	This credential detection method checks for valid username submissions.
Group Mapping	The firewall determines if the username a user submits to a restricted site matches any valid corporate username.
Domain Credential	This credential detection method enables the firewall to check for a valid corporate username and the associated password.

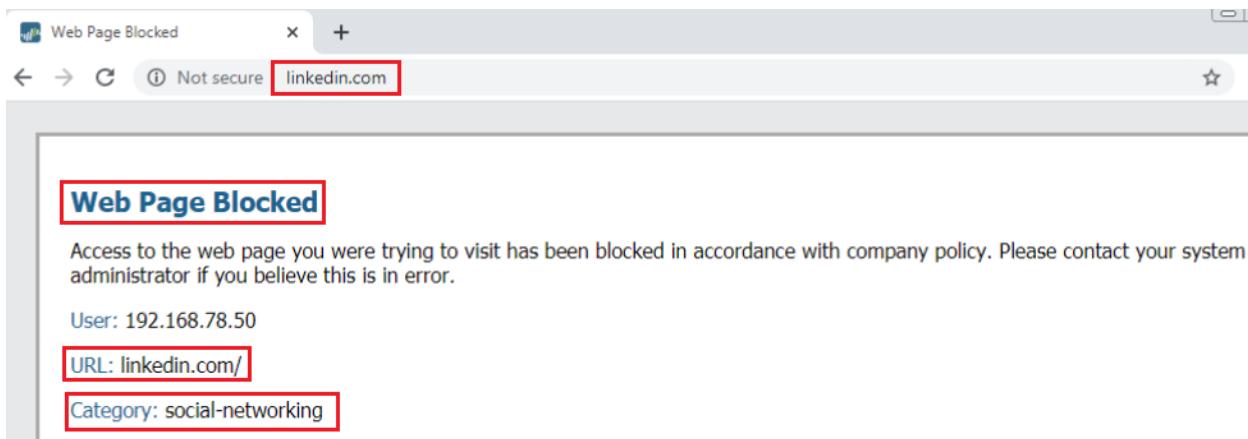
Let's modify the URL Filtering Profile go to Objects > Security Profiles > URL Filtering > click on custom created ULR Profile named: URL-Profile on categories tab in search type social and type enter button or arrow to search for Social-networking in Site access change the action to block. Click OK and commit the changes.

Network > Network Profiles > Interface-Mgmt

Create an interface management profile with response pages enabled or enable response pages on already created ping interface management profile.



From inside any PC access any Social-Networking Websites such as LinkedIn.com, twitter.com or instagram.com it will show Web Page Blocked page as shown below.



Go to Monitor > Logs >Logs >URL Filtering to see the URL logs.

paloalto NETWORKS[®]

Dashboard ACC **Monitor** Policies Objects Network Device

Logs **Traffic** Threat **URL Filtering** 2 WildFire Submissions Data Filtering HIP Match User-ID Tunnel Inspection Configuration System Alarms Authentication Unified Packet Capture App Scope Summary Change Monitor Threat Monitor Threat Map

3

Receive Time	Category	URL	From Zone	To Zone	Source	Destination	Application	Action
01/17 01:52:33	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:33	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:33	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:33	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:33	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:32	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:32	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:32	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue
01/17 01:52:32	social-networking	facebook.com/	Inside	Outside	192.168.78.134	157.240.196.35	ssl	block-continue

admin@PA-VM> show log url

Time	App	From	Src Port	Source
Rule	Action	To	Dst Port	Destination
Severity	Src User	Dst User	Threat	Pcap_id
2020/01/17 01:03:32	facebook-base	Inside	54666	192.168.78.134
Inside-To-Outside	block-url	Outside	443	157.240.195.35
info			(9999)	0
2020/01/17 01:03:32	facebook-base	Inside	54668	192.168.78.134
Inside-To-Outside	block-url	Outside	443	157.240.195.35
info			(9999)	0
2020/01/17 01:03:34	facebook-base	Inside	54670	192.168.78.134
Inside-To-Outside	block-url	Outside	443	157.240.195.35
info			(9999)	0
2020/01/17 01:03:34	facebook-base	Inside	54676	192.168.78.134
Inside-To-Outside	block-url	Outside	443	157.240.195.35
info			(9999)	0
2020/01/17 01:03:34	facebook-base	Inside	54678	192.168.78.134
Inside-To-Outside	block-url	Outside	443	157.240.195.35
info			(9999)	0

URL Filtering Profile

Name **URL-Profile**

Description

Categories Overrides URL Filtering Settings User Credential Detection HTTP Header Insertion

Override Site Access

Category	Site Access	User Credential Submission
<input checked="" type="checkbox"/> social-networking	override	block
<input type="checkbox"/> society	allow	allow

* indicates a custom URL category, + indicates external dynamic list

Check URL Category

OK Cancel

Web Page Blocked

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

User: 192.168.78.60

URL: http://facebook.com/

Category: social-networking

If you require access to this page, have an administrator enter the override password here:

Continue

Override Rule require password to access

Let's go to Device > Setup > Content-ID URL Settings for URL Admin Override click on Add and specify the settings that apply when URL filtering profile blocks page & Override action is specified.

Password/Confirm Password—Enter the password that the user must enter to override the block page.

The screenshot shows the Palo Alto Networks Device setup interface. The top navigation bar has tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device (which is highlighted). The left sidebar contains a tree view of configuration categories like Setup, Certificate Management, and Response Pages. The main content area is titled 'Content-ID' (highlighted with a red box) and shows 'URL Filtering' settings. A modal dialog box is open, titled 'URL Admin Override' (highlighted with a red box). Inside the dialog, there are fields for 'Password' and 'Confirm Password' (both highlighted with red boxes), an 'SSL/TLS Service Profile' dropdown set to 'None' (highlighted with a red box), and a 'Mode' radio button group where 'Transparent' is selected (highlighted with a red box). At the bottom of the dialog are 'OK' and 'Cancel' buttons (both highlighted with red boxes). Numbered callouts (1 through 8) point to various UI elements: 1 points to the 'Device' tab, 2 points to the 'Setup' icon in the sidebar, 3 points to the 'Content-ID' tab, 4 points to the 'URL Admin Override' link in the sidebar, 5 points to the 'Add' button at the bottom of the sidebar, 6 points to the 'Password' field, 7 points to the 'Mode' radio buttons, and 8 points to the 'OK' button.

SSL/TLS Service Profile—To specify a certificate and the allowed TLS protocol versions for securing communications when redirecting through the specified server, select an SSL/TLS Service profile.

Mode—Determines whether the block page is delivered transparently (it appears to originate at the blocked website) or redirects the user to the specified server. If you choose Redirect, enter the IP address for redirection.

Test URL Category:

CLI Command to test URL Category type test url and then input your website to check category.

admin@PA-VM> test url facebook.com

facebook.com social-networking (Base db) expires in 1800 seconds

facebook.com social-networking (Cloud db)

Or visit this Palo Alto Network Firewall URL link to find out any website category.

<https://urlfiltering.paloaltonetworks.com/query/>

example youtube.com

Category: Streaming Media

Description: Sites that stream audio or video content for free and/or purchase.

Example Sites: www.hulu.com, www.youtube.com, www.pandora.com, www.spotify.com, www.grooveshark.com