paloalto TECHDOCS

PAN-OS ® New Features Guide

11.0 (EoL)

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

November 17, 2024

Table of Contents

Networking Features

The networking features for PAN-OS 11.0 are documented in the 11.0 PAN-OS Networking Administrator's Guide. The VPN and LSVPN features are documented in the PAN-OS Administrator's Guide.

- (PAN-OS 11.0.1 and later 11.0 releases) PPPoE Client Support on a Subinterface
- DHCPv6 Client with Prefix Delegation
- IPSec Transport Mode
- Multicast Source Discovery Protocol on Advanced Routing Engine
- Web Proxy
- Power Over Ethernet (PoE)

PPPoE Client Support on a Subinterface

The firewall supports a PPPoE (Point-to-Point Protocol over Ethernet) IPv4 client on a Layer 3 subinterface for when your ISP indicates that PPPoE over 802.1Q VLAN is the way in which to connect to its internet services. The firewall establishes a PPPoE connection to the ISP using an 802.1Q VLAN tag. The PPPoE client that you configure on the subinterface learns its IPv4 address from the ISP, along with other information such as the IP address of the server, DNS information, and MTU.

You can configure a PPPOE client on either a physical interface or a subinterface, but not both at the same time. Only one PPPoE subinterface is supported on a physical interface. Before you begin configuring a PPPoE client, ask your ISP what VLAN tag to use for your connection. You will enter that tag when you configure the subinterface number and Tag. The following task assumes you have already configured a Layer 3 Ethernet interface on the firewall with a security zone.

STEP 1 | Configure a subinterface as a PPPoE client (termination point).

1. Select **Network** > **Interfaces** > **Ethernet** and highlight a Layer 3 Ethernet interface.
2. **Add Subinterface**.
3. To the right of the **Interface Name** and dot, enter the subinterface number, which is the VLAN tag number that your ISP provided.
4. Enter the **Tag**, which is the VLAN tag number that your ISP provided. The actual VLAN tag ID is read from this Tag field.
5. Select **IPv4**.
6. Select the **Type** of address as **PPPoE**.
7. Select **General** and **Enable** the subinterface.
8. Enter the **Username** and **Password** for the authentication you will choose.

STEP 2 | Configure additional characteristics of the PPPoE subinterface, such as the type of authentication, requesting a specific IPv4 address, and creating a default route that points to the default gateway that the PPPoE server provides.

STEP 3 | Click **OK**.

STEP 4 | **Commit** the changes.

STEP 5 | View information about the PPPoE client.

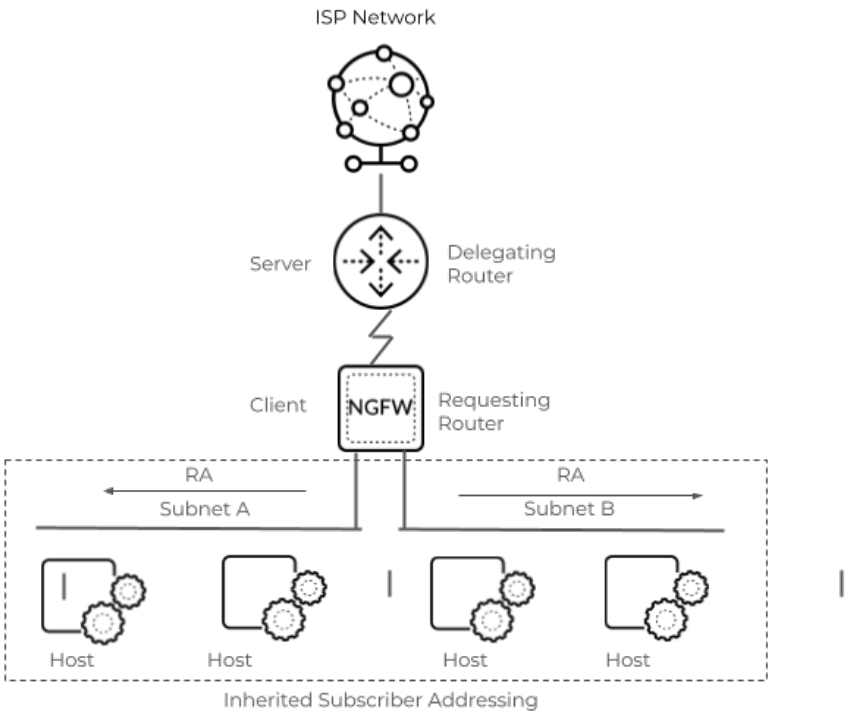
DHCPv6 Client with Prefix Delegation

A PAN-OS firewall can act as a DHCPv6 client to request an IPv6 address for its interface and an IPv6 prefix and options from a DHCPv6 server, thereby provisioning a Layer 3 Ethernet, VLAN, or Aggregate Ethernet (AE) interface. DHCPv6 client reduces your IPv6 address provisioning effort and potential errors, and automates the task of getting your hosts onto the network.

Furthermore, the DHCPv6 client firewall supports prefix delegation. An ISP assigns prefixes to a DHCPv6 server, which assigns prefixes to the DHCPv6 client firewall. The firewall then assigns a subnet from the prefix pool of delegated prefixes to one or more of its host-facing interfaces. The delegated interfaces distribute the addresses from the delegated pool to the local network using Neighbor Discovery Protocol (NDP) with stateless address autoconfiguration (SLAAC). The delegated interfaces also provide other parameters using NDP. Configure prefix delegation if there are hosts connected to the firewall that need dynamic IPv6 addressing. Prefix delegation simplifies network provisioning on customer-facing LAN networks.

To configure a firewall interface that is facing the hosts on the network, you configure the interface type to be **inherited**. Only inherited interfaces can advertise those selected prefixes from the prefix pool to the hosts. Each host constructs its own IPv6 address using the delegated prefix and its MAC address or EUI-64 (Extended Unique Identifier), at the discretion of the host.

The following example topology has a firewall, a DHCPv6 server north of the firewall, and hosts on two LANs south of the firewall.



The firewall interface that faces the delegating router is a Stateless Address Autoconfiguration (SLAAC) client. The firewall interface that faces the host is a SLAAC server; the host is a SLAAC client. The DHCPv6 client allocates a /64 prefix from the prefix pool to the inherited interface.

The firewall configures an IPv6 address on an inherited interface using SLAAC and sends RAs with the prefix to autoconfigure the host interfaces using SLAAC.

You first configure the interface facing the DHCPv6 server and ISP to be a **DHCPv6 Client** and request a Non-Temporary or Temporary address for itself. This interface also requests a delegated prefix on behalf of the host-facing interface. You then configure an interface facing the hosts as an **inherited** interface that provides prefix delegation to the LAN hosts.

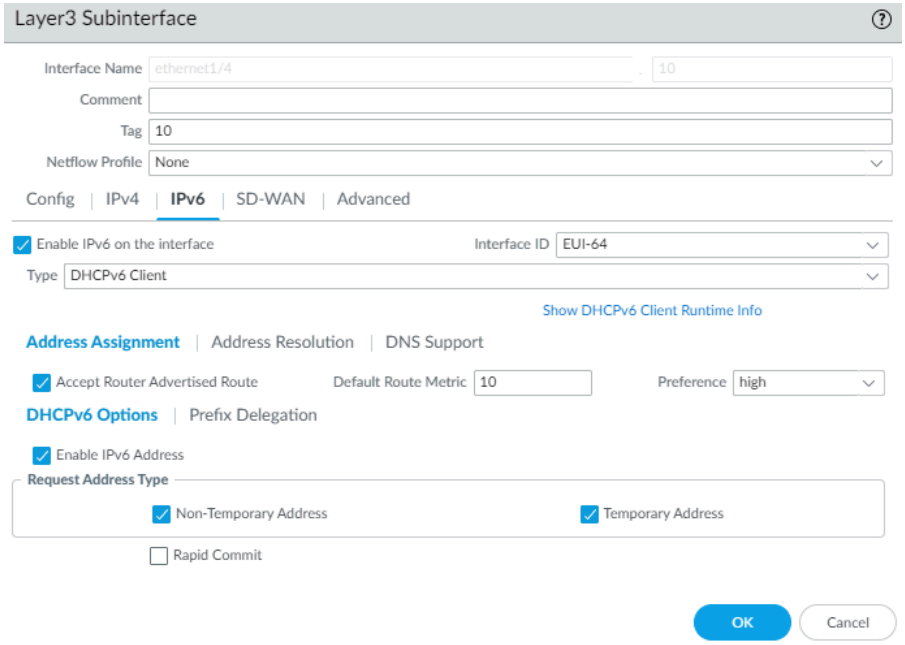
STEP 1 | Select an Ethernet, AE, or VLAN interface (that faces the DHCPv6 server and ISP) to be a DHCPv6 client.

1. Select **Network** > **Interfaces** > **Ethernet** or select **Network** > **Interfaces** > **Ethernet** and select an AE interface, or select **Network** > **Interfaces** > **VLAN**.
2. For **Interface Type**, select **Layer3**.
3. **Add Subinterface** if you want a single Ethernet or VLAN interface facing the ISP to be separated into subinterfaces.

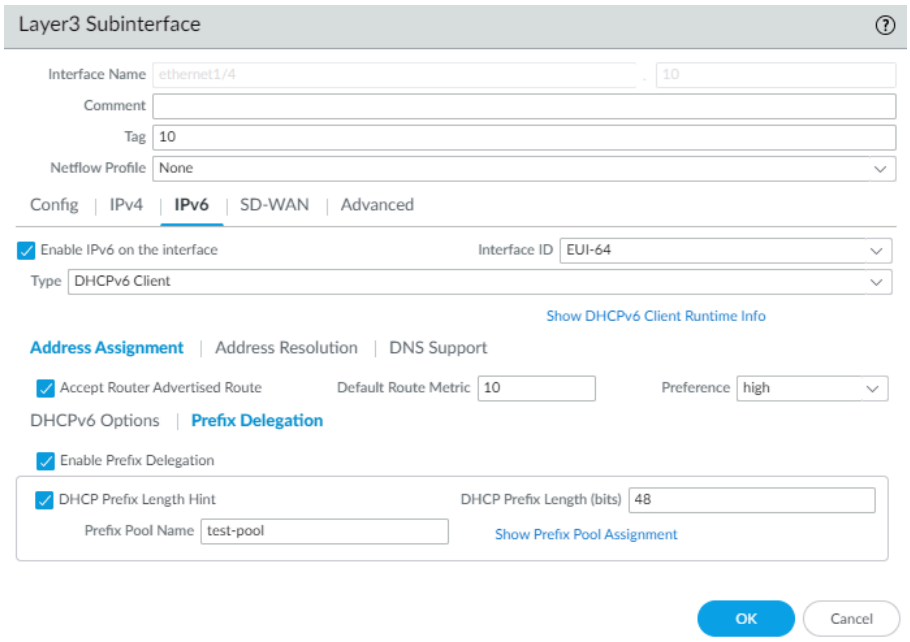
STEP 2 | Select **IPv6** and **Enable IPv6 on the interface**.

STEP 3 | Configure an interface that faces the ISP to be a DHCPv6 client and request its leased, temporary and/or non-temporary IPv6 address.

1. For **Type**, select **DHCPv6 Client**.
2. Select **Address Assignment** and **Accept Router Advertised Route**.



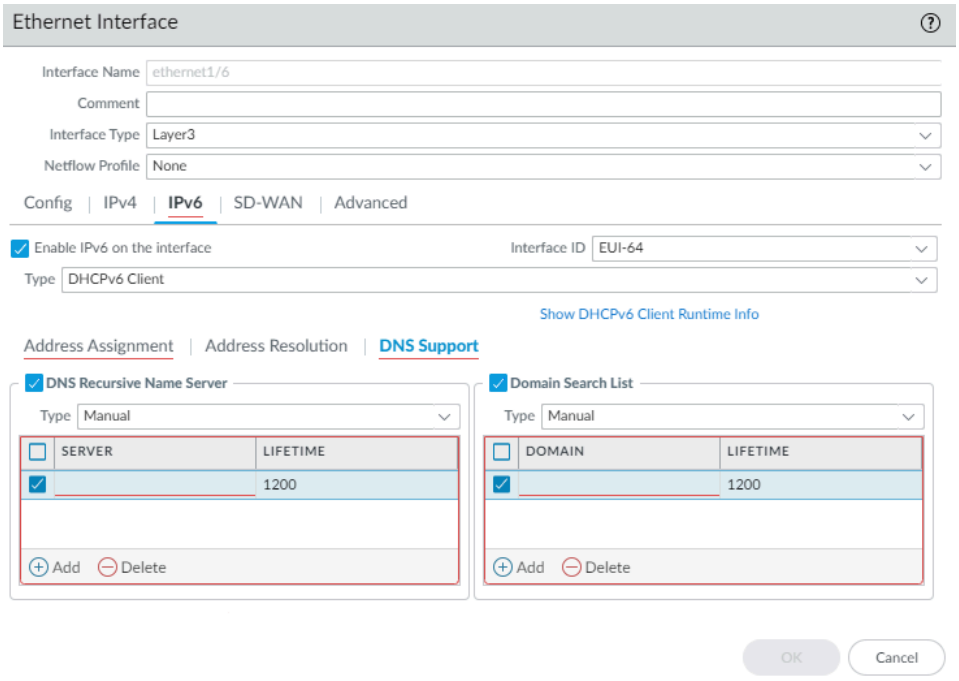
3. Select **DHCPv6 Options** and **Enable IPv6 Address**. Request a Non-Temporary and/or Temporary Address.
4. Select **Prefix Delegation** and **Enable Prefix Delegation**.



STEP 4 | For a DHCPv6 Client, configure address resolution.

STEP 5 | For a DHCPv6 Client, configure DNS support.

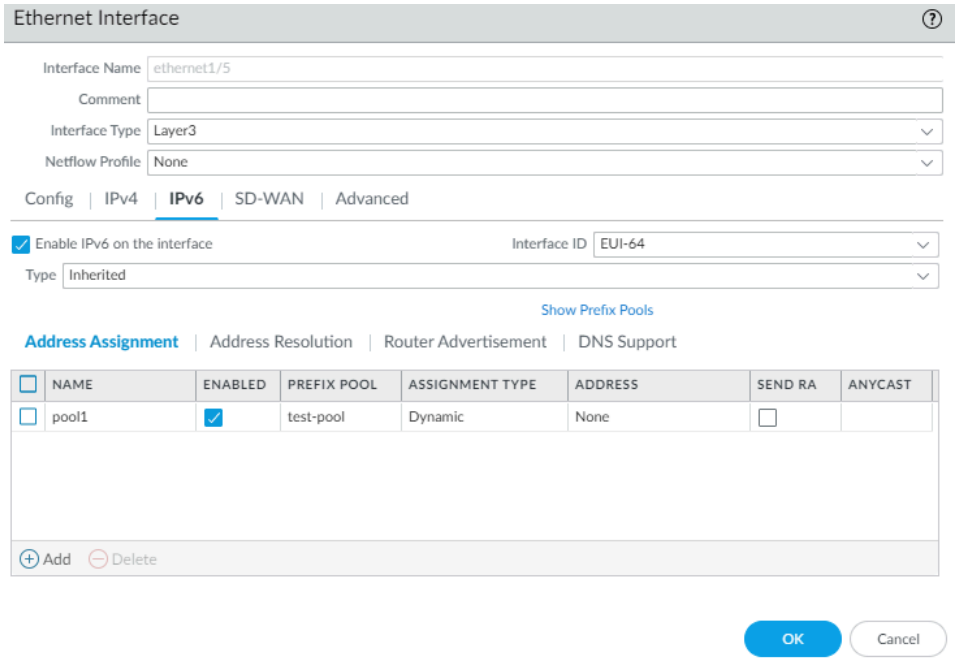
1. Enable **DNS Recursive Name Server** and select:
   - **DHCPv6**—The DHCPv6 Server sends the DNS Recursive Name Server information to the client.
   - **Manual**—You configure the DNS Recursive Name Server.



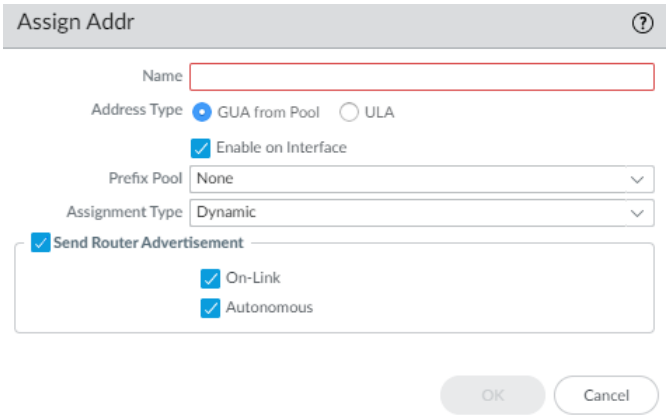
2. Configure **Domain Search List**.

STEP 6 | Configure a host-facing interface to inherit the IPv6 prefix and advertise allocated /64 prefixes to the hosts.

1. Select **Network** > **Interfaces** > **Ethernet** or select **Network** > **Interfaces** > **Ethernet** and select an AE interface, or select **Network** > **Interfaces** > **VLAN**.
2. Select a Layer 3 interface, select **IPv6**, and **Enable IPv6 on the interface**.
3. For **Type**, select **Inherited**.



4. Select **Address Assignment** and **Add** a pool.



5. For **Address Type**, select one of the following:
   - **GUA from Pool**—Global Unicast Address that comes from the Prefix Pool.
   - **ULA**—Unique Local Address is a private address in the address range fc00::/7 for connectivity within a private network. Select ULA if there is no DHCPv6 Server.
6. **Enable on Interface**.
7. Select the **Prefix Pool** from which to get the GUA.
8. Select **Assignment Type**:

- **Dynamic**—The DHCPv6 client chooses an identifier to configure the inherited interface.
- **Dynamic with Identifier**—Enter an identifier in the range 0 to 4,000.

STEP 7 | For Inherited interface, configure Address Resolution, Router Advertisement, and DNS Support.

STEP 8 | **Commit**.

IPSec Transport Mode

While PAN-OS® supports tunnel mode by default, you can now configure IPSec tunnels to use transport mode when encrypting host-to-host communications. Transport mode encrypts only the payload while retaining the original IP header. You can use transport mode to encrypt the management traffic with the most secure protocols.

Transport mode supports:

- IPv4 address only.
- Encapsulating Security Payload (ESP) protocol only.
- IKEv2 only.
- DH-group 20 for Diffie-Hellman (DH) group and perfect forward secrecy (PFS).
- Only AES with 256-bit keys in GCM mode.

Certain protocols do not provide payload encryption when exchanging information with other peer. Some protocols use MD5 authentication between peers, which is no lon4ger adequate for communication exposed to a public internetwork. By using IPSec, we can protect the content of management plane protocols. The default setting of IPSec is tunnel mode, which uses both encryption and authentication to protect a complete site. In some cases, this is not sufficient to protect management protocol peers since the cipher used may be independent of the site. Even within a single domain, management plane data may have to be confidential. In such cases, IPSec in transport mode enables you to encrypt the management traffic with the most secure protocols.

In transport mode, data within the original IP packet is protected, but not the IP header. Transport mode sends encrypted traffic directly between two hosts that have previously established a secure IPSec tunnel. Transport mode should only be enabled when the device that generates and protects the packet is also the one that verifies and decrypts the packet.

A transport mode process does not create a new IP header, therefore it is less complex.

While configuring an IPSec tunnel, you can now select the **IPSec Mode** as **Tunnel** or **Transport** mode to establish a secure connection. That is, you can select whether to encrypt or authenticate packets in transport mode or tunnel mode.

Differences between Tunnel and Transport Mode

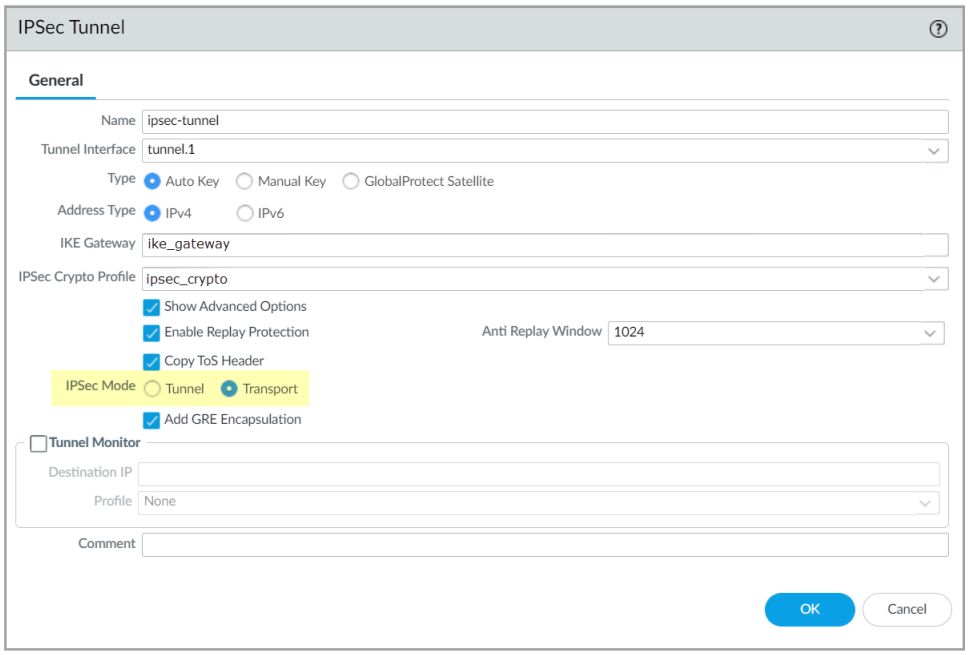
Tunnel Mode	Transport Mode
Encrypts the entire packet, including the IP header. A new IP header is added to the packet after encryption.	Encrypts only the payload, while the original IP header is retained.
Tunnel monitoring uses the tunnel interface IP address.	Tunnel monitoring automatically uses the IP address of the physical interface (gateway interface IP address), and tunnel interface IP address is ignored.
Supports double encapsulation.	No support for double encapsulation.

Tunnel Mode	Transport Mode
This mode is commonly used for site-to-site communications.	This mode is commonly used for host-to-host communications.

Important points to remember before enabling the transport mode:

- You can't select transport mode when NAT-T is enabled.
- You can't configure an IKE gateway on a loopback interface to an IPSec tunnel with transport mode.
- IPSec transport mode does not use proxy ID settings for negotiation. Hence, you cannot configure a proxy ID in transport mode. If you attempt to configure proxy ID by any other method, it will be replaced with 0.0.0.0/0 automatically.
- You can use transport mode only with an **auto-key** key exchange.
- If you configure a IKE gateway without an IPSec tunnel, by default IKE negotiates a tunnel mode child security association (SA).
- In IPSec transport mode without GRE encapsulation, don't route the user traffic through the associated tunnel interface. Configure the control protocols (like, BGP peering sessions) on a physical interface (for example, ethernet1/1) instead of a tunnel interface. While IPSec tunnel mode for BGP routes works with the tunnel interface, IPSec transport mode for BGP routes works with the physical interface only.
- By default, IPSec tunnel operates in **Tunnel** mode.
- You should enable **Add GRE Encapsulation** in **Transport** mode to encapsulate multicast packets.

To enable IPSec transport mode, select **Network** > **IPSec Tunnel** and then select **Show Advanced Options**. From **Show Advanced Options**, select the **IPSec Mode** as **Transport** mode to encrypt or authenticate packets in transport mode.



Multicast Source Discovery Protocol on Advanced Routing Engine

Advanced Routing mode supports Multicast Source Discovery Protocol (MSDP) in PIM Sparse Mode (PIM-SM). MSDP-enabled firewalls in one domain can peer with MDSP-enabled devices in a different domain or autonomous system. The peers exchange control information and discover multicast sources outside their own domain. MSDP tracks active sources and shares them with configured peers. MSDP reduces the complexity of interconnecting multiple PIM-SM domains by allowing the domains to use an interdomain source tree.

MSDP uses well-known TCP port 639 for peering. Before you configure MSDP, be familiar with RFC 3618.

MSDP message types are Source Active (SA), Keepalive, and Notification messages.

STEP 1 | Configure a logical router.

STEP 2 | Select **Multicast** and **enable multicast protocol** and **MSDP** for the logical router.

STEP 3 | Configure MSDP.

STEP 4 | Create an MSDP Authentication Profile, which uses MD5 authentication.

STEP 5 | Create an MSDP Timer Profile.

STEP 6 | **Commit**.

STEP 7 | View MSDP information from **More Runtime Stats**.

Web Proxy

If your network uses a proxy device for security, you can now leverage the same level of protection using the on-premises web proxy capability with PAN-OS 11.0. The web proxy features enables additional options for migrating from an existing web proxy architecture to a simple unified management console. Using the web proxy feature with Prisma Access provides a seamless method for migrating, deploying, and maintaining secure web gateway (SWG) configurations from an easy to use and simplified interface. Web proxy helps during the transition from on-premises to the cloud with no loss to security or efficiency.

The web proxy supports two methods for routing traffic:

- For the explicit proxy method, the request contains the destination IP address of the configured proxy and the client browser sends requests to the proxy directly. You can use one of following methods to authenticate users with the explicit proxy:
  - Kerberos, which requires a web proxy license.
  - SAML 2.0, which requires Panorama, a Prisma Access license, the Cloud Services 3.2.1 plugin (and later versions), and the add-on web proxy license.
  - Cloud Identity Engine, which requires Panorama, a Prisma Access license, the Cloud Services 3.2.1 plugin (and later versions), and the add-on web proxy license.
- For the transparent proxy method, the request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). There is no client configuration and Panorama is optional. Transparent proxy requires a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules. Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP).

The following platforms support web proxy:

- PA-1400
- PA-3400
- VM Series (with a minimum of four vCPUs)
- Panorama using PAN-OS 11.0
- Cloud services plugin 3.2.1 (and later versions) for Explicit Proxy using SAML authentication

Web proxy supports IPv4.

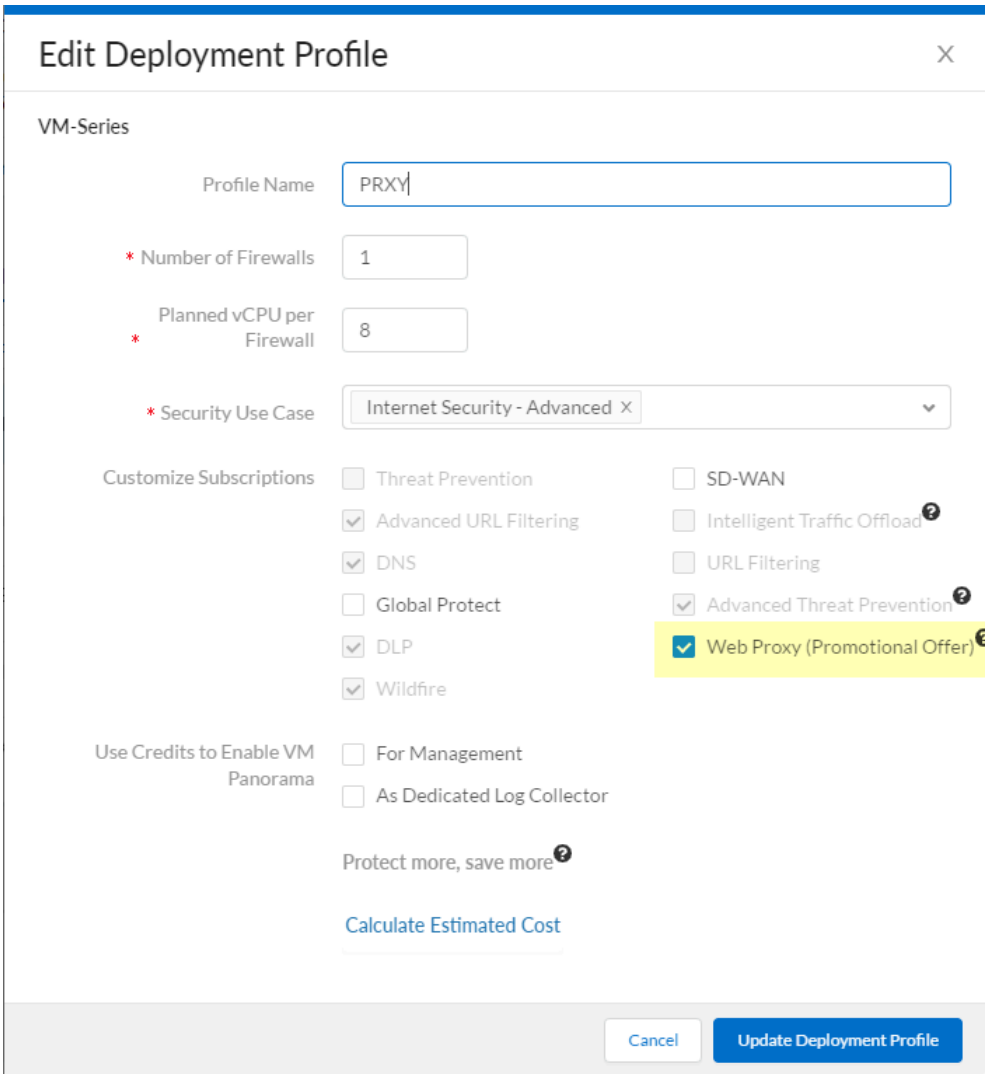
Configure Explicit Proxy

The explicit proxy method allows you to troubleshoot issues more easily, since the client browser is aware of the existence of the proxy.

1. If you have not already done so, activate the license for web proxy.

   You must activate the web proxy license for the PA-1400 Series, PA-3400 Series, and VM-Series. Learn how to activate your subscription licenses for the PA-1400 Series and PA-3400 Series or activate the web proxy license for the VM-Series in the following step.

1. Log in to the Customer Service Portal (CSP).
2. **Edit** the deployment profile.
3. Select **Web Proxy (Promotional Offer)**.



4. Click **Update Deployment Profile**.
5. On the firewall, retrieve the license keys from the server.

If the license key retrieval is not successful, restart the firewall and repeat this step before proceeding.

2. Set up the necessary interfaces and zones.

   As a best practice, use Layer 3 (L3) for the three interfaces the web proxy uses and configure a separate zone for each interface within the same virtual routers and the same virtual systems.

   1. Configure an interface for the client traffic.

      *Be sure to carefully copy the IP address for this interface and save it in a secure location because you must enter it as the **Proxy IP** address when you configure the web proxy.*

   2. Configure an interface for the outgoing traffic to the internet.
   3. Configure a loopback interface for the proxy.

      All incoming traffic is routed through this interface to the proxy.

3. Set up the DNS proxy for Explicit Proxy.
   1. Configure a DNS proxy object for the proxy connection.
   2. Configure a DNS Server profile with both primary and secondary DNS servers.

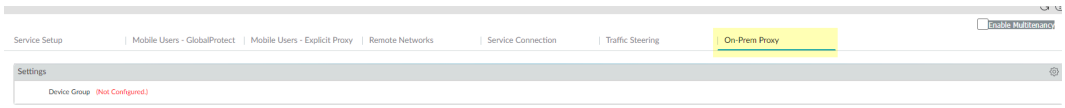
      You must configure both a primary and a secondary DNS server for web proxy.

   3. Specify the interface for the proxy connection.

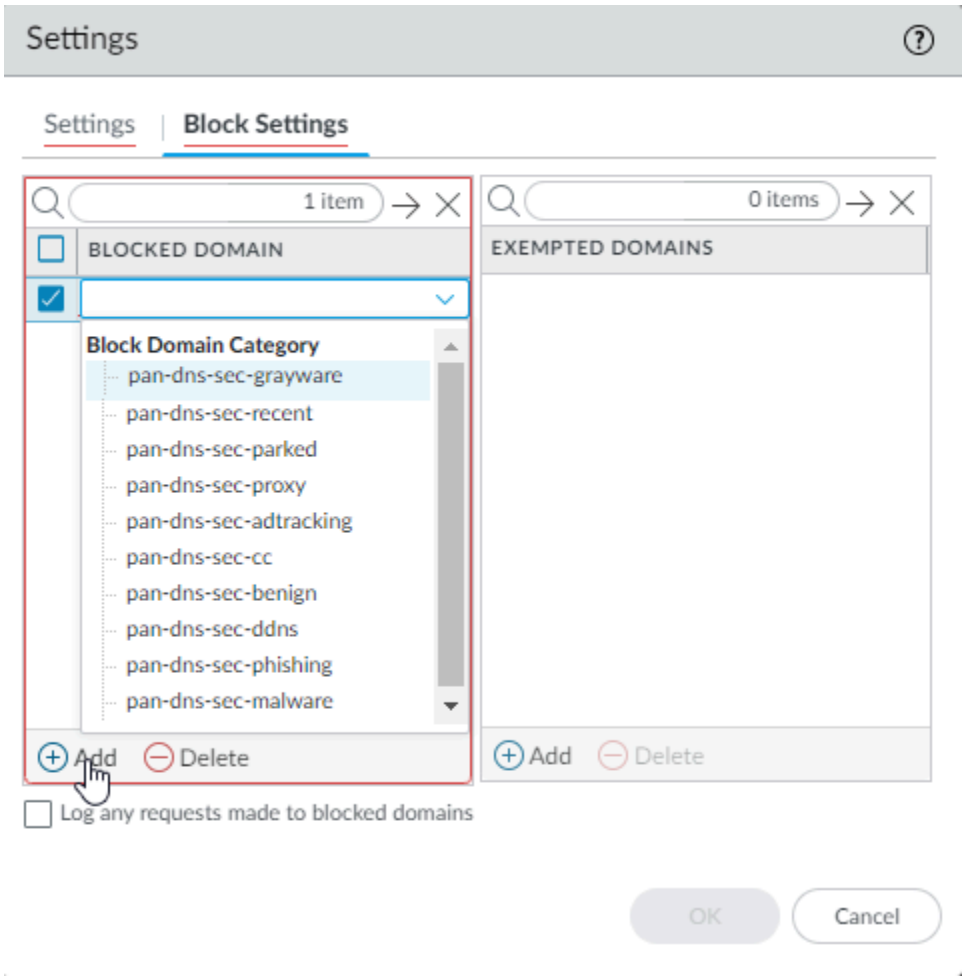
      Specify either the traffic ingress interface or a loopback interface.

4. To enable decryption for MITM detection, create a self-signed root CA certificate or import a certificate signed by your enterprise certificate authority (CA). For more information, refer to the best practices for administrative access.
5. Ensure you have completed the pre-deployment steps for the authentication method you want to configure. Select only one of the following authentication methods.
   - Configure Kerberos Authentication
   - Configure SAML Authentication
   - Configure Cloud Identity Engine Authentication
6. If you have a DNS security subscription, integrate the web proxy firewall with Explicit Proxy to sinkhole any requests that match the DNS security categories that you specify.
   1. Select **Panorama** > **Cloud Services** > **Configuration** > **On-Prem Proxy**.
   2. **Edit** the settings then select the **Device Group** you want the web proxy firewall to use or **Add** a new device group.

To integrate the web proxy firewall with Prisma Access, you must configure the web proxy firewall in a separate device group that contains no other firewalls or virtual systems. If the firewall is already a member of a device group, create a child device group as a sub-group and move the firewall to the child device group.



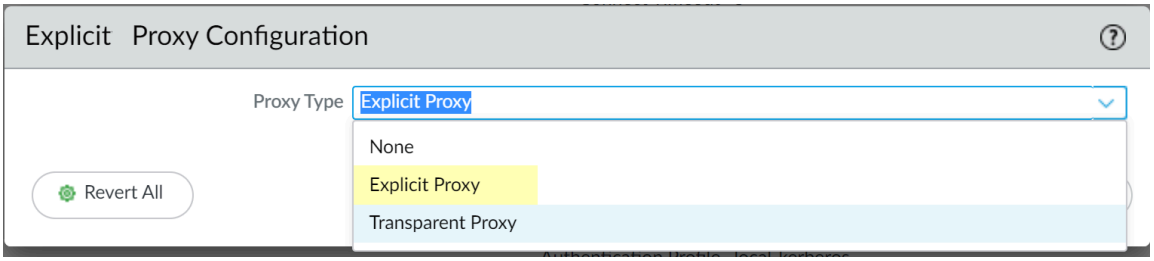
3. (Optional) Select **Block Settings** to **Add** a **Blocked Domain** or any domains that are **Exempted Domains** because they are sinkholed due to matching one or more of the DNS Security categories.



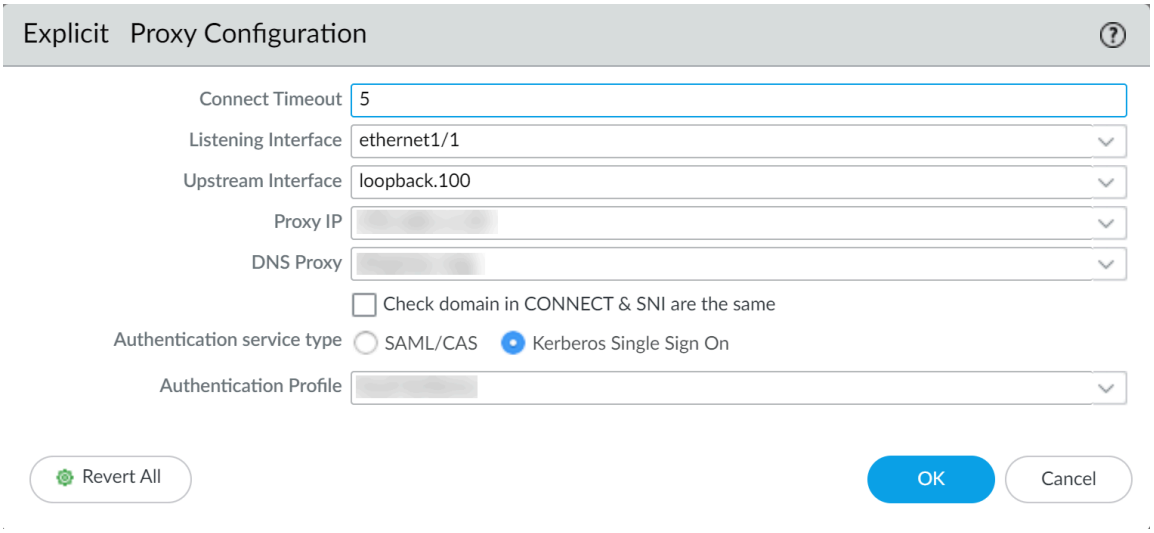
4. (Optional) Select whether you want to **Log any requests made to blocked domains**.
5. Click **OK**.

7. Set up the Explicit Proxy.
   1. On the firewall, select **Network** > **Proxy** then **Edit** the **Proxy Enablement** settings.
   2. Select **Explicit Proxy** as the **Proxy Type** then click **OK** to confirm the changes.

If the only available option is None, verify that you have an active license for the web proxy feature.



3. **Edit** the **Explicit Proxy Configuration**.



4. Specify the **Connect Timeout** to define (in seconds) how long the proxy waits for a response from the web server. If there is no response after the specified amount of time has elapsed, the proxy closes the connection.
5. Select the **Listening Interface** that contains the firewall where you want to enable the web proxy.

   Specify the ingress interface for the client traffic.
6. Select the **Upstream Interface** that contains the interface with the web proxy that reroutes the traffic to the server.

   *If you are using a loopback interface, specify that interface as the **Upstream Interface**.*
7. Specify the IP address of the listening interface as the **Proxy IP**.

   Enter the IP address of the interface you created in Step 2.a.
8. Specify the **DNS Proxy** object you created in Step 3.a.

9. Select **Check domain in CONNECT & SNI are the same** to prevent domain fronting attacks by specifying different domains between the CONNECT request and the Server Name Indication (SNI) field in the HTTP header.
10. Select the **Authentication service type** you want to use (either **SAML/CAS** or **Kerberos Single Sign On**).

    Be sure to complete all necessary pre-deployment and configuration steps for the authentication method you select. Select only one of the following authentication methods:

    - Configure Kerberos Authentication
    - Configure SAML Authentication
    - Configure Cloud Identity Engine Authentication

11. Click **OK** to confirm the changes

8. Configure the necessary security policy rules to decrypt traffic and reroute applicable traffic to the proxy.

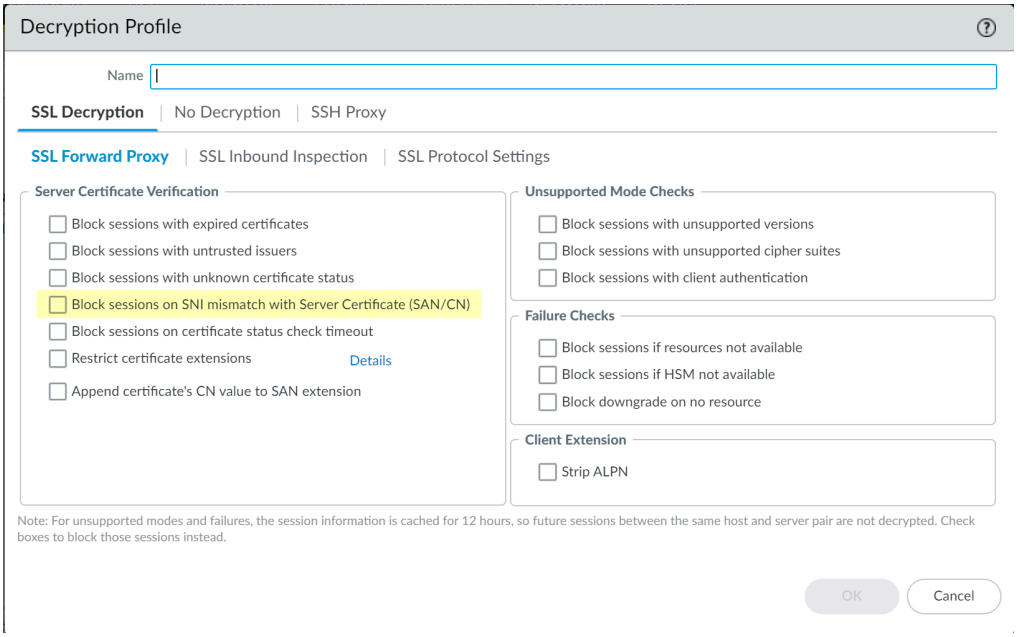
   You will need to create the following types of rules:

   - *Source NAT (if applicable)*
   - *Decryption*
   - *Security*

1. Configure a decryption policy to decrypt the traffic so it can be rerouted if necessary.

   To avoid decrypting traffic twice, select the zone that contains the upstream interface as the source zone for the decryption policy.

2. (Optional but recommended) Select **Objects** > **Decryption Profile** and select **Block sessions on SNI mismatch with Server Certificate (SAN/CN)** to automatically deny any sessions where the Server Name Indication (SNI) does not match the server certificate.



3. Configure the necessary security policy rules.
    1. Create a security policy rule to allow traffic from the client to the interface you selected as the listening interface.
    2. Configure a security policy rule to allow traffic from the zone that contains the upstream interface to the internet.
    3. Configure a security policy rule to allow traffic from the DNS proxy zone to the internet.
4. Configure a security policy rule using the authentication profile you configured in Step 5 to route traffic to the proxy as appropriate.

- **Configure Transparent Proxy**

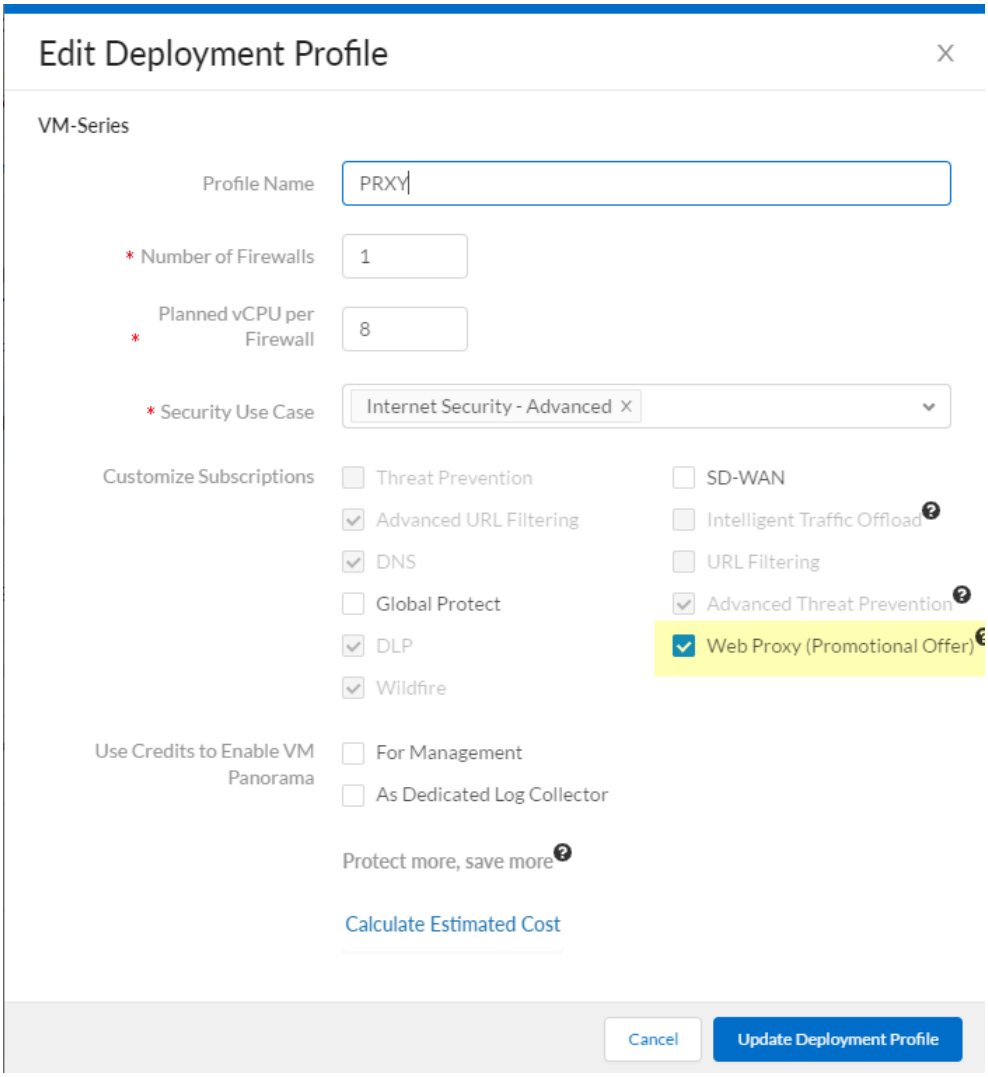
  With transparent proxy, the client browser is not aware of the proxy. Transparent proxy supports inline mode deployment and does not support web cache communication

protocol (WCCP). Transparent proxy is transparent to the user without requiring additional authentication.

1. If you have not already done so, activate the license for web proxy.

   This step is required for the PA-1400, PA-3400, and VM Series. The following steps are for the VM series; for the PA-1400 and PA-3400, follow the steps to activate subscription licenses.

   1. Log in to the Customer Service Portal (CSP).
   2. **Edit** the deployment profile.
   3. Select **Web Proxy (Promotional Offer)**.



   4. Click **Update Deployment Profile**.
   5. On the firewall, retrieve the license keys from the server.

      If the license key retrieval is not successful, restart the firewall and repeat this step before proceeding.

2. Set up zones and interfaces.

As a best practice, use Layer 3 (L3) for all interfaces and configure a separate zone for each interface within the same virtual routers and the same virtual systems.

1. Configure an interface for the client.
2. Configure an interface for the outgoing traffic to the internet.
3. Configure a loopback interface for the proxy.

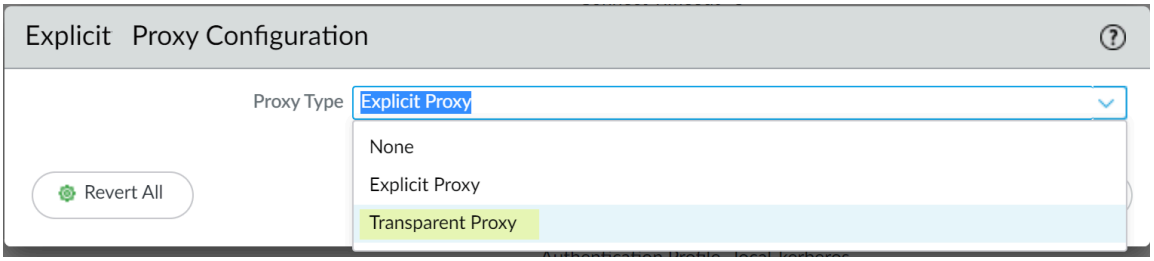
   *All incoming traffic is routed through this interface to the proxy. Be sure to carefully copy the IP address for this interface and save it in a secure location because you must enter it as the **Proxy IP** address when you configure the web proxy.*

3. Set up the DNS proxy for Transparent Proxy.
   1. Configure a DNS proxy object for the proxy connection.
   2. Configure a DNS Server profile with both primary and secondary DNS servers.

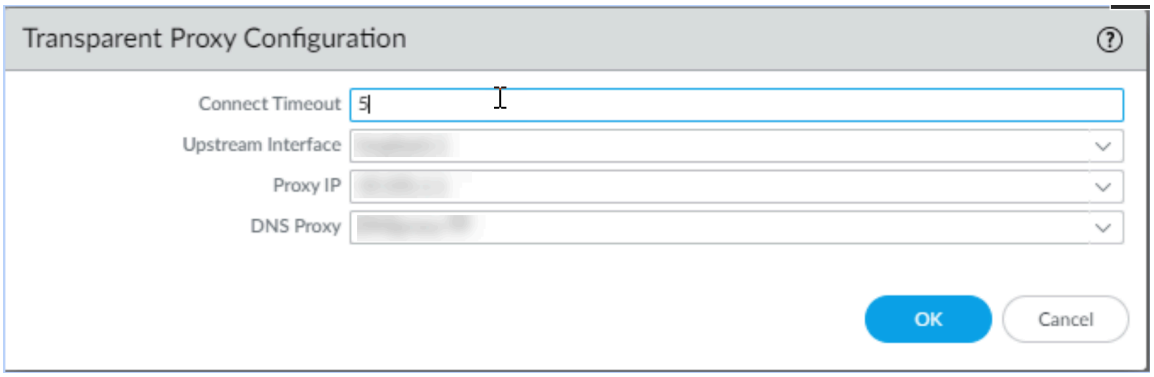
      You must configure both a primary and a secondary DNS server for web proxy.

   3. Specify the loopback interface for the proxy connection.
4. To enable decryption for MITM detection, create a self-signed root CA certificate or import a certificate signed by your enterprise certificate authority (CA). For more information, refer to the best practices for administrative access.
5. Set up the Transparent Proxy.
   1. On the firewall, select **Network** > **Proxy** then **Edit** the **Proxy Enablement** settings.
   2. Select **Transparent Proxy** as the **Proxy Type** then click **OK** to confirm the changes.

      If the only available option is None, verify that you have an active license for the web proxy feature.



   3. **Edit** the **Transparent Proxy Configuration**.



4. Specify the **Connect Timeout** to define (in seconds) how long the proxy waits for a TCP response from the web server. If there is no response after the specified amount of time has elapsed, the proxy closes the connection.
5. Select the **Upstream Interface**.

   The upstream interface must be a loopback interface that is not associated with any other subnets.
6. Specify the IP address of the loopback interface as the **Proxy IP**.

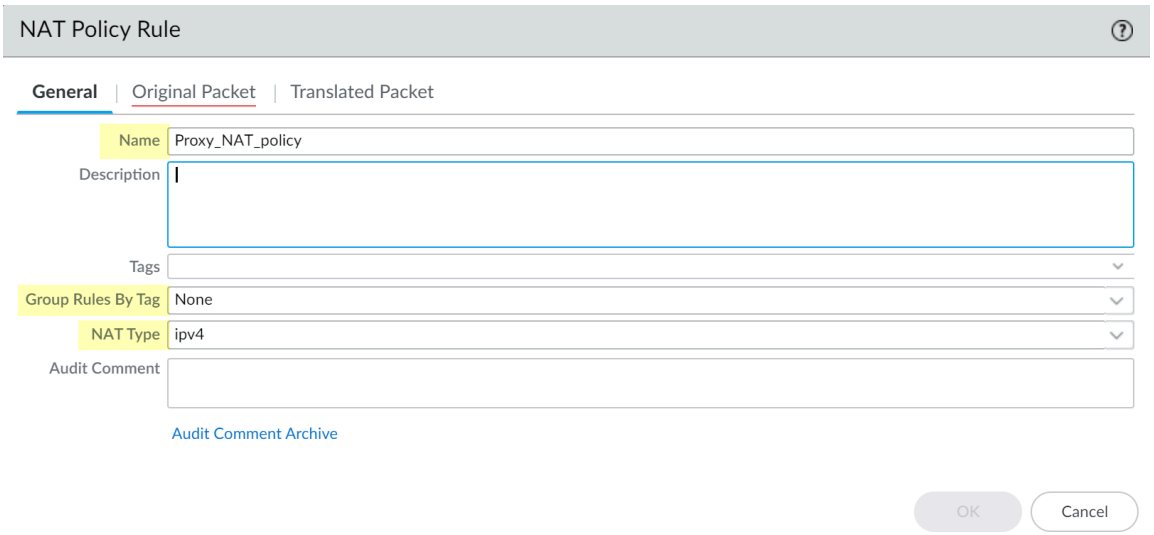
   Enter the IP address of the interface you configured in Step 2.3.
7. Specify the **DNS Proxy** object you created in Step 3.

   *Specify the loopback interface as the **Upstream Interface**.*
8. Click **OK** to confirm the changes.

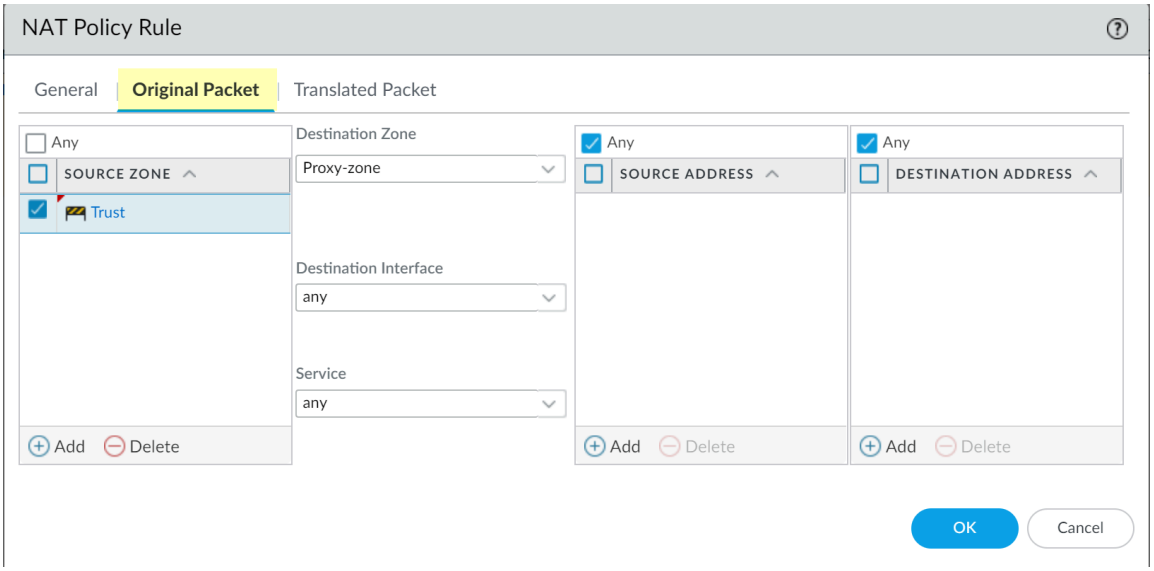
6. Configure the destination network address translation (DNAT) policy.

   You must configure the DNAT policy rule exactly as described in the following steps for the firewall to successfully use the web proxy to route traffic. Be sure to configure the DNAT policy rule so that it precedes the source network address translation (SNAT) policy rule.

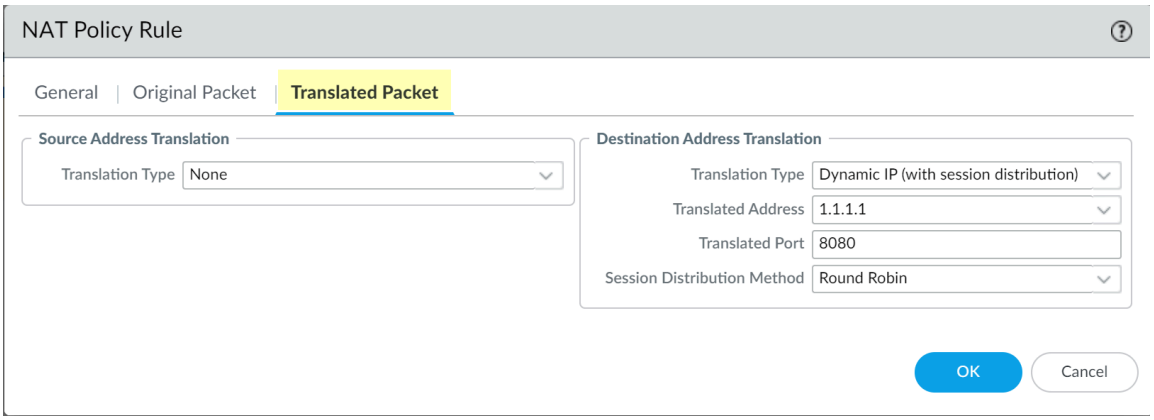
   1. Select **Policies** > **NAT** and **Add** a NAT policy rule.
   2. Enter a unique **Name** and verify that **Group Rules by Tag** is **None** then select the **NAT Type**.



3. Select **Original Packet** and **Add** a trusted zone as the **Source Zone** and the **Destination Zone** as the interface that contains the web proxy.



4. Select **Translated Packet** and verify that **Translation Type** for **Source Address Translation** is **None**.



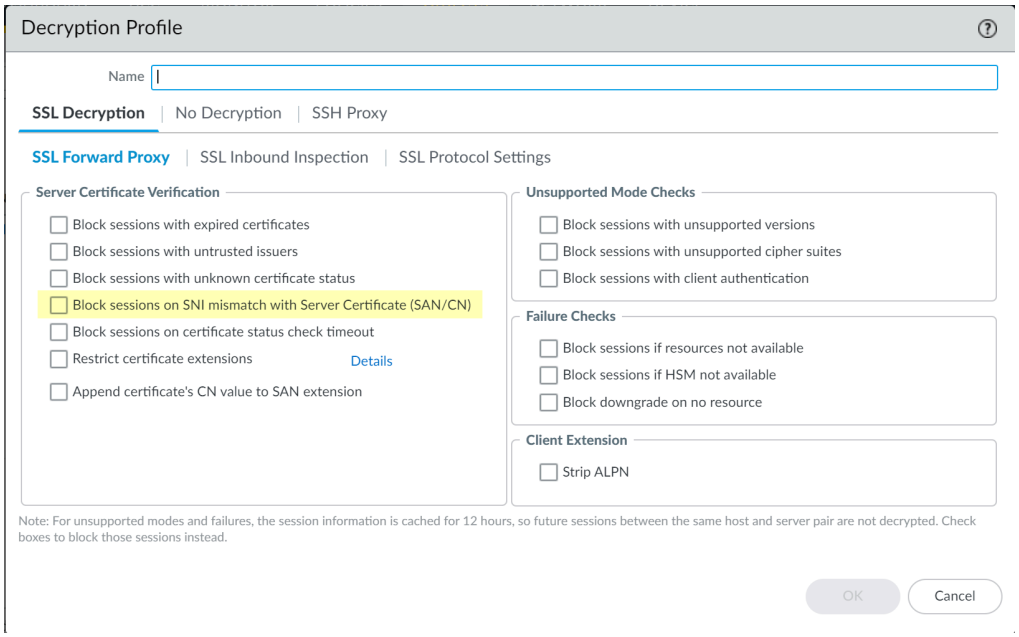
5. Select **Dynamic IP (with session distribution)** as the **Translation Type** for the **Destination Address Translation**.
6. Enter the IP address of the web proxy as the **Translated Address**.

   Enter the same IP address as the Proxy IP address specified in Step 2.3 and Step 5.6.
7. Enter **`8080`** as the **Translated Port**.
8. Select a **Session Distribution Method** (for example, **Round Robin**).

   The session distribution method is not applicable for web proxy.
9. Click **OK** and **Commit** the changes.

7. Configure a security policy to allow and route the proxy traffic.
   1. Configure a source network address translation (SNAT) policy rule after the DNAT rule.
   2. Configure a decryption policy to decrypt traffic.

      Select the zone that contains the proxy interface as the source zone.
   3. (Optional but recommended) Select **Objects** > **Decryption Profile** and select **Block sessions on SNI mismatch with Server Certificate (SAN/CN)** to automatically deny any sessions where the Server Name Indication (SNI) does not match the server certificate.



4. Configure policy rules to allow access to the DNS proxy servers for both the client and the proxy.
5. Configure a policy rule to allow traffic from the client to the proxy.
6. Configure a policy rule to allow traffic from the proxy to the internet.

Power Over Ethernet (PoE)

You can configure Power Over Ethernet (PoE) on the interfaces of supported firewalls to transfer electrical power from the firewall to a connected network device. This allows you to meet the power needs of other devices while continuing to transmit data to them using a single Ethernet cable per physical PoE port.

This table lists each Palo Alto Networks® Next-Generation firewall with PoE ports as well as the maximum power they offer, the total allowed power budget, and the interface types they support.

Firewall	PoE Ports	Maximum Reserved Power (per port)	Total PoE Budget Allowed (all ports)	Supported Interface Types
PA-415 and PA-445	6, 7, 8, and 9	60W	91W	• Aggregate Ethernet (AE) • High Availability (HA) • Layer 3 • Tap • Virtual Wire
PA-1410 and PA-1420	9, 10, 11, and 12	90W	151W	

The following task describes the procedure for setting up PoE on your firewall.

STEP 1 | Ensure that the device you want to provide power to is connected to the firewall using an Ethernet cable through a supported PoE port on the firewall.

Using a Cat5 or Cat6 Ethernet cable ensures the most reliable power transfer. A Cat3 cable, for example, will only be able to transfer as much as 20W.

STEP 2 | Select **Network** > **Interfaces** > **Ethernet** and choose the interface you have cabled.

STEP 3 | PoE is active on all PoE ports by default. On the Ethernet Interface window, selecting **Advanced** and viewing **PoE Settings** shows that **PoE Enable** is already enabled.

STEP 4 | Set the amount of power reserved by the port by entering a value (in Watts) for **PoE Rsvd Pwr**. This value must be a number between **0** and the Maximum Reserved Power of the port as defined in the table above. A **0** indicates that no power will be sent through the port connection.

*The total **PoE Rsvd Pwr** of all of your PoE ports should not exceed the Total PoE Budget Allowed in the table above. If you go over the Total PoE Budget Allowed, one or more powered devices will enter the **Den** (Power Denied) state until you reallocate the reserved power.*

*If no device is connected to a PoE port, ensure that either **PoE Enable** is disabled or the **PoE Rsvd Pwr** value is **0** to avoid consuming a portion of the PoE budget.*

STEP 5 | Click **OK**.

STEP 6 | **Commit** your changes.

Panorama Features

- Admin-Level Commit with Policy Reordering
- Static Security Group Tag (SGT) for TrustSec Plugin

Admin-Level Commit with Policy Reordering

The Panorama management server running PAN-OS 11.0.1 enables Panorama admin to commit or revert their own policy rulebase reordering configuration changes. This enables and supports concurrent Panorama admins making policy reordering changes and does not require you to commit or revert all configuration changes on Panorama when policy rulebase reordering is required. Additionally, this allows you to accurately track and audit policy rulebase reordering changes made by each individual admin. Admin-level commit and revert of policy reordering changes is supported when adding a new policy rule between existing rules, moving and reordering existing policy rules, and deleting an existing policy rule. A configuration log is generated when an admin-level commit or revert for a policy rulebase reordering is performed.

When you preview your configuration commit, a policy rule added between existing policy rules is displayed as a modified configuration object rather than an added configuration object. For example, `Policy1` and `Policy2` are existing policy rules. A Panorama admin later creates `Policy3` and adds the policy rule between `Policy1` and `Policy2`. When the Panorama admin goes to preview the configuration changes, `Policy3` is displayed as a modified configuration object.

Panorama must be running PAN-OS 11.0.1 to perform an admin-level commit when a policy rulebase is reordered and then push the change to managed firewalls.

STEP 1 | Log in to the Panorama web interface.

STEP 2 | Reorder a policy rulebase.

- **Reorder a Policy Rulebase—** In your **Policies**, reorder a policy rulebase.
  - **Add** a new policy rule in-between existing policy rules.
  - Select and **Delete** a policy rule ordered between two other policy rules.

    Deleting a policy rule at the bottom of your policy rulebase is not considered reodering.
  - Select and **Move** a policy rule.
- **Revert the Panorama Configuration**—Select **Panorama** > **Setup** > **Operations** and revert the Panorama configuration.

  Please note that any other configuration changes associated with the device group are also reverted.

  1. **Revert to last saved Panorama configuration** or **Revert to running Panorama configuration**.
  2. **Select Device Groups & Templates**.
  3. Select the device group the policy rulebase you reordered is a part of and click **OK**.
  4. You are prompted that the specified device group is reverted. Click **OK** to continue.

STEP 3 | Select **Commit** and **Commit to Panorama**.

STEP 4 | Select **Commit Changes Made By** and verify the device group and associated policy rulebase reordering changes are displayed in the Commit Scope

STEP 5 | **Commit.**

Static Security Group Tag (SGT) for TrustSec Plugin

The Panorama plugin for Cisco TrustSec enables you to create security policy for your TrustSec environment using dynamic or static address groups. The plugin monitors for changes in TrustSec security groups and registers that information with Panorama. It forwards IP information to the firewall, so Panorama can apply the correct policy to corresponding endpoints. The Panorama plugin for Cisco TrustSec supports up to 16 pxGrid (Cisco ISE) servers.

Differences between dynamic and static addresses

The mapping received from the Cisco ISE Server is converted before being processed by the Panorama plugin framework. This conversion, representing a custom tag, is based on the pxGrid server name and the Security Group Tag (SGT) received:

```
cts.svr_<server-name>.sgt_<SGT-name>
```

SGT names are represented in a Cisco ISE Server in 3 different formats:

- String (for example, BYOD).
- Decimal number (for example, 15).
- Hexadecimal number (for example, 000F).

The format of the SGT name depends on the type of SGT:

- The com.cisco.ise.session service, used by dynamic SGTs, returns the tag in a string format. As a result, the matching criteria for a dynamic SGT is cts.svr_<server-name>.sgt_BYOD.
- The com.cisco.ise.sxp service, used by static SGTs, returns the tag in a decimal format. As a result, the matching criteria for a static SGT is cts.svr_<server-name>.sgt_15.

You can include both dynamic and static SGTs in the same address group, however, the matching criteria must include both formats. For example:

```
‘cts.svr_<server-name>.sgt_BYOD’ or ‘cts.svr_<server-name>.sgt_15’
```

Create a dynamic or static address group

STEP 1 | Create active sessions so that Panorama can learn SGT tags for dynamic or static address group definition. To create active sessions, use ISE to authenticate devices. Panorama does not collect default SGT tags on ISE. Create address groups and verify that they are added.

STEP 2 | Select **Objects > Address Groups.**

STEP 3 | Select the Device Group you created for monitoring endpoints in your Cisco TrustSec environment from the **Device Group** drop-down.

STEP 4 | Click **Add** and enter a **Name** and **Description** for the address group. The dynamic address group naming convention is cts.svr_(server-name).sgt_<SGT-name>. Static address group naming convention is: cts.svr_<server-name>.sgt_<SGT-decimal number>.

STEP 5 | Select **Type** as **Dynamic** or **Static** in the drop-down.

STEP 6 | Click **Add Match Criteria**.

STEP 7 | Select the **And** or **Or** operator and click the plus (+) icon next to the security group name to add it to the dynamic or static address group. Panorama can only display security group tags it has learned from active sessions. Security group tags in live sessions appear in the match criteria list.

STEP 8 | Click **More** in the **Addresses** column of the address group. Panorama displays a list of IP addresses added to that address group based on the match criteria you specified.

STEP 9 | Use dynamic or static addresses groups in policy. Dynamic address groups are empty until you attach them to a policy. You won't see dynamic address groups unless a policy is using it. To use a address group in policy:

1. Select **Policies > Security.**
2. Click **Add**. Enter a **Name** and a **Description** for the policy.
3. Add the **Source Zone** to specify the zone from which traffic originates.
4. Add the **Destination Zone** at which traffic is terminating.
5. For the **Destination Address**, select the address group you just created.
6. Specify the action, **Allow** or **Deny**, for the traffic. Optionally attach the default security profiles to the rule.
7. Repeat steps a-f to create another policy rule.
8. Click **Commit**.

STEP 10 | Optionally update the objects from the pxGrid server at any time by synchronizing objects. Synchronizing objects enables you to maintain context on changes in the virtual environment and allows you to enable applications by automatically updating the address groups used in policy rules.

STEP 11 | Select **Panorama > Cisco TrustSec > Monitoring Definition.**

STEP 12 | Click **Synchronize Dynamic Objects.**

Management Features

Skip Software Version Upgrade

In PAN-OS 11.0, you can now skip up to three software versions when upgrading or downgrading standalone devices or Panorama managed devices running PAN-OS 10.1 or a later release. This feature builds on the Simplified Software Upgrade process introduced in PAN-OS 10.2, which includes capabilities such as a multi-image download option and a pre-install validation check, to make the upgrade process even faster.

TLSv1.3 Support for Management Access

PAN-OS 11.0 introduces two settings that let you secure web connections to your management interface with TLSv1.3. The Management TLS Mode setting allows you to set TLSv1.3 as your preferred TLS protocol, and the Certificate setting accepts a TLSv1.3 certificate. The settings function similarly to an SSL/TLS service profile but only apply to web interface management connections.

Configuring an SSL/TLS service profile is the only way to customize individual TLS protocols and algorithms for other firewall and Panorama services, such as Authentication Portal and GlobalProtect.

TLSv1.3 delivers several performance and security improvements, including shorter SSL/TLS handshakes and more secure cipher suites. Palo Alto Networks supports the following TLSv1.3 cipher suites for management access:

- TLS-AES-128-CCM-SHA256
- TLS-AES-128-GCM-SHA256
- TLS-AES-256-GCM-SHA384
- TLS-CHACHA20-POLY1305-SHA256

For the Management TLS Mode setting, you can choose among three options: `tlsv1.3_only`, `mixed-mode`, and `exclude_tlsv1.3`.

- `tlsv1.3_only` allows web management interface connections secured only by TLSv1.3. If a client cannot negotiate TLSv1.3 ciphers, the connection fails.

  This mode is ideal for passing PCI audits.

- `mixed-mode` allows web management interface connections secured by any TLS protocol version (TLSv1.0-TLSv1.3). For example, if a client's browser only supports TLSv1.2, the firewall negotiates the connection with TLSv1.2 and its associated cipher suites.
- (Default) `exclude_tlsv1.3` disables TLSv1.3 support, allowing web management interface connections secured by either TLSv1.0, TLSv1.1, or TLSv1.2. This mode is the default configuration for PAN-OS 11.0 and maintains the functionality of previous releases.

  The Certificate setting is only available for modes that support TLSv1.3. In `exclude_tlsv1.3` mode, configure an SSL/TLS service profile to specify a certificate and restrict TLS protocol versions and cipher suites.

STEP 1 | Log in to your management interface.

STEP 2 | Edit the General Settings (**Device** > **Setup** > **Management**).

You can also configure these settings on the Panorama™ web interface (**Panorama** > **Setup** > **Management**).

STEP 3 | For **Management TLS Mode**, select either `tlsv1.3_only` or `mixed-mode`, and then click **OK**.

STEP 4 | For **Certificate**, select your management server certificate, and then click **OK**.

STEP 5 | **Commit** your changes.

STEP 6 | Inspect the security details for your server to confirm that TLSv1.3 is in use.

For example, on Google Chrome, you can click the lock symbol to the left of the address bar. Then, click **Connection is secure**. Next, click **Certificate is valid**. The Details section displays certificate fields, such as the TLS version and signature algorithm.

Policy Rulebase Management Using Tags

Tags allow you to identify the purpose or function of a policy rule and help you better organize your policy rulebase. PAN-OS 11.0.3 introduces the ability to visually group and manage your policy rulebase using the assigned tags from the Tag Browser. When viewing your policy rulebase using tags, you can perform operation procedures such as adding, deleting, or moving the rules with the applied tag more easily. Viewing your policy rulebase using tags maintains the rule evaluation order.

For firewalls managed by a Panorama management server, you can create and assign tags to policy rules from Panorama. Both Panorama, managed firewalls, and standalone firewalls running PAN-OS 11.0.3 or later 11.0 release support policy rulebase base management using tags. Policy rulebase management using tags is supported for all policy types.

STEP 1 | Log in to the Panorama or firewall web interface.

STEP 2 | Create your policy rulebase.

- Create a Security Policy Rule
- Create a Network Address Translation (NAT) Policy Rule
- Create a Quality of Service (QoS) Policy Rule
- Create a Policy Based Forwarding (PBF) Policy Rule
- Create a Decryption Policy Rule
- Create an Application Override Policy Rule
- Create an Authentication Policy Rule
- Create a Denial-of-Service (DoS) Policy Rule

STEP 3 | Create and apply tags to the policy rules you created.

*You must apply tags to the policy rule **Tag** field and not the **Group Rules by Tag** field.*

STEP 4 | Select **Policies** and change the policy rulebase view from the `Default View` to **Rulebase by Tags**.

On the left-hand size, the **Tag Browser** is displayed and all tags applied to all rules in the policy rulebase, the number of policy rules with the tag applied, and the `Rule Number` indicating the rule order for all policy rules within the policy rulebase with the tag applied.

STEP 5 | Select the Tag Browser display settings.

1. (Optional) Use the search bar to search for a specific tag.
2. Keep enabled or disable **Filter by first tag in rule**.

   When enabled, the Tag Browser displays the `Rule Count` and `Rule Number` data based on the first tag applied to each policy rule when multiple tags are applied. When

disabled, the Tag Browser displays total `Rule Count` and `Rule Number` data when multiple tags are applied to your policy rules.

3. Select how to order tags in the Tag Browser.
   - **Rule Order**—Order the policy rule tag data in the Tag Browser data based on how policy rules are ordered in the policy rulebase. This may mean that a tag applied to multiple policy rules will display multiple times in the Tag Browser if the tagged policy rules are dispersed throughout the policy rulebase.
   - **Alphabetical**—Order the policy rule tag data in the Tag Browser based on the alphabetical order of applied tags.

STEP 6 | Apply or remove tags from the Tag Browser.

The Tag Browser allows you to both apply a tag to policy rules within the policy rulebase, and remove a tag from all policy rules where the tag is currently applied.

- **Apply a tag from the Tag Browser**

  You can also drag and drop tags you want to apply from the Tag Browser to the policy rule you want to apply it to.

  1. In the policy rulebase, select one or more policy rules that you want to apply a tag to.
  2. In the Tag Browser `Tag (Rule Count)` column, select one or more tags you want to apply to the selected policy rules.
  3. Expand the tag options and **Apply Tag to the Selection(s)**.

     Review which tags you are apply to the selected policy rules and click **Yes** to apply the tags.

- **Remove tags from the Tag Browser**

  1. In the Tag Browser `Rule Number` column, expand the tag options and **Untag Rule(s)**.
  2. A confirm window is displayed to confirm you want to untag your policy rules.

     You can remove the tags from only the selected policy rules or check **Untag all the rules with the selected tag** to remove the tag from all policy rules with the tag.
  3. Click **Yes** to untag all policy rules that have the selected tag applied.

STEP 7 | Move tagged rules within your the policy rulebase.

You can use the Tag Browser to move multiple tagged rules at once to change the policy rulebase hierarchy as needed.

1. Select the **Rule Order** Tag Browser display setting.
2. In the Tag Browser `Rule Number` column, expand the tag options and **Move Rule(s)**.

   Alternatively, you can drag and drop rules to reorder them in the policy rulebase.

3. Select the tag around which you want to move.
4. **Move Before** or **Move After** as needed.

STEP 8 | Add a new policy rule from the Tag Browser.

You can add a new policy rule with tags already assigned directly from the Tag Browser. The new policy rule is added as the lowest rule in the rule order based on the selected tag.

1. Select the **Rule Order** Tag Browser display setting.
2. In the Tag Browser `Rule Number` column, expand the tag options and **Add New Rule** and configure the policy rule as needed.

STEP 9 | Filter the policy rulebase using a tag.

In the Tag Browser `Rule Number` column, expand the tag options and **Filter** the policy rulebase. This allows you to apply one or more tag search filters to the policy rulebase to narrow down the list of policy rules displayed.

Certificate Management Features

- Support for OCSP Verification through HTTP Proxy

Support for OCSP Verification through HTTP Proxy

PAN-OS 11.0 adds support for Online Certificate Status Protocol (OCSP) certificate revocation checks through HTTP/S proxies. If your network deployment consists of a web proxy, you can configure OCSP to validate certificates. All OCSP requests and responses will pass through your proxy server. The benefits of checking certificate status using OCSP instead of or in addition to certificate revocation lists (CRLs) include real-time status responses and reduced usage of network and client resources.

The workflow of OCSP certificate validation through a web proxy is as follows:

1. An authenticating client (firewall) forwards an OCSP request to the proxy. The request contains the serial number for the certificate the client wants to validate.
2. The proxy validates the request and identifies the OCSP responder for the certificate authority (CA) that issued the certificate.
3. The proxy forwards the OCSP request to the responder, and the OCSP responder looks up the revocation status for the certificate in the CA database.
4. The OCSP responder sends the certificate status (`good`, `revoked`, or `unknown`) to the proxy.
5. The proxy forwards the certificate status to the client.

The following procedure assumes you have not set up a web proxy.

STEP 1 | Configure an HTTP proxy (**Device** > **Setup** > **Services**).

You can use the following CLI commands to configure a proxy server for OCSP status checks (and CRL downloads).

- **set deviceconfig system secure-proxy-server *<value>***
- **set deviceconfig system secure-proxy-port *<1-65535>***
- **set deviceconfig system secure-proxy-user *<value>***
- **set deviceconfig system secure-proxy-password *<value>***

STEP 2 | Configure an OCSP responder.

If your enterprise has its own public key infrastructure (PKI), you can configure a firewall as an OCSP responder.

STEP 3 | Configure revocation status verification of certificates.

Cloud Identity Features

- User Context for the Cloud Identity Engine

User Context for the Cloud Identity Engine

User Context for the Cloud Identity Engine allows you to quickly locate and share important user and device information (such as tags, quarantine lists, and mappings, which now includes Terminal Server agent mappings) across your network for actionable information and consistent user-based policy enforcement.

To learn more about User Context for the Cloud Identity Engine, refer to the Cloud Identity Engine Getting Started guide.

Content Inspection Features

DNS Security Support for DNS Over HTTPS (DoH)

PAN-OS 11.0 and later can now analyze and categorize the DNS payload contained within encrypted DNS traffic requests to DNS hosts using HTTPS (DoH—[DNS-over-HTTPS]). If your organization currently blocks all DoH requests as Palo Alto Networks recommends, you can transition away from that policy as DNS Security now enables you extract the DNS hostname from the encrypted request and apply your organization's existing DNS Security policies. This allows you to safely access more websites as support for DoH widens. DNS Security support for DoH is enabled by configuring the firewall to decrypt the payload of DNS requests originating from a user-specified list of DNS resolvers, providing support for a range of server options. The decrypted DNS payload can then be processed using the Anti-spyware profile configuration containing your DNS policy configuration. DNS requests that have been determined to be DoH are labeled as **dns-over-https** in the traffic logs.

Palo Alto Networks also provides the option to block ECH (Encrypted Client Hello), which is a draft state proposal to encrypt the entire 'client hello' message. While that offers some data privacy, such as ALPN and SNI, it can also prevent certain firewall services that use the client hello from operating as intended. To maintain optimal function of the security services of the firewall, Palo Alto Networks recommends blocking all ECH-supporting record types.

STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | Create a Custom URL Category list that includes all DoH resolvers you want to enable traffic to/from (you will need the DNS server URL(s)).

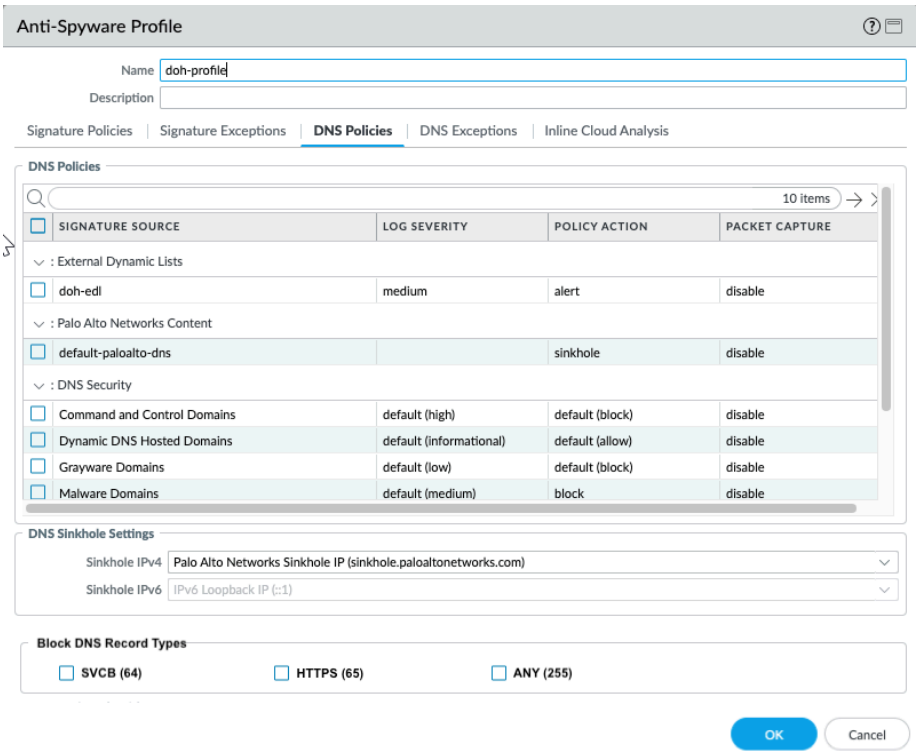
STEP 3 | Create a Decryption Policy Rule that references the custom URL category list that you created in the previous step.

STEP 4 | Update or create a new anti-spyware security profile used to inspect DoH requests.

1. Enable DNS Security.
2. (Optional) Block the specified DNS resource record types record types used to exchange keying information during the encryption of the client hello in the subsequent TLS

connection. The following DNS RR types are available: SVCB (64), HTTPS (65), and ANY (255).

- *While it is not necessary to block ECH in order to enable DNS Security over DoH, Palo Alto Networks currently recommends blocking all DNS record types used by ECH for optimum security.*
- *Type 64 and type 65 resource record standards are still in flux (in a draft state) and are subject to change. For more information on DNS SVCB and HTTPS RRs, refer to:* Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs) *as defined by the* IETF.



3. Click **OK** to exit the anti-spyware profile configuration dialog and **Commit** your changes.

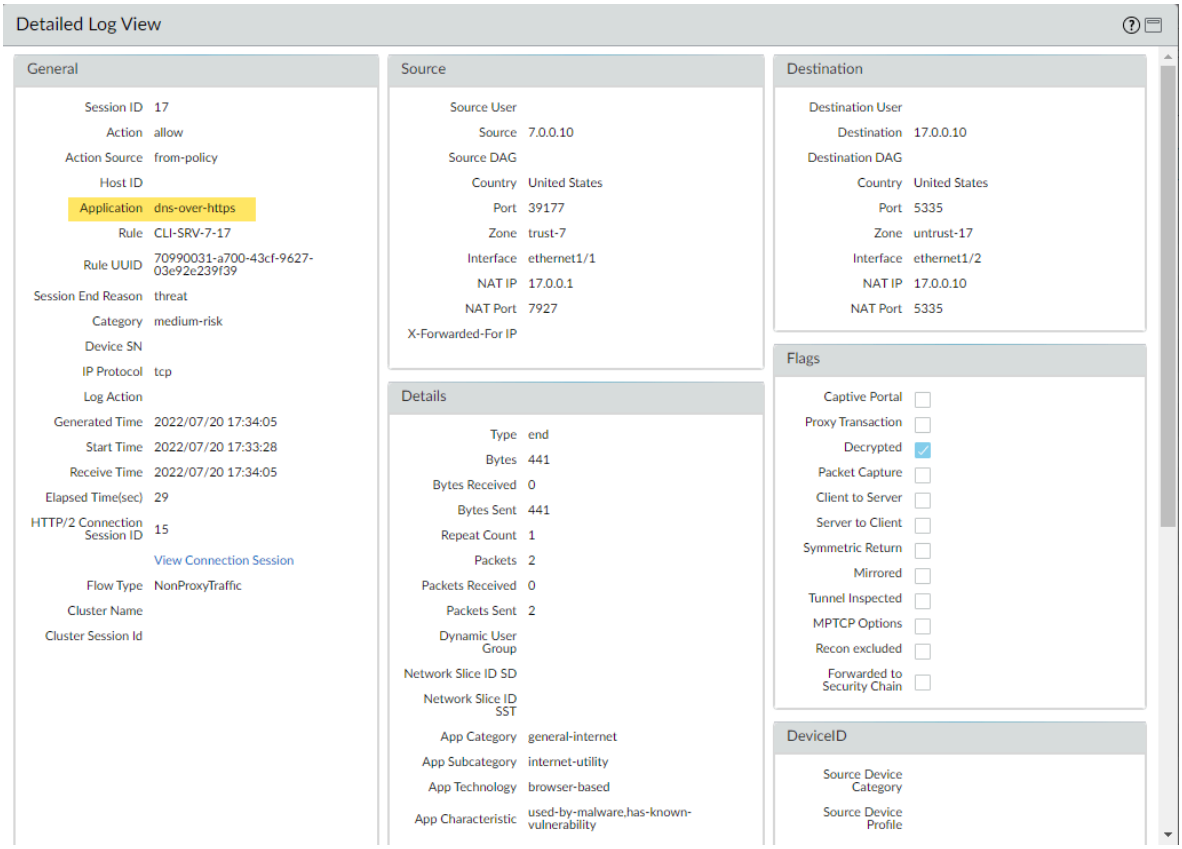
STEP 5 | Create or update a security policy rule and reference an anti-spyware profile with the DNS Security settings and a custom URL category list (**Objects** > **Custom Objects** > **URL Category**) containing the approved list of DoH servers.

STEP 6 | Create a block policy to decrypt HTTPS traffic and block all remaining unsanctioned DoH traffic that is not explicitly allowed by the custom URL category list (referenced in step 5) by using the App-ID: **dns-over-https** and the following URL category: **encrypted-dns**.

If you already have an existing block policy to block DoH traffic, verify that the rule is placed below the previous security policy rule used to match with specific DoH resolvers listed in a custom URL category list object.

STEP 7 | (Optional) Search for activity on the firewall for HTTPS-encrypted DNS queries that have been processed using DNS Security.

1. Select **Monitor** > **Logs** > **Traffic** and filter based on the application using **dns-over-https**, for example, `( app eq dns-over-https )`.
2. Select a log entry to view the details of a detected DNS threat.
3. The **Application** should display dns-over-https in the **General** pane of the detailed log view, indicating that this is DoH traffic that has been processed using DNS Security. Other relevant details about the threat are displayed in their corresponding windows.



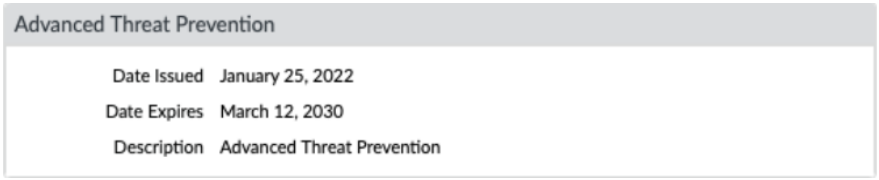
Advanced Threat Prevention Support for Zero-day Exploit Prevention

Palo Alto Networks now operates new inline deep learning detection engines in the Advanced Threat Prevention cloud to analyze traffic for command injection and SQL injection vulnerabilities in real-time to protect users against zero-day threats. By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages or operate process intensive, firewall-based analyzers which can sap resources. Inline cloud analysis for your firewall Vulnerability Protection profile supports two analysis engines: SQL injection and Command injection. Additional analysis models are delivered through content updates, however, enhancements to existing models are performed as a cloud-side update, requiring no firewall update. Inline cloud analysis is enabled and configured using the Vulnerability Protection profile and requires an active Advanced Threat Prevention license.

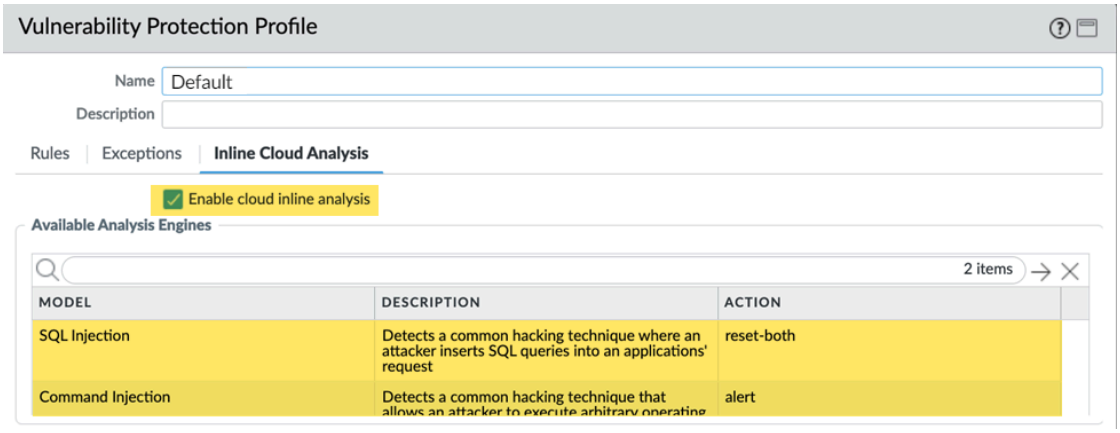
STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | To take advantage of inline cloud analysis of vulnerability exploits, you must have an active Advanced Threat Prevention subscription.

To verify subscriptions for which you have currently-active licenses, select **Device** > **Licenses** and verify that the appropriate licenses are available and have not expired.



STEP 3 | Update or create a new Vulnerability Protection Security profile to enable inline cloud analysis.

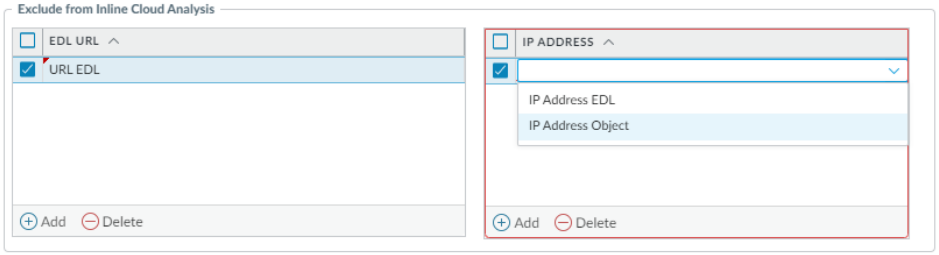


1. Select an existing Vulnerability Protection security profile or **Add** a new one (**Objects** > **Security Profiles** > **Vulnerability Protection**).
2. Select your Vulnerability Protection profile and then go to **Inline Cloud Analysis** and **Enable cloud inline analysis**.
3. Specify an **Action** to take when a vulnerability exploit is detected using a corresponding analysis engine. There are currently two analysis engines available: **SQL Injection** and **Command Injection**.
   - **Allow**—The request is allowed and no log entry is generated.
   - **Alert**—The request is allowed and a Threat log entry is generated.
   - **Reset-Client**—Resets the client-side connection.
   - **Reset-Server**—Resets the server-side connection.
   - **Reset-Both**—Resets the connection on both the client and server ends.
4. Click **OK** to exit the Vulnerability Protection Profile configuration dialog and **Commit** your changes.

STEP 4 | (Optional) Add URL and/or IP address exceptions to your Vulnerability Protection profile if Inline Cloud Analysis produces false-positives. You can add exceptions by specifying an external dynamic list (URL or IP address list types) or an **Addresses** object.

1. Add an **External Dynamic Lists** or [IP] **Addresses** object exception.
2. Select **Objects > Security Profiles > Vulnerability** to return to your Vulnerability Protection profile.
3. Select a Vulnerability profile for which you want to exclude specific URLs and/or IP addresses and then select **Inline Cloud Analysis**.
4. **Add** an **EDL URL** or **IP Address**, depending on the type of exception you want to add, and then select a pre-existing URL or IP address external dynamic list. If none are available,

create a new external dynamic list. For IP address exceptions, you can, optionally, select an **Addresses** object list.



5. Click **OK** to save the Vulnerability Protection profile and **Commit** your changes.

STEP 5 | Install an updated firewall device certificate used to authenticate to the Advanced Threat Prevention inline cloud analysis service. Repeat for all firewalls enabled for inline cloud analysis.

If you have already installed an updated firewall device certificate as part of your IoT Security, Device Telemetry, Advanced Threat Prevention, or Advanced URL Filtering onboarding process, this step is not necessary.

STEP 6 | (Optional) Set the Cloud Content Fully Qualified Domain Name (FQDN) used by the firewall to handle inline cloud analysis service requests. The default FQDN connects to hawkeye.services-edge.paloaltonetworks.com and then resolves to the closest cloud services server. You can override the automatic server selection by specifying a regional cloud content server that best meets your data residency and performance requirements.

The Cloud Content FQDN is a globally used resource and affects how other services that rely on this connection sends traffic payloads.

Verify that the firewall uses the correct Content Cloud FQDN (**Device** > **Setup** > **Content-ID** > **Content Cloud Setting**) for your region and change the FQDN if necessary:

- US—**`us.hawkeye.services-edge.paloaltonetworks.com`**
- EU—**`eu.hawkeye.services-edge.paloaltonetworks.com`**
- UK—**`uk.hawkeye.services-edge.paloaltonetworks.com`**

  The UK-based cloud content FQDN provides Advanced Threat Prevention inline cloud analysis service support by connecting to the backend service located in the EU (eu.hawkeye.services-edge.paloaltonetworks.com).
- APAC—**`apac.hawkeye.services-edge.paloaltonetworks.com`**

STEP 7 | (Optional) Verify the status of your firewall connectivity to the Advanced Threat Prevention cloud service.

Use the following CLI command on the firewall to view the connection status.

```
show ctd-agent status security-client
```

For example:

```
show ctd-agent status security-client

...
Security Client AceMlc2(1)
Current cloud server:          hawkeye.services-
edge.paloaltonetworks.com
Cloud connection:              connected
...
```

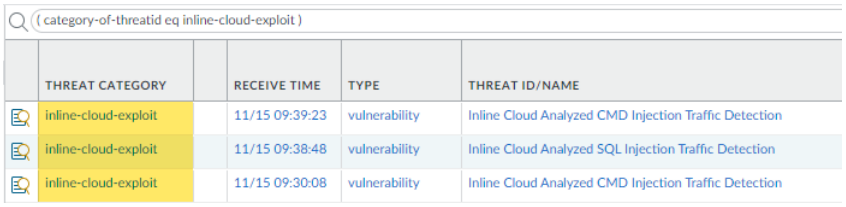
CLI output shortened for brevity.

If you are unable to connect to the Advanced Threat Prevention cloud service, verify that the cloud content FQDN is not being blocked: hawkeye.services-edge.paloaltonetworks.com. If you specified a regional cloud content server in step 6, enter that FQDN instead.

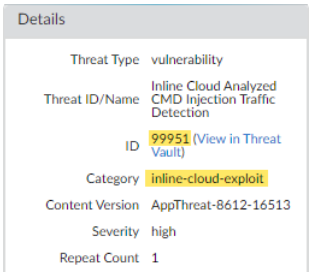
STEP 8 | (Optional) Monitor activity on the firewall for vulnerability exploits that have been detected using inline cloud analysis.

1. Select **Monitor** > **Logs** > **Threat** and filter by `( category-of-threatid eq inline-cloud-exploit )` to view logs that have been analyzed using the inline cloud analysis mechanism of Advanced Threat Prevention. Inline exploit (SQL injection)

threats have an ID of 99950 while inline exploit (command injection) threats have an ID of 99951.



2. Select a log entry to view the details of a vulnerability exploit.
3. The threat **Category** is displayed under the **Details** pane of the detailed log view. Vulnerability exploits that have been detected using inline cloud analysis have a threat category of inline-cloud-exploit.



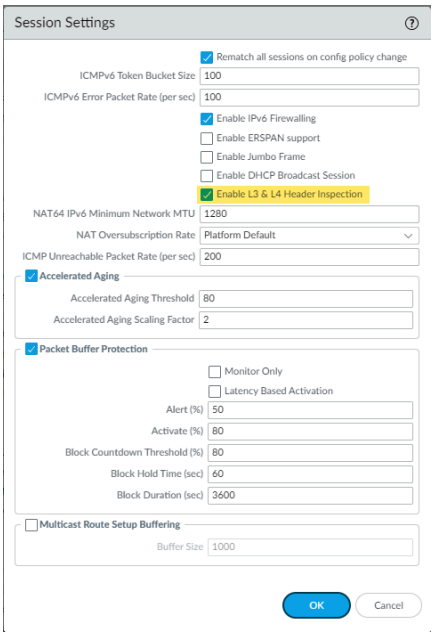
Support for Custom Layer 3 and Layer 4 Threat Signatures

As part of zone security enhancements, you can now write custom threat (vulnerability) signatures based on Layer 3 and Layer 4 header fields (such as IP flags, acknowledgment numbers, etc). This enables you to provide improved vulnerability signature coverage resulting from old and deprecated TCP/IP stacks used in embedded / IoT devices.

Custom L3 & L4 vulnerability signatures are expressed through your Zone and Zone Protection profile configuration. You must specify how the firewall responds when it detects a threat.

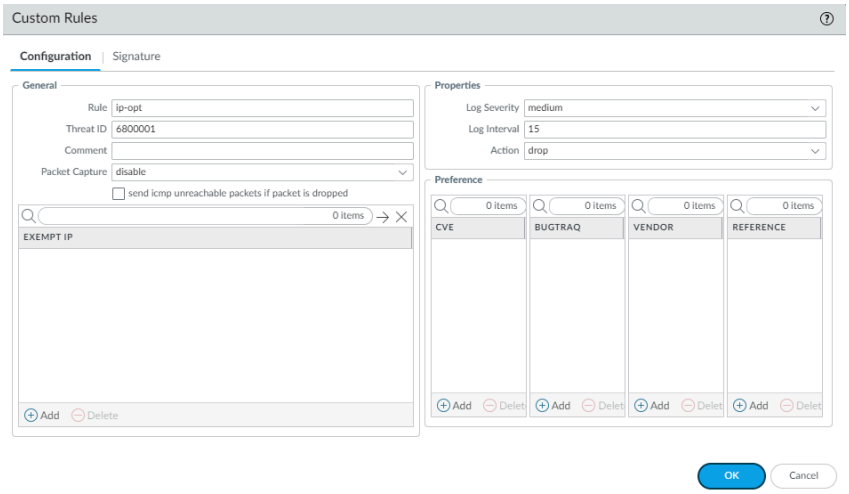
STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | Select **Device** > **Setup** > **Session** and enable **L3 & L4 Header Inspection** globally on the firewall.



STEP 3 | Create a Zone Protection profile and configure the L3 & L4 header inspection settings.

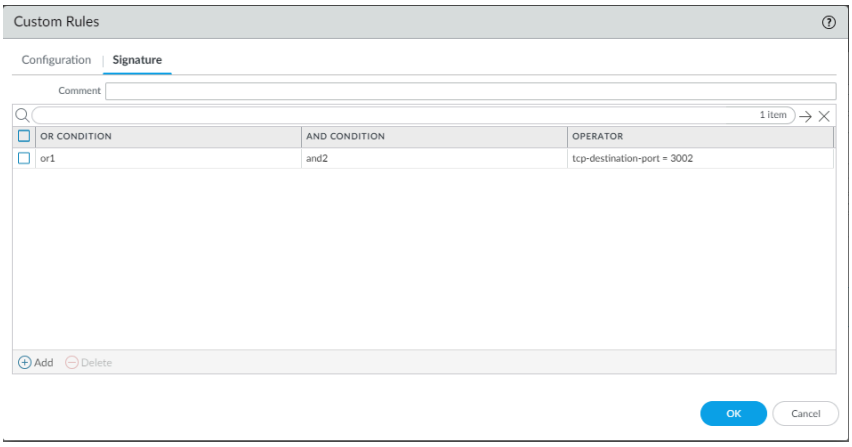
1. Select **Network** > **Network Profiles** > **Zone Protection** and either select an existing profile or **Add** a new profile.
2. If you are creating a new zone protection profile, enter a **Name** for the profile and an optional **Description**.
3. Select **L3 & L4 Header Inspection** to define your custom vulnerability signatures.
4. **Add** new custom rules by defining the configuration and signature details for each entry, which are performed in their respective tabs: **Configuration** and **Signature**.
5. Under **Configuration**, fill out the following required fields in the General, Properties, and Preference section.



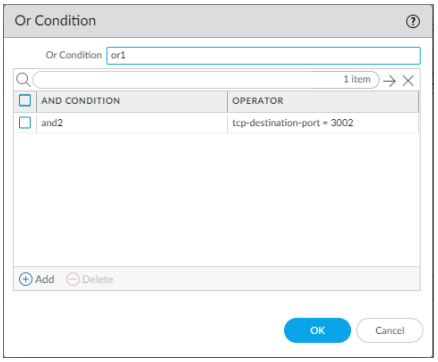
- **Rule**—Specify the custom rule name.
- **Threat ID**—Enter a numeric ID between 41000 and 45000 or 6800001 and 6900000.
- **Comment**—Optionally, add a description of the custom rule.
- **Packet Capture**—Select a packet capture setting.

  *Optionally, select **send icmp unreachable packets if packet is dropped** to send an ICMP unreachable response to the client upon packet loss.*
- **Exempt IP**—Enter the IP address(es) for which you do not want the custom rule to apply to.
- **Log Severity**—Select the severity of the threat.
- **Log Interval**—Indicates how frequently an event is logged.
- **Action**—Choose the action to take when there is a custom signatures match. Options include alert, drop, reset-client, reset-server, and reset-both. Refer to Security Policy Actions for more information about these action settings.
- **Preference**—Add references to provide context or related information about the custom threat signature. You can add CVEs, Bugtraq citations, 3rd party vendor IDs, or reference links to additional analysis or background information.

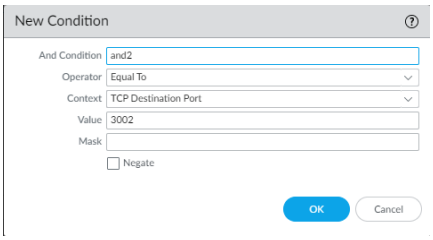
6. From the **Signature** tab, provide a name or description of the custom vulnerability under **Comment**. After specifying a name, select **Add** to provide the custom signature details.



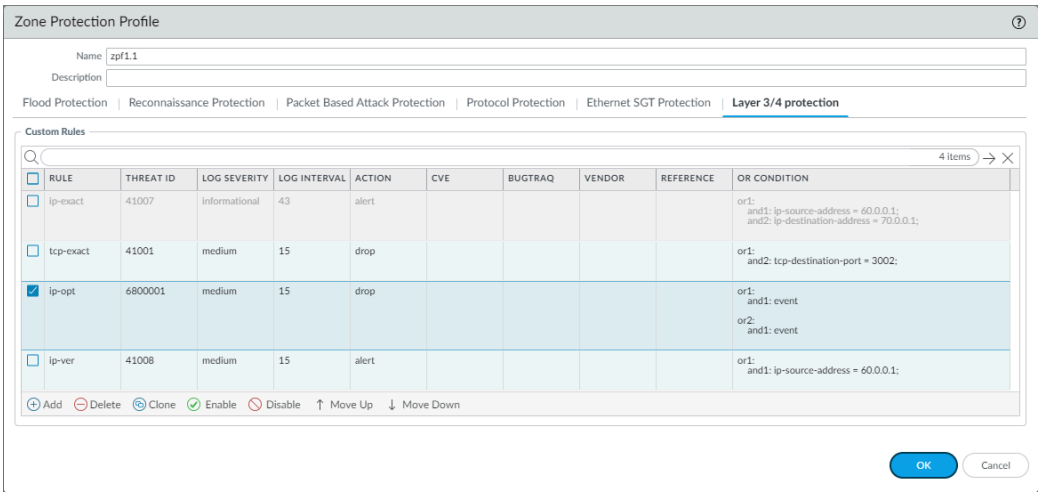
- Specify a matching Or Condition. When finished, select **Add** to configure an And Condition and the associated values in a new window.



- If you select a **Less Than** or **Greater Than** operator, specify a **Context** and a **Value**. The **Equal To** operator additionally has **Mask** and **Negate** options. Click OK when you have finished configuring the new and condition.

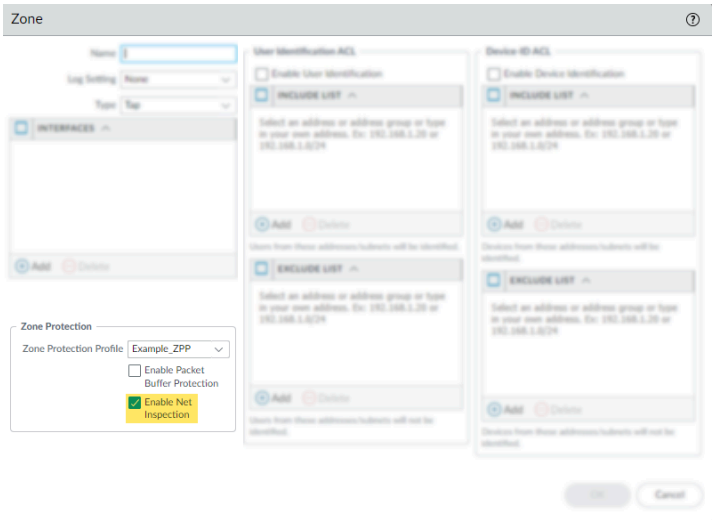


7. Repeat for each matching condition that you want to add.
8. Click **OK** and review your signatures. Click **OK** again to return to the zone protection profile.
9. From the **L3 & L4 Header Inspection** tab, you can reorder, disable, and clone the custom rule entries as necessary. Click **OK** to exit the zone protection profile.



STEP 4 | Apply the Zone Protection profile to a security zone that is assigned to interfaces you want to protect.

1. Select **Network** > **Zones** and select the zone where you want to assign the Zone Protection profile.
2. **Add** the **Interfaces** belonging to the zone.
3. For **Zone Protection Profile**, select the profile you just created.
4. Select **Enable Net Inspection** to enable the L3 & L4 header inspection configuration settings.



5. Click **OK**.

STEP 5 | **Commit** your changes.

STEP 6 | Test your custom threat signature.

IoT Security Features

IoT Security Policy Rule Recommendation Enhancements

One of the benefits of integrating IoT Security with next-generation firewalls is the automatic creation of Security policy rules to extend the framework of zero-trust and least-privilege access to IoT devices. Instead of figuring out the types of traffic that each IoT device generates and their destinations on your own, you simply let IoT Security use AI and machine learning to do it for you and create a set of policy rule recommendations based on observed network behaviors. You can then keep the set of recommended rules as is or change its name and add tags, security profiles, and source and destination zones as you like. When done, activate the policy rules set and let IoT Security automatically push it to Panorama or directly to your firewalls. It's then up to you to select which rules you want to enforce and import them into your policy rulebase. In this release, it's easier than ever to manage and scale policy rule recommendations from IoT Security thanks to the following enhancements:

- IoT Security automatically pushes only rule recommendations that you've activated in IoT Security to Panorama and next-generation firewalls.
- Policy rule names are automatically generated through a concatenation of the policy set name and application name.
- You can import multiple rules from the policy recommendation database in Panorama to multiple device groups. From the Panorama web interface, you can also remove the mapping between multiple rules in the rulebase and the policy recommendation database.
- You can import multiple rules from the policy recommendation database on an individual firewall into your policy rulebase. From the PAN-OS® web interface, you can also remove the mapping between multiple rules in the rulebase and the policy recommendations database.

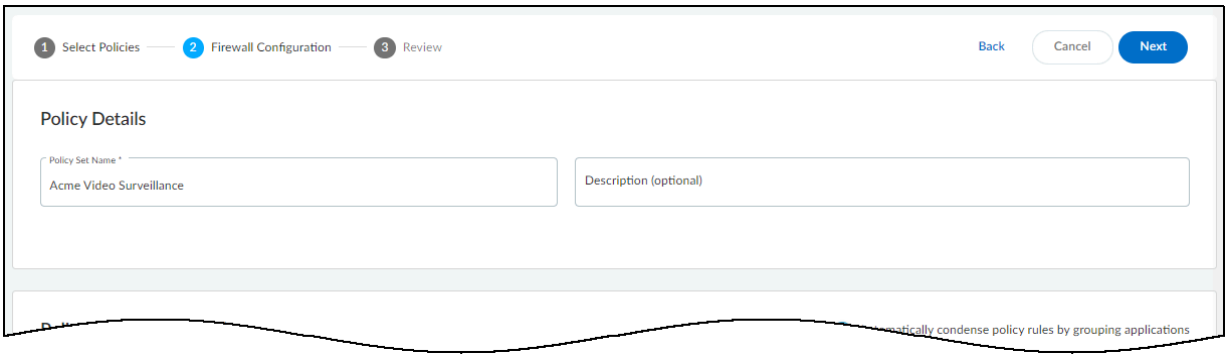
The following section describes policy recommendation enhancements in more detail.

- **Activated Policy Rule Sets Get Pushed Automatically**

  Although IoT Security allows you to create multiple policy rule sets for a device profile, you can only activate one at a time. When you activate a policy set in IoT Security, IoT Security automatically pushes it to Panorama and all next-generation firewalls subscribed to the IoT Security service. Because Panorama and firewalls have only activated policy sets, the Activate Recommendation column no longer appears on **Panorama** > **Policy Recommendation** > **IoT** in Panorama nor on **Device** > **Policy Recommendation** > **IoT** in the PAN-OS web interface.

Automatically Generated Rule Names

When you create a policy rule set in IoT Security, IoT Security assigns it a default name. You can either keep the default name or change it to something else.



When you activate the policy set and IoT Security automatically pushes it to Panorama and your next-generation firewalls, it generates policy rule names by concatenating the policy set name with the name of the application in each rule. These names appear in the Policy Rule Name column on **Panorama** > **Policy Recommendation** > **IoT** in Panorama and on **Device** > **Policy Recommendation** > **IoT** in the PAN-OS web interface.

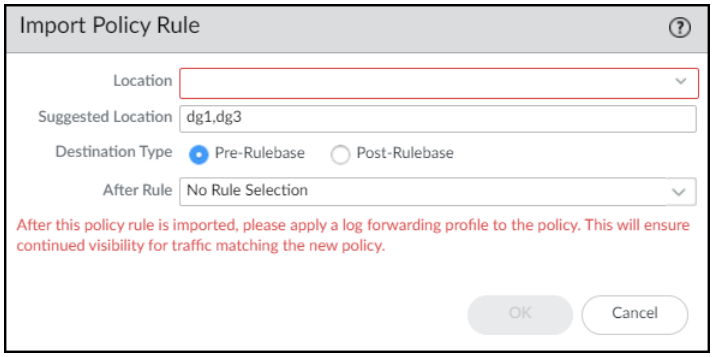
Import Multiple Rules into Multiple Device Groups

The ability to import policy rules into multiple firewall rulebases in multiple device groups can save you a lot of time. From this release, Panorama lets you do just that. You can now import one or more recommended policy rules—up to a maximum of ten at a time—into the rulebase of firewalls in one or more device groups.

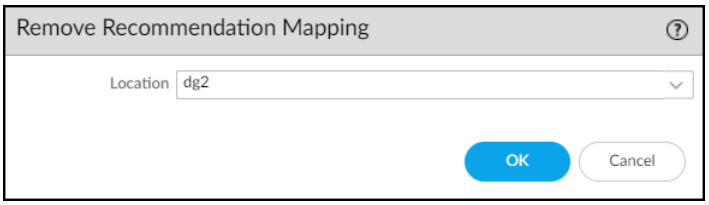
1. In Panorama, select **Panorama** > **Policy Recommendation** > **IoT**, select up to ten policy rules to import and then **Import Policy Rule(s)**.
2. In the Import Policy Rule dialog box that appears, enter the following, and then click **OK**:
   - **Location**: Choose one or more device groups.
   - **Suggested Location**: IoT Security learns about zones and device groups in the logs it receives from next-generation firewalls and suggests device groups for various policy

rules accordingly. You can choose these suggested device groups among those available in the **Location** list or any other device groups if you prefer.

- **Destination Type**: Select either **Pre-Rulebase** to add the recommended policy rules before rules defined locally on a firewall or **Post-Rulebase** to add them after rules defined locally.
- **After Rule**: Choose a rule after which you want to add the imported rule or rules. If you choose **No Rule Selection**, the firewall imports the selected rules to the top. This is an optional setting. If you don't choose a rule, the imported rules are added to the top of the rulebase.



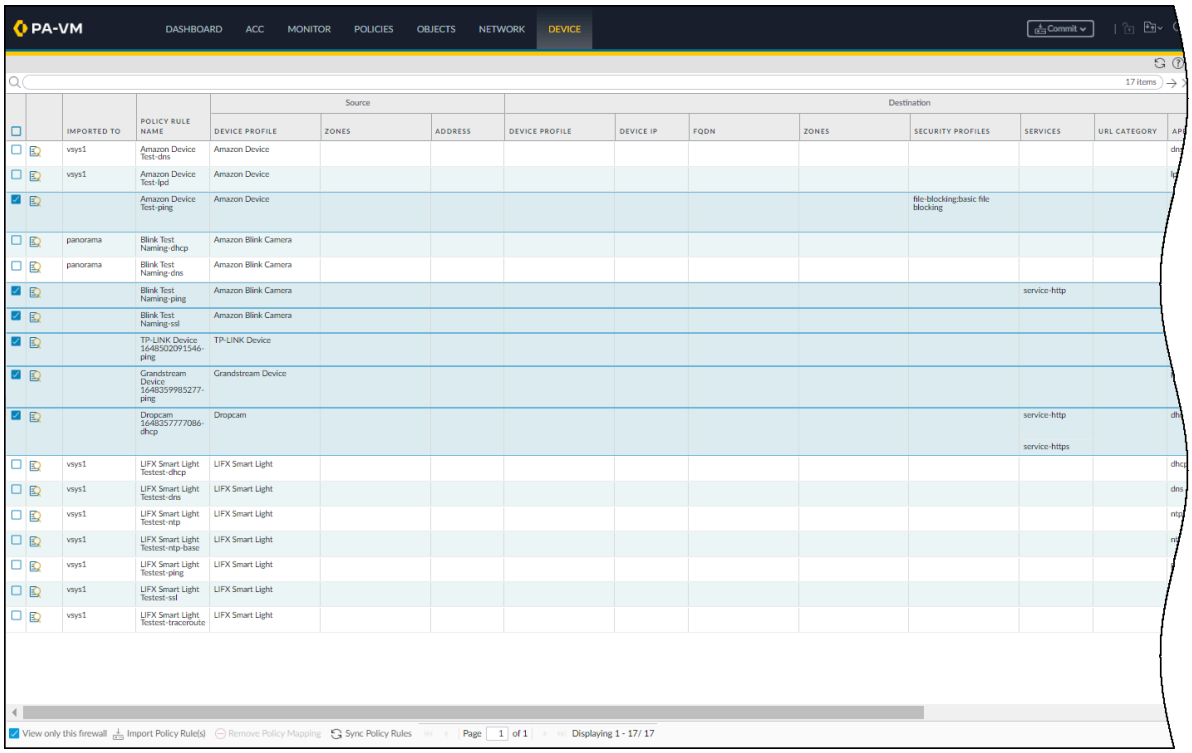
3. To remove the mapping between rules in the policy rulebase and their counterparts in the policy recommendation database, select **Panorama** > **Policy Recommendation** > **IoT**, select up to ten rules that have already been imported, and then **Remove Policy Mapping**.
4. Indicate a device group from which you want to remove the policy mapping and then confirm the removal. Repeat this if you want to remove the mapping from any other device groups.



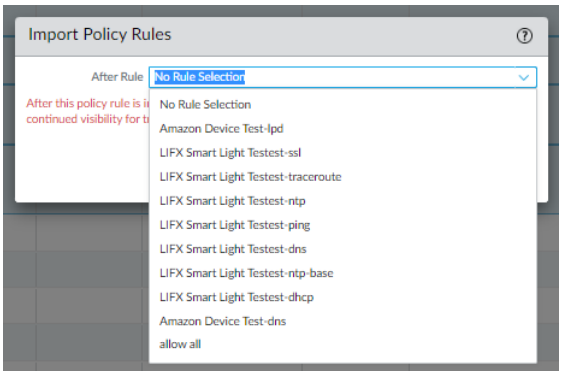
5. After confirming the policy mapping removal, you can then manually delete up to ten rules at a time from the rulebase in each device group on **Policies** > **Device Group** <name>.

- **Import Multiple Rules in Individual Firewalls**

  1. To import multiple rules at a time into the policy rulebase in the PAN-OS web interface on a single next-generation firewall, select **Device** > **Policy Recommendation** > **IoT**, select up to ten rules that have not already been imported, and then **Import Policy Rule(s)**.

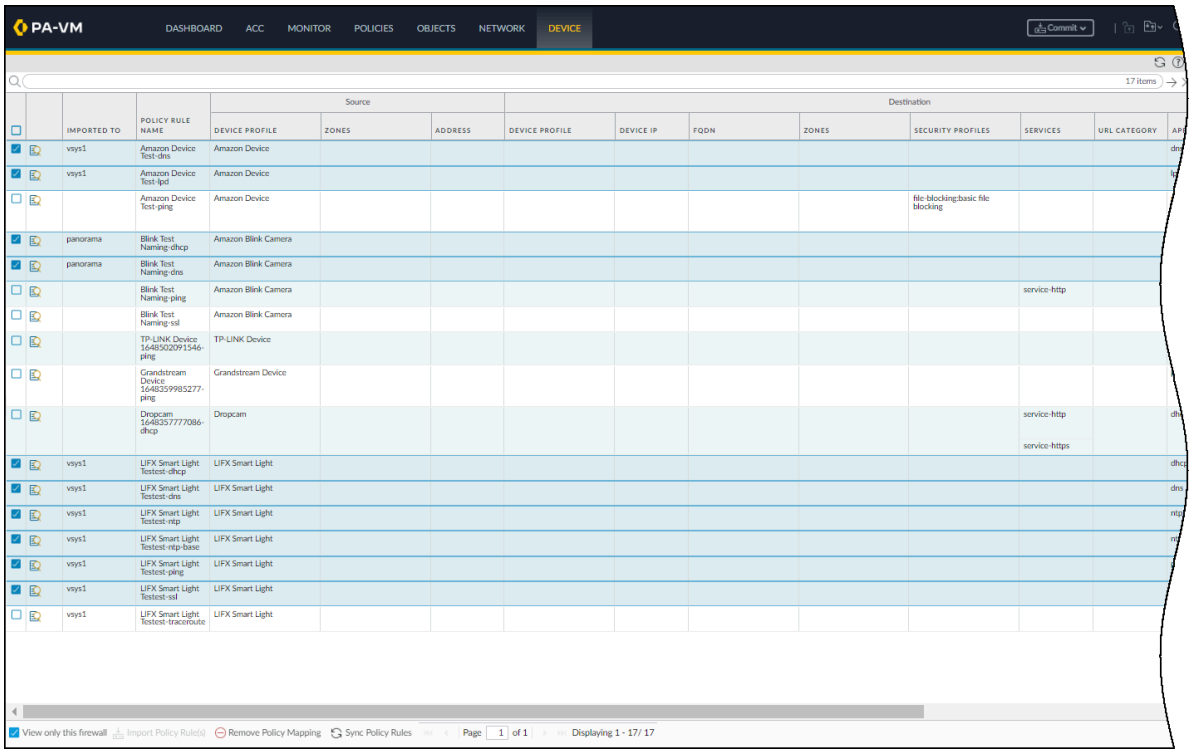


2. Choose the name of a rule in the rulebase after which you want PAN-OS to place the imported rules. If you choose **No Rule Selection**, the firewall imports the selected rules to the top.



- **Remove Mappings between Imported Rules and Recommendations**

  1. To remove the mapping between rules in the policy rulebase and their counterparts in the policy recommendation database, select **Device** > **Policy Recommendation** > **IoT**, select up to ten rules that have already been imported, and then **Remove Policy Mapping**.

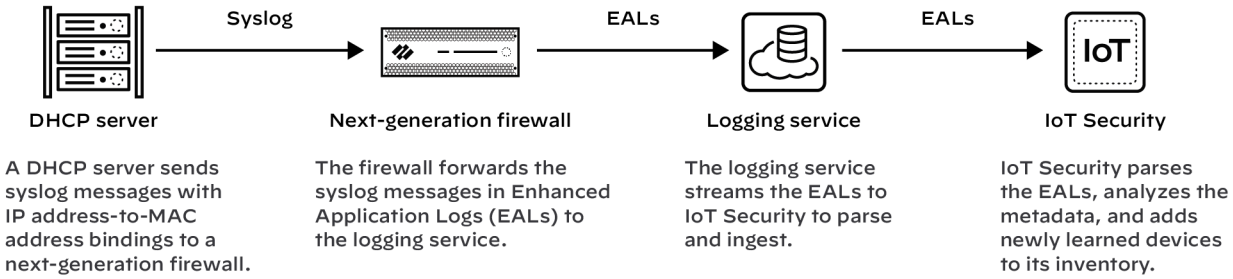


2. After confirming the policy mapping removal, you can then manually delete the rules from the rulebase.

Improved DHCP Traffic Visibility for IoT Security

IoT Security relies on IP address-to-MAC address bindings to ascribe observed network behaviors to IoT devices and uniquely track them. IoT Security typically uses DHCP traffic collected by next-generation firewalls to learn IP address-to-MAC address bindings and track IP address changes. However, when it's not possible to position a firewall in the DHCP data path, you can use this method to ingest DHCP server logs and expand DHCP traffic visibility.

In areas of the network where it's difficult to route DHCP traffic to or through a firewall, configure DHCP servers to send their server logs as syslog messages to the firewall. The firewall then forwards the messages as Enhanced Application Logs (EALs) with a subtype of dhcp-syslog through the logging service to IoT Security. IoT Security parses them to learn the IP address-to-MAC address bindings and then adds newly learned devices to its inventory.



- **Prerequisites**
  - A DHCP server with syslog capabilities configured to send messages to a syslog server running on a next-generation firewall
  - A next-generation firewall running PAN-OS® 11.0 or later with an active IoT Security subscription

Set up the Next-generation Firewall

Set up your next-generation firewall to receive syslog messages from one or more DHCP servers. The firewall will automatically forward the syslog messages it receives as EALs to the logging service, which streams them to IoT Security to parse and analyze.

1. Add a DHCP server to the next-generation firewall.

   Log in to your next-generation firewall, select **Device** > **IoT Security** > **+ Add**, configure the following, and then click **OK**:

   Name: Enter a name for the DHCP server. It can be up to 32 characters, including spaces.

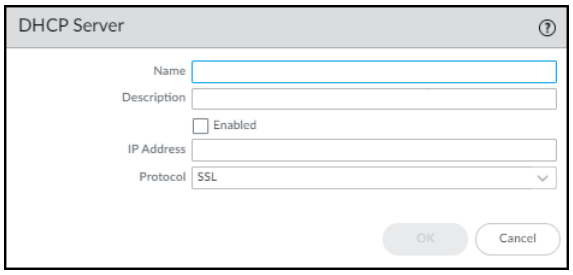
   Description: Enter a note about the DHCP server for future reference. It can be up to 256 characters, including spaces.

   Enabled: Select to enable the firewall to listen for connections from the DHCP server and process them when they come.

   IP Address: Enter the IP address from which the DHCP server will connect to the firewall. The address can be in IPv4 or IPv6 format. An FQDN is not allowed.

   Protocol: Select **TCP**, **UDP**, or **SSL**. When making your choice, consider what's important for the connection between the DHCP server and firewall. TCP provides transmission reliability but not security. UDP provides low processing overhead and faster speeds but lacks reliability and security. SSL provides reliability and security but incurs more overhead.

   The firewall listens for DHCP server connections using TCP and UDP on port 10514 and connections using SSL on port 16514.

2. Repeat the previous step to add more DHCP servers.

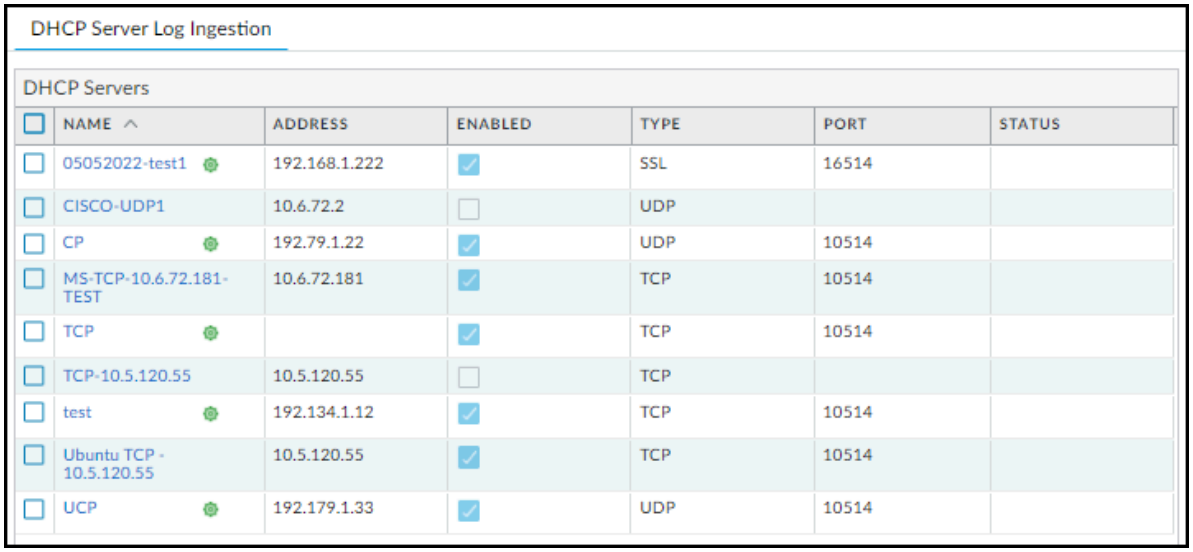
   Add more DHCP servers to expand visibility of DHCP traffic throughout your network as needed. All next-generation firewalls support a maximum of 100 DHCP servers per firewall.

Set up DHCP Servers for Syslog

Configure your DHCP servers to send syslog messages of their server logs to the management interface on the next-generation firewall. Make sure to configure the DHCP servers to use the same protocol configured for them on the firewall: TCP, UDP, or SSL. You can use DHCP servers such as Windows, Linux, Cisco, or Infoblox for example. See your product documentation for specific DHCP server configuration instructions.

Check DHCP Server Connection Status

1. To see all the configured DHCP servers, select **Device** > **IoT Security**.



   A green circle next to a DHCP server name means it was configured in Panorama and is read-only when viewed in the web interface of the local next-generation firewall.

   When a DHCP server using TCP or SSL is currently connected to the firewall, “Connected” appears in the Status column. “Connected” also appears in this column if a DHCP server using UDP has been connected within the past two hours. At all other times, the Status column is empty, indicating that the server isn’t currently connected to the firewall.

2. Use the following CLI commands to check DHCP server settings, the status of their connections, and the data they’re providing to IoT Security.

`show iot dhcp-server status { all | server <server-name> }`	Entering **`all`** shows a table with all DHCP servers configured and enabled on the firewall, the port numbers on which they connect, and their current connection status. Entering **`server <server-name>`** shows detailed information about a specific DHCP server and its recent activity.
`show iot eal dhcp-syslog-eal`	This command shows information related to EALs carrying DHCP server syslog messages.

Mobile Infrastructure Security Features

- User Equipment (UE) to IP Address Correlation with PFCP for 4G

User Equipment (UE) to IP Address Correlation with PFCP for 4G

As mobile service providers migrate from 4G/LTE to 5G, control and user plane separation (CUPS) architecture is a common deployment in 4G networks. With CUPS architecture, the User Plane Function (UPF) is closer to the enterprise (either on the edge service or in an on-premises location) while the control plane remains in a central location, such as a data center.

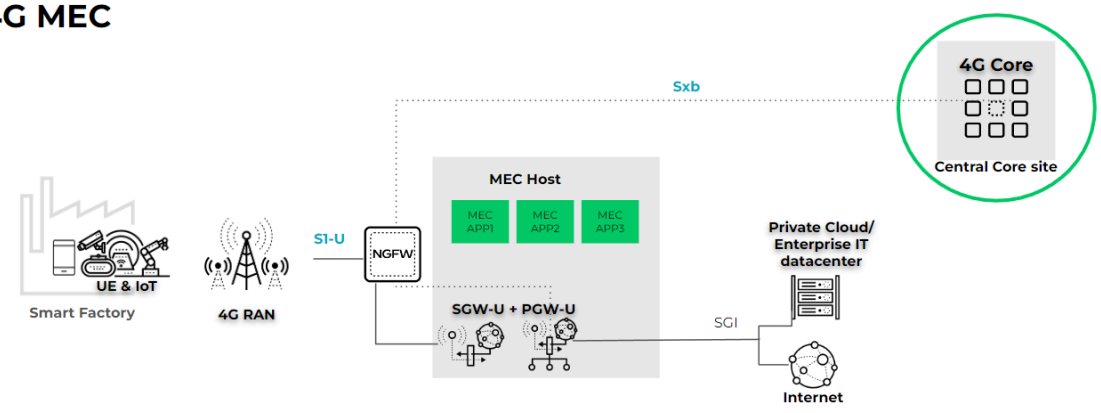
Subscriber ID (IMSI) and equipment ID (IMEI) correlation requires inspection of both control plane and user plane traffic by the same firewall. UEIP Correlation provides a way to ensure uninterrupted security policy enforcement during migration to a CUPS architecture through correlation of the subscriber ID and equipment ID to user equipment (UE) IP-based traffic and GTP-U content inspection.

For a solution for 5G networks, refer to 5G Multi-access Edge Computing Security.

The firewall monitors traffic for PFCP control messages at the Sxb interface and extracts the User Equipment IP Address (UE_IP) and Mobile User Identification (User_ID), which it uses to map the UE_IP to the IMEI, the IMSI, or both. It adds the mapping to a database which it distributes to other data planes and uses the mapping to perform GTP-U content inspection. You can query the database for the UE_IP to view the correlated Mobile User information for the UE IP traffic inside the GTP-U tunnels that comprise the CUPS architecture.

The following diagram represents a possible configuration for correlation for a 4G MEC topology using CUPS architecture:

Subscriber ID and Equipment ID policy in CUPS architecture - 4G MEC



S1-U represents a 3GPP interface that connects a 4G Radio Access Network (RAN) to the serving gateway user plane (SGW-U) and PDN gateway user plane (PGW-U) combo node using the GTP-U protocol. The control plane (Sxb) is a 3GPP interface that connects the PGW-U in the MEC location to the PGW-C in the 4G core at the central location (such as a public cloud or on-premises data center) using the PFCP protocol.

The SGI is also a 3GPP interface that connects the PGW-U to the external network (such as the internet or enterprise IT data center) using traditional IP-based interfaces.

In this topology, you can deploy the firewall as external to the MEC host in a hardware form factor or deploy the firewall on an MEC host in a virtual or container form factor.

To enforce security policy based on Subscriber ID or Equipment ID for a 4G MEC-based enterprise, position the firewall on the user plane (S1-U) and control plane (Sxb) interfaces at the MEC location.

The firewall inspects the control plane to extract information for correlation with the user plane, providing subscriber and equipment-level visibility, as well as policy control for vulnerabilities, malware, viruses, URLs, C2, and applications at the SP's MEC location.

To support correlation, the PFCP control message must contain the UE_IP and related User ID IE (Information Element).

The following platforms support UEIP Correlation:

- VM Series
- CN Series
- PA-3430 and PA-3440
- PA-5410, PA-5420, PA-5430, and PA-5440

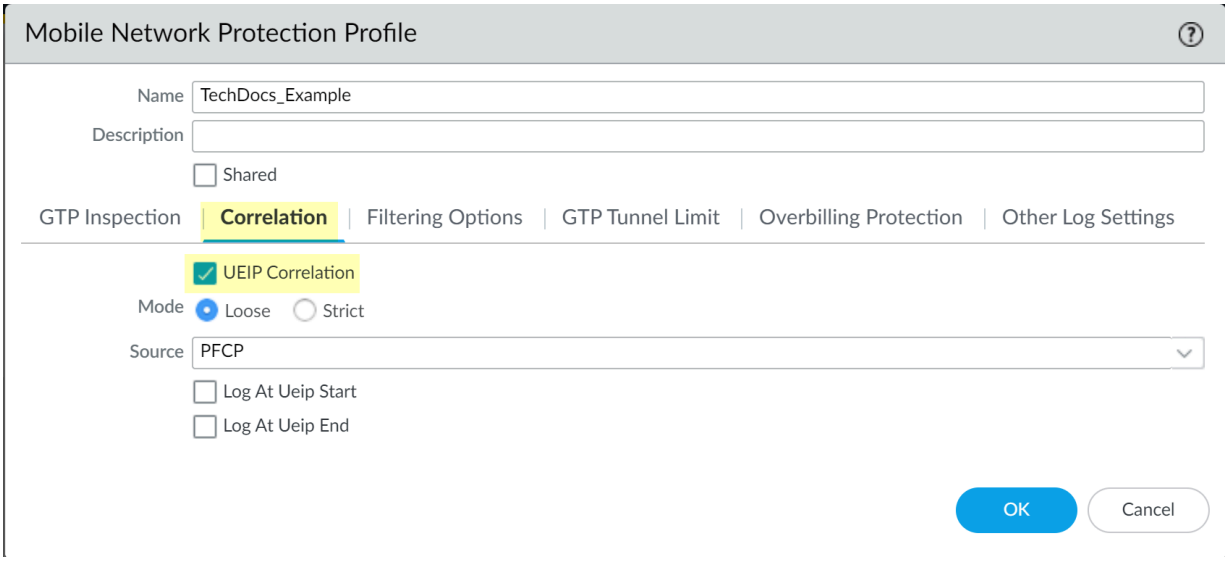
If you enable UEIP Correlation, the following options are not available in the same Mobile Network Protection Profile:

- *GTP-C*
- *5G-C*
- *PFCP*

STEP 1 | Select **Objects** > **Security Profiles** > **Mobility Network Protection**.

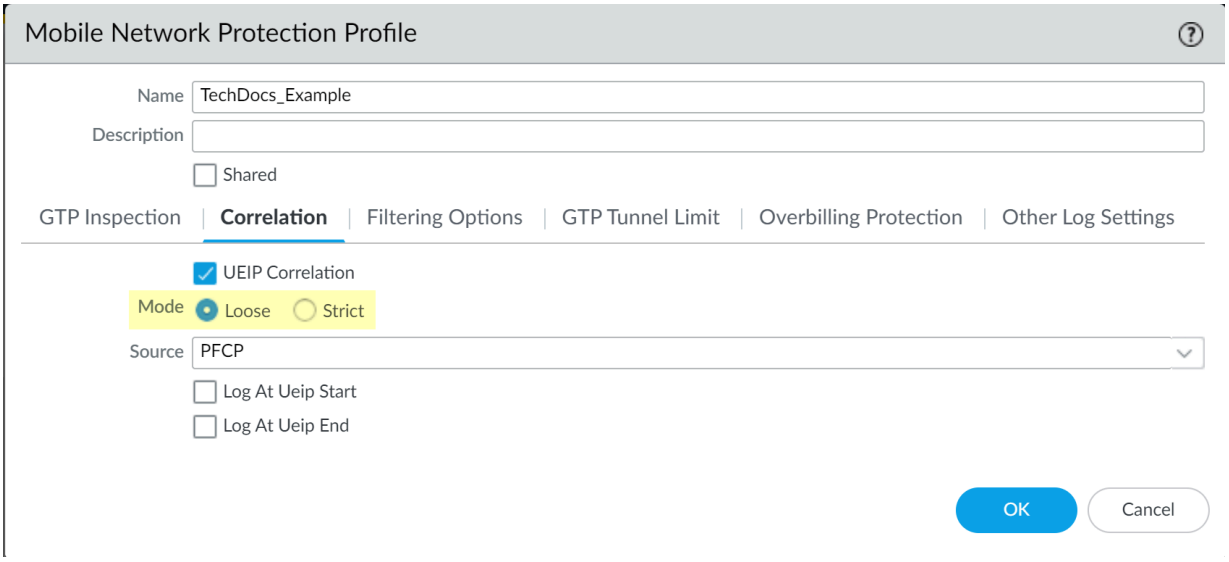
STEP 2 | **Add** or **Edit** a profile.

STEP 3 | Select **Correlation** and enable **UEIP Correlation**.



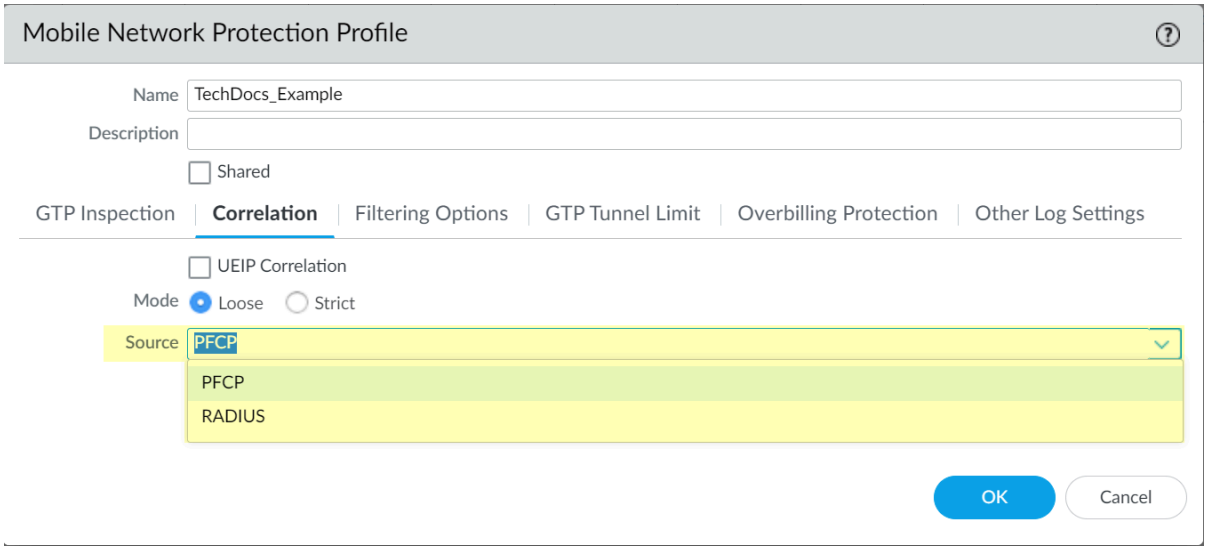
STEP 4 | Select the handling **Mode** to define the action if a query for the correlated information is not successful.

- **Loose**—(Default) When the firewall detects GTP-U inner traffic, it queries the source or destination address to find the correlated IMEI/IMSI information. If there are no results, the firewall forwards the traffic.
- **Strict**—Drops the GTP-U traffic if the query fails.

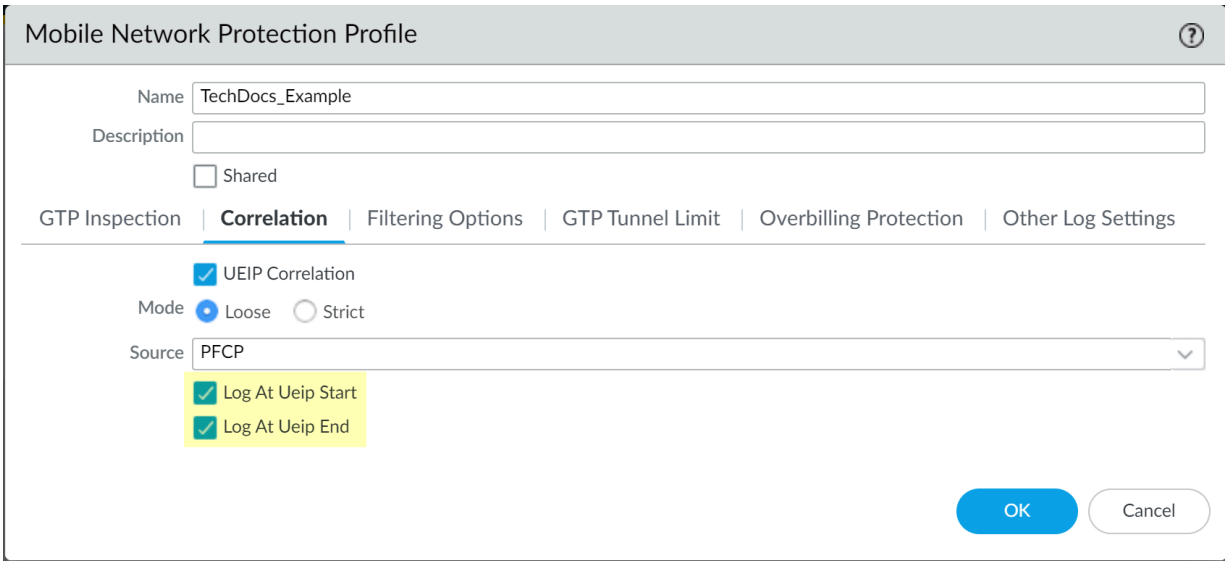


STEP 5 | Select **PFCP** as the **Source**.

For deployments using CUPS, select PFCP.



STEP 6 | (Optional) Select whether you want to log UEIP correlation events when the firewall allocates an IP address to the UE (**Log At Ueip Start**), when the firewall releases the allocated IP address (**Log At Ueip End**), or both.



STEP 7 | Click **OK** to save your changes.

STEP 8 | (Optional but recommended) Enable stateful inspection for GTP traffic.

STEP 9 | Confirm that the profile is **Enabled** (**Policies** > **Security** > **Security Policy Rule** > **Actions** > **Profile Setting** > **Mobile Network Protection**) and **Commit** the changes.

STEP 10 | Use App-IDs to configure the Mobile Network Protection Profile in a security policy to decapsulate the GTP-U tunnels and correlate the IP address with the Subscriber ID and Equipment ID.

1. Using App-ID, configure a security policy rule for the Sxb interface that allows PFCP traffic between the Sxb nodes (PGW-C and PGW-U) and select the **Mobile Network Protection** Profile you configured as the **Profile Setting** (traffic can originate from either endpoint).
2. Using App-ID, configure a security policy rule for the S1-U interface that allows GTP-U traffic between the S1-U nodes (eNodeB and SGW-U) and select the **Mobile Network Protection** Profile you configured as the **Profile Setting** (traffic can originate from either endpoint).

SD-WAN Features

- (PAN-OS 11.0.2 and later 11.0 releases) SD-WAN IPv6 Basic Connectivity
- SD-WAN Plugin Support for Advanced Routing Engine

SD-WAN IPv6 Basic Connectivity

Beginning with PAN-OS 11.0.2 and SD-WAN plugin 3.1.1, the legacy routing engine supports SD-WAN in a dual stack environment using IPv6 BGP loopback addresses for BGP peering. Thus, you can establish IPv6 connectivity by having the IPv6 traffic coming from the client to the branch then go over an IPv4 SD-WAN tunnel to reach the server via the hub.

This topic assumes you are familiar with how to configure SD-WAN and add an SD-WAN device. Configure basic IPv6 connectivity when your client connection to the SD-WAN branch and the server connection to the SD-WAN hub use IPv6, while your SD-WAN tunnel from the branch to the hub uses IPv4.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Select **Panorama** > **SD-WAN** > **Devices** and **Add** a new SD-WAN firewall.

STEP 3 | Perform the steps to add an SD-WAN device, including the steps to enable and configure IPv4 BGP.

STEP 4 | Perform the following steps to enable and configure IPv6 BGP.

1. Select the **IPv6 BGP** tab.
2. **Enable IPv6 BGP support**.
3. Specify a static **IPv6 Loopback Address** for BGP peering.
4. **Add** the IPv6 **Prefixes to Redistribute**. You must add at least one prefix when configuring a hub.
5. Click **OK**.

SD-WAN Plugin Support for Advanced Routing Engine

Advanced Routing Engine allows the firewall to scale and provide stable, high-performing, and highly available routing functions to large data centers, ISPs, enterprises, and cloud users. The Advanced Routing Engine relies on industry-standard configuration methodology, which facilitates the administrator tasks. It allows the creation of profiles that are used for different functions (such as, filtering, redistribution, and metric changes), all of which can be used across logical routers. These profiles provide finer granularity to filter routes for each dynamic routing protocol and improve route redistribution across multiple protocols.

You'll need the following to configure advanced routing engine on SD-WAN:

Platform	Firewalls running PAN-OS Release	SD-WAN Plugin
Panorama™	11.0 and later	3.1.0 and later

The Panorama SD-WAN plugin 3.1.0 can concurrently manage firewalls using the Advanced Routing Engine and firewalls using the legacy routing engine. The benefit is that you can migrate select managed firewalls to the new Advanced Routing Engine while still maintaining your current legacy routing engine configuration on others.

While the SD-WAN plugin 3.1.0 manages a firewall regardless of the routing engine, only one routing engine configuration can be in effect at a time on a managed firewall. You can use the **Advanced Routing** option to enable or disable the advanced routing engine. Each time you change the engine that the firewall uses (you enable or disable Advanced Routing to access the advanced engine or legacy engine, respectively), you must commit the configuration and reboot the firewall for the changes to take effect.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Upgrade Panorama to 11.0 and install the SD-WAN plugin 3.1.0.

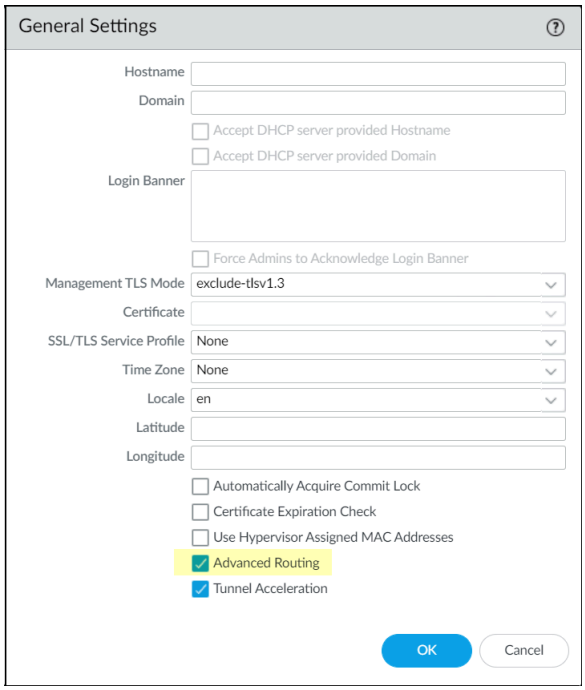
STEP 3 | Add your hub and branch firewalls as managed devices to the Panorama™ management server.

STEP 4 | Make a backup of your current configuration before you enable Advanced Routing.

STEP 5 | In the **Device** section, select appropriate template stack from the **Template** context drop-down.

STEP 6 | Enable advanced routing engine.

1. Select **Device** > **Setup** > **Management** and edit the General Settings.
2. Enable advanced routing.



3. **Commit**.
4. Select **Device** > **Setup** > **Operations** and **Reboot Device**.

STEP 7 | Select **Commit** > **Commit to Panorama** and **commit** your changes.

STEP 8 | Commit and push your configuration changes to your managed firewalls. **Push to Devices** to view the logical routers added in the selected SD-WAN firewalls.

1. Select **Commit** > **Push to Devices** and **Edit Selections**.
2. Select **Templates** and choose the templates stack and template from the list.
3. Enable **Force Template Values** to overwrite local configuration with the updated template values. Before you use this option, check for overridden values on the firewalls to ensure your commit does not result in any unexpected network outages or issues caused by replacing those overridden values.
4. Click **OK** and **Push** to devices.

STEP 9 | Log back into the firewall.

STEP 10 | Select **Network**.

Notice the menu items, which are more industry-standard and more detailed than the single item (Virtual Routers) on the legacy menu. **Routing** includes **Logical Routers** and **Routing Profiles**, which include **BGP**, **BFD**, **OSPF**, **OSPFv3**, **RIPv2**, **Filters**, and **Multicast**.

STEP 11 | You must enable **Advanced Routing** for each template stack individually when you have more than one template stack in your configuration. Repeat Steps 5 through 10 for other template stacks on firewalls that you intend to update for advanced routing.

According to our design requirement, the logical router name must be the same as the virtual router name for the same template when using the advanced routing engine. This means that hubs and branches have always the same router name. When manually creating logical routers rather than using a migration script, you must make sure the logical router name and virtual router name are the same.

STEP 12 | Select virtual or logical router in your SD-WAN deployment.

Select **Panorama** > **SD-WAN** > **Devices**, to add an SD-WAN device (SD-WAN hub or branch firewall) to be managed by the Panorama management server.

In addition to existing configuration options for adding an SD-WAN device, you can now select a logical router (for advanced routing engine) or virtual router (for legacy engine) for a **Router Name**. It is important that the logical router name and the virtual router name are same for the same template when using the advanced routing engine.

Select the **Router Name** (logical or virtual router) to use for routing between the SD-WAN hub and branches:

- If the virtual router and logical router names are the same, then the **Router Name** displays one name.
- If virtual router and logical router names are different, then the **Router Name** displays both virtual and logical router name. You can select either virtual router (for legacy engine) or logical router (for advanced routing engine) based on your requirement.

Virtualization Features

KMS Support for VM-Series

This release integrates cloud-native key managers, Azure Key Vault and AWS Secrets Manager, to store certificates for VM-Series firewalls. Decryption policy rules are configured using Panorama or the CLI.

For environments using auto scaling, VM-Series instances boot up in a state with the necessary certificates retrieved and ready to decrypt traffic without additional manual configuration.

Consider the following when integrating cloud-native key managers:

- Use a certificate in cloud-native key manager for outbound or inbound decryption.
- Specify the key manager stored certificate as part of the bootstrap.
- Specify the key manager-stored certificate as part of the decryption policy on PAN-OS (using VM-Series or through Panorama).
- Add new certificates, or edit an existing certificate of a decryption profile at any time.
- View and clear logs containing information about certificates in decryption profiles.
- You don't have to specify platform-specific information beyond certificate details. The VM-Series instance uses the appropriate APIs to communicate with the platform's native key manager.

Azure Key Vault integration is only applicable to Azure rulestack policy management and isn't supported for Panorama managed Cloud NGFW.

See Integrate Key Management Service for AWS and Integrate Key Management Service for Azure.

Software Cut-Through Based Offload on Software Firewalls

This release introduces software cut-through based offload support on VM-Series and CN-Series CNF Mode software firewalls. With the software cut-through based offload, CN-Series CNF Mode NGFWs eliminate the tradeoff between network performance, security, and cost. With software cut-through enabled, the first few packets complete the L7 packet inspection where the firewall determines if the session qualifies as an elephant flow. Consequently, the sessions then follow the software cut-through data path. It bypasses unnecessary operations, and leverages cache to complete the operation, thereby improving throughput handling and performance of the software firewall. By only inspecting flows that can benefit from security inspection, the overall load on the firewall is greatly reduced and performance increases without sacrificing the security posture.

For infrastructures that lack DPUs or are in public cloud, and have a traffic pattern that has offloadable elephant flows, the software cut-through based offload is able to function by taking advantage of the available NICs. See Hypervisor Support Matrix to learn about the supported NICs and Hypervisors.

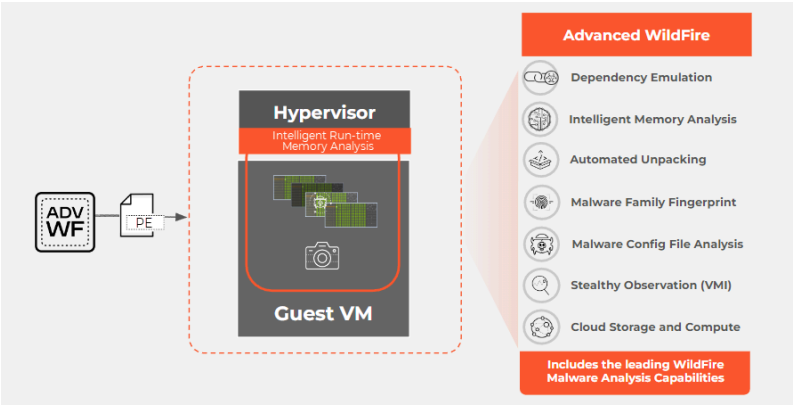
The software cut-through based offload also supports GTP-U traffic offloads. With GTPU Inner Session software-cut-through, for every GTP-U packet that CN-Series Kubernetes CNF mode will inspect, a full Layer7 inspection will be completed on the inner sessions. If the firewall determines that the inner sessions for this GTP-U packet qualifies to be offloaded - all subsequent GTP-U packets belonging to this session will get offloaded. This improves software firewall throughput handling capability, especially in 5G security use-cases that involve tunnel content inspection for consumer traffic within GTP-U.

In CN-Series firewall, only the CN-Series K8s CNF Mode supports software cut-through based offloads.

WildFire Features

Advanced WildFire Support for Intelligent Run-time Memory Analysis

Advanced WildFire is a new subscription offering available on NGFWs operating PAN-OS 10.0 and later that provides access to Intelligent Run-time Memory Analysis: a cloud-based advanced analysis engine that complements existing static, and dynamic analysis engines, to detect and prevent evasive malware threats. Advanced threats rely on techniques such as environmental checks and obfuscation to bypass detection; additionally, they often display signs of bespoke design with ephemeral behaviors that lead to fast-dissemination throughout the network, after an attack has been initiated. By leveraging a cloud-based detection infrastructure, Intelligent Run-time Memory Analysis detection engines operate a wide array of detection mechanisms to target these highly-evasive malware. To keep up with the latest threats, Advanced WildFire analysis engines are updated and deployed automatically, without requiring the user to download content update packages or run resource intensive, appliance-based analyzers.



Intelligent Run-time Memory Analysis relies on the existing WildFire analysis profile settings and does not require any additional configuration; it is only necessary to install the new Advanced WildFire license on your preferred NGFW platform. Samples that display or otherwise indicate evasive and/or advanced malware qualities are automatically forwarded to the appropriate analysis environments. Samples that receive a verdict with a high level of certainty using other analysis platforms may forego Advanced WildFire analysis. The resulting sample analysis details can be further examined by reviewing the WildFire analysis reports, which show a detailed account of what was discovered.

Intelligent Run-time Memory Analysis...

- *supports PE sample analysis.*
- *is not currently available in the WildFire EU and U.S. Government clouds.*

STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | To take advantage of Intelligent Run-time Memory Analysis, you must have an active Advanced WildFire subscription on your NGFW. For more information, refer to: Licensing, Registration, and Activation.

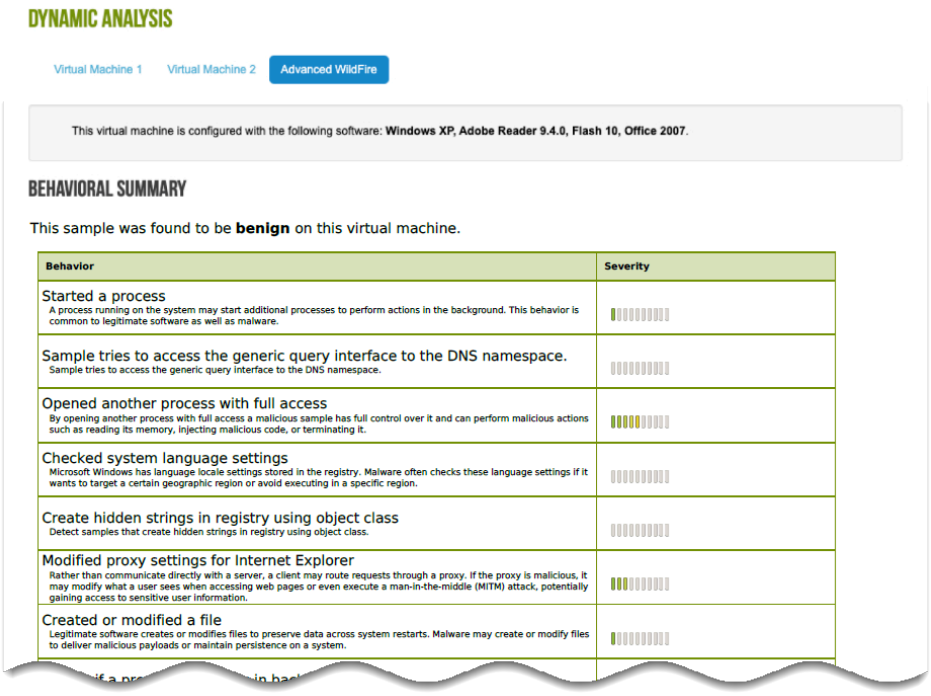
To verify subscriptions for which you have currently-active licenses, select **Device** > **Licenses** and verify that the appropriate licenses are available and have not expired.

If your current WildFire license has expired, you must first remove the license from the NGFW before installing the Advanced WildFire license.

STEP 3 | Verify that you have configured PAN-OS to Forward Files for WildFire Analysis.

STEP 4 | Download a malicious PE test file to verify that the file is forwarded for WildFire analysis, and view the analysis results.

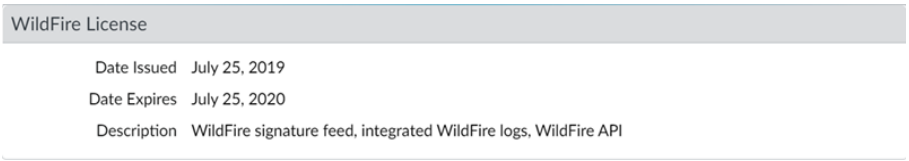
STEP 5 | View WildFire submissions logs for forwarded samples. Samples analyzed using Intelligent Run-time Memory Analysis analysis (Advanced WildFire) have an additional selectable VM category under the **Dynamic Analysis** heading labeled Advanced WildFire that displays the analysis details and supporting evidences for how a verdict conclusion was reached.



Hold Mode for WildFire Real-Time Signature Lookup

PAN-OS 11.0.2 now supports the option to hold file a sample transfer while the firewall queries the real-time signature cloud to perform a signature lookup. When the lookup is completed, the file is released to the requesting client, based on your organization's security policy for specific WildFire verdicts - this prevents the initial transfer of known malware; in other words, reduces the likelihood of a patient zero outbreak from occurring. You can configure the hold mode on a per antivirus profile basis and apply a global setting for the signature lookup timeout and the associated action. This feature is available to all users with an active WildFire or Advanced WildFire subscription.

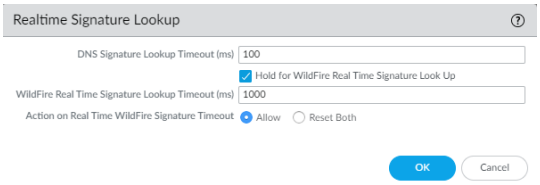
STEP 1 | To enable hold mode for WildFire real-time signature lookups, you must have either a WildFire or Advanced WildFire subscription service license. Make sure to activate the license on the firewall if you have not done so already. To verify subscriptions for which you have currently-active licenses, select **Device** > **Licenses** and verify that the appropriate licenses display and are not expired. The example below shows the description for the standard WildFire license.



STEP 2 | Log in to the PAN-OS web interface.

STEP 3 | Configure the timeout setting and action when the request exceeds the timeout.

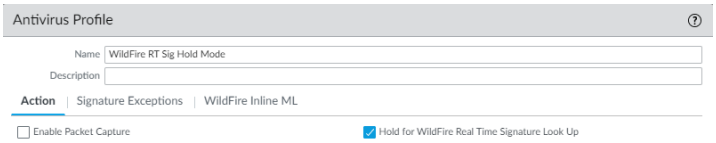
You must enable hold mode for WildFire real-time signature lookups globally before you enable hold mode on a per-Antivirus profile basis.



1. Select **Device Setup** > **ContentID** > **Realtime Signature Lookup**
2. Enable **Hold for WildFire Real Time Signature Look Up**.
3. Specify the **WildFire Real Time Signature Lookup Timeout (ms)** in milliseconds (the default value is 1000).

   Palo Alto Networks recommends using the default value of 1000ms unless you experience repeated timeouts during testing.
4. Specify the **Action on Real Time WildFire Signature Timeout**. The default value is **Allow**, however, Palo Alto Networks recommends setting this to **Reset-Both** when hold mode is enabled. The options include the following:
   - Allow—The NGFW allows packets through when the hold timeout threshold is reached.
   - Reset Both—The NGFW resets the connection on both the client and server ends when the hold timeout threshold is reached.
5. Select **OK** when finished.

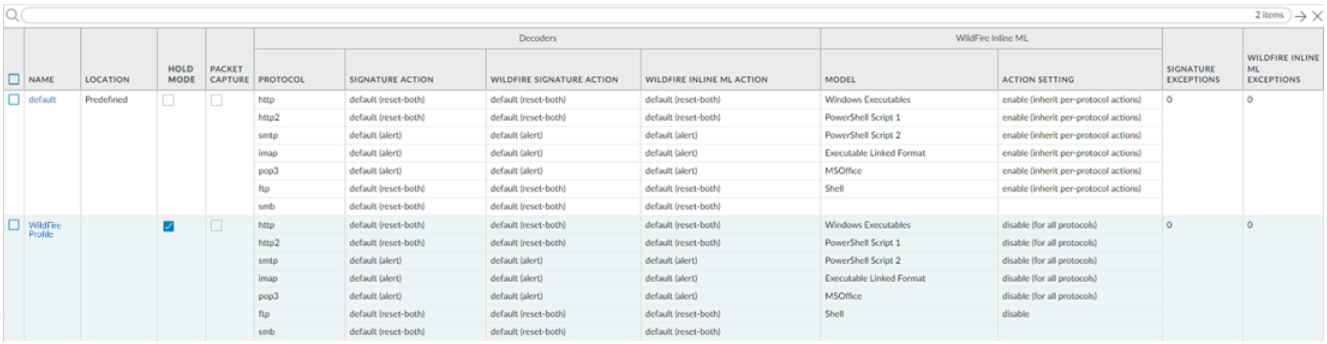
STEP 4 | Update or create a new Antivirus Security profile to enable hold mode for WildFire real-time signature lookups.



1. Select an existing antivirus security profile or **Add** a new one (**Objects** > **Security Profiles** > **Antivirus**).
2. Select your antivirus security profile and then go to **Action**.
3. Select **Hold for WildFire Real Time Signature Look Up**.
4. Repeat steps 4a-4c for all active antivirus profiles for which you want to enable hold mode for WildFire real-time signature lookups.

STEP 5 | **Commit** your changes.

STEP 6 | (Optional) You can view a summary of your antivirus security profile settings, including hold mode enablement, on the antivirus summary view page.



					Decoders				WildFire Inline ML			
NAME	LOCATION	HOLD MODE	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	MODEL	ACTION SETTING	SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
default	Predefined			http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	enable (inherit per-protocol actions)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	enable (inherit per-protocol actions)		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				
WildFire Profile		✓		http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	disable (for all protocols)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	disable (for all protocols)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	disable (for all protocols)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	disable (for all protocols)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	disable (for all protocols)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	disable		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				

Enterprise Data Loss Prevention Features

- File Type Include or Exclude List for Data filtering Profiles

File Type Include or Exclude List for Data filtering Profiles

Enterprise Data Loss Prevention (E-DLP) now supports creating a file type include or exclude list for data filtering profiles configured for file-based inspection. This allows you to select one of two modes:

- **Inclusion Mode**—Allow only specified file types be scanned by Enterprise DLP.
- **Exclusion Mode**—Allow all supported files to be scanned by Enterprise DLP by default but excluding the file types you specify.

  Exclusion Mode includes True File Type Support and does not rely on file extensions to determine file types.

To create a file type include or exclude list for Enterprise DLP data filtering profiles, the Panorama management server and managed firewalls using Enterprise DLP must be running PAN-OS 11.0.2 or later release. Additionally, the Enterprise DLP plugin must be version 4.0.1 or later.

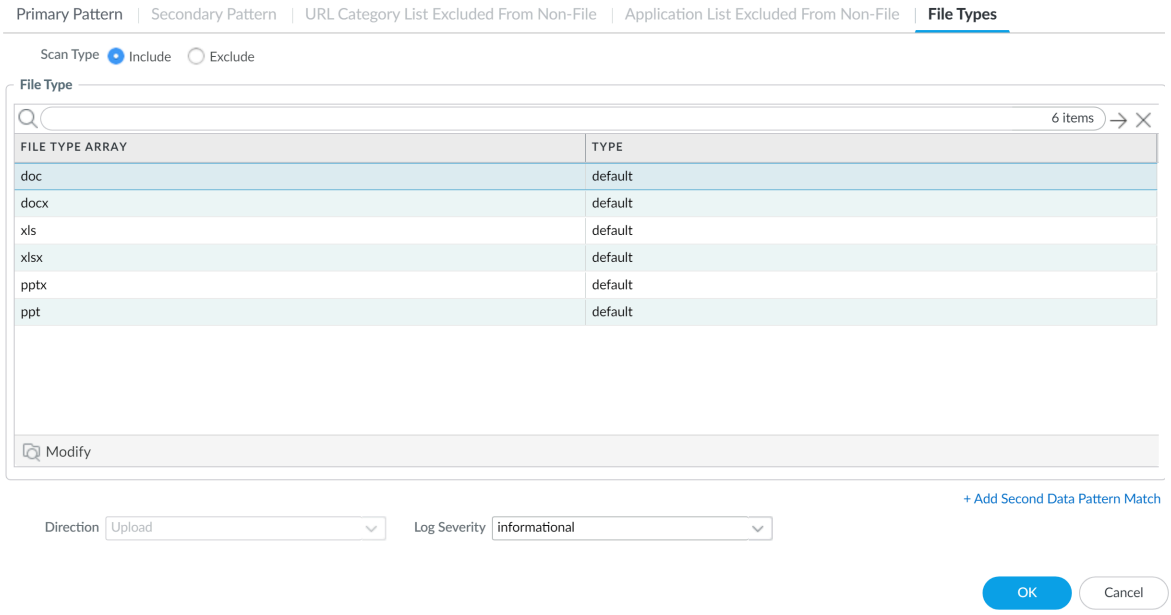
STEP 1 | Log in to the Panorama web interface.

STEP 2 | Select **Objects** > **DLP** > **Data Filtering Profiles** and specify the **Device Group**.

STEP 3 | Create a data filtering profile on Panorama for file-based inspection.

STEP 4 | When creating the data filtering profile, specify the file types the DLP cloud service takes action against.

1. Select **File Types**.
2. Select the Scan Type to create a file type include or exclude list.
   - **Include**—DLP cloud service inspects only the file types you add to the File Type Array.
   - **Exclude**—DLP cloud service inspects all supported file types except for those added to the File Type Array.
3. Click **Modify** to add the file types to the File Type Array and click **OK**.



STEP 5 | Click **OK** to save your changes.

STEP 6 | Attach the data filtering profile to a Security policy rule.

1. Select **Policies** > **Security** and specify the **Device Group**.
2. Select the Security policy rule to which you want to add the data filtering profile.
3. Select **Actions** and set the **Profile Type** to **Profiles**.
4. Select the **Data Filtering** profile you created previously.
5. Click **OK**.

STEP 7 | Commit and push your configuration changes to your managed firewalls that are using Enterprise DLP.

> *The **Commit and Push** command isn't recommended for Enterprise DLP configuration changes. Using the **Commit and Push** command requires the additional and unnecessary overheard of manually selecting the impacted templates and managed firewalls in the Push Scope Selection.*

1. Select **Commit** > **Commit to Panorama** and **Commit**.
2. Select **Commit** > **Push to Devices** and **Edit Selections**.
3. Select **Device Groups** and **Include Device and Network Templates**.
4. Click **OK**.
5. **Push** your configuration changes to your managed firewalls that are using Enterprise DLP.

