paloalto TECHDOCS

NGFW Getting Started

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2025-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

June 6, 2025

Table of Contents

Get Started with NGFWs

Where Can I Use This?	What Do I Need?
• NGFW	

Palo Alto Networks Next-Generation Firewalls (NGFWs) implement a security architecture that extends beyond traditional firewall capabilities. Traditional firewalls primarily filter traffic based on port, protocol, and IP addresses, while Palo Alto Networks 's NGFWs use App-ID technology to identify and control applications regardless of port, protocol, or encryption status. This application-based approach enables for more precise security controls than port-based methods, enabling administrators to create policy rules based on applications and user identities rather than just network attributes.

The core functions include: **App-ID technology**, which identifies and controls applications regardless of port, protocol, or encryption, moving beyond traditional firewall limitations. This application awareness is seamlessly integrated into **unified security policies** that combine all protection mechanisms into a single, streamlined rule base for simplified management. To address the growing challenge of encrypted traffic, **SSL/TLS decryption capabilities** provide visibility into threats hiding within encrypted communications. **Advanced threat intelligence and sandboxing** through WildFire continuously protect against unknown malware and zero-day attacks in real-time, while **URL filtering** blocks access to malicious websites and enforces acceptable use policies. Finally, **integrated VPN connectivity** ensures secure remote access for today's distributed workforce. Together, these core features create a unified security platform that provides unprecedented visibility, control, and protection across all network traffic.

Administrators have several options for managing Palo Alto Networks NGFWs, depending on your network's deployment scale and technical requirements:

□ PAN-OS

□ Panorama

□ Strata Cloud Manager

For more information about the management styles available for your NGFWs, click here.

Determine Your NGFW Management Strategy

Where Can I Use This?	What Do I Need?
• NGFW	Prerequisites are determined by your management strategy of choice.

Palo Alto Networks provides three distinct management approaches for NGFWs, each designed to address different operational requirements and network architectures.

Direct device management through the **PAN-OS** web interface offers administrators granular control over an individual firewall's configurations, suitable for small deployments or environments with limited devices.

Panorama provides centralized management capabilities as either a hardware appliance or virtual machine, enabling security teams to implement consistent policy rules, collect unified logs, and generate comprehensive reports across the entire NGFW infrastructure.

Strata Cloud Manager is a cloud-native management solution that eliminates the need for on-premises management infrastructure, offering similar centralized control while providing built-in scalability and simplified deployment for distributed networks. Each management option maintains consistent security capabilities while offering different operational models to align with an organization's existing infrastructure, technical resources, and security management preferences.

While thinking about how you want to manage your NGFWs, you can begin the process of integrating NGFWs into your network.

- PAN-OS
- Panorama
- Strata Cloud Manager

Determine Your Management Strategy (PAN-OS)

The PAN-OS web interface provides direct device management for individual NGFW, offering administrators complete control through a browser-based console. This management approach delivers immediate access to all NGFW functions without requiring additional infrastructure. The interface is organized into logical sections including Dashboard, ACC (Application Command Center), Policies, Objects, Network, Device, and Monitor, providing intuitive navigation for both configuration and operational monitoring.

Key advantages include zero deployment overhead, immediate configuration changes without synchronization delays, and direct access to hardware-specific settings. The PAN-OS web interface is particularly suitable for small deployments, lab environments, or scenarios where granular device-specific control is required. This management method enables administrators to leverage the full functionality of the firewall without dependencies on external management systems.

Determine Your Management Strategy (Panorama)

Panorama serves as an on-premises centralized management solution for organizations with multiple NGFWs, available as either a dedicated hardware appliance or virtual machine. Its hierarchical management model enables administrators to define shared policy rules that apply across the entire NGFW estate while still enabling for device-specific configurations when needed. Standout features include template stacks for standardizing network configurations, device groups for organizing security policy rules, and consolidated logging that aggregates security data across all Panorama managed devices.

Panorama excels in providing consistent rule enforcement, simplified compliance management, and reduced administrative overhead in multidevice environments. The solution supports role-based access control for distributed security teams and offers comprehensive change management capabilities including commit previews and audit trails. Panorama is valuable for organizations with regulatory requirements necessitating centralized logging or those maintaining significant on-premises infrastructure.

Determine Your Management Strategy (Strata Cloud Manager)

Strata Cloud Manager represents a Palo Alto Networks cloud-native management platform, offering centralized control of security infrastructure without requiring on-premises management servers. This SaaS-based solution provides similar policy rule management capabilities to Panorama but adds cloud-specific advantages including automatic scaling, continuous updates without maintenance windows, and global accessibility. Standout features include simplified deployment through Zero Touch Provisioning, integrated cloud-delivered security services, and unified management of both physical and cloud-based security controls.

Strata Cloud Manager excels in managing distributed environments and supports hybrid deployments spanning traditional data centers, branch offices, and multicloud environments. The platform offers consumption-based licensing models that align costs with actual usage and provides built-in high availability without additional infrastructure. This management option is advantageous for organizations embracing cloud-first strategies, supporting remote workforces, or seeking to reduce the operational complexity associated with maintaining management infrastructure.

Integrate NGFWs into Your Network

Where Can I Use This?	What Do I Need?
• NGFW	

All Palo Alto Networks NGFWs provide an out-of-band management port (MGT) that you can use to perform the administrative functions. By using the MGT port, you separate the management functions of the NGFW from the data processing functions, safeguarding access to the NGFW, and enhancing performance. When using the web interface, you must perform all initial configuration tasks from the MGT port even if you plan to use an in-band data port for managing your NGFW going forward. This requirement applies whether you're setting up the firewall for standalone operation or onboarding to Panorama or Strata Cloud Manager.

Some management tasks, such as retrieving licenses and updating the threat and application signatures on the firewall require access to the internet. If you don't want to enable external access to your MGT port, you will need to either set up an in-band data port to provide access to required external services (using service routes) or plan to manually upload updates regularly.

⚠ *Don't enable access to your management interface from the internet or from other untrusted zones inside your enterprise security boundary. This applies whether you use the dedicated management port (MGT) or you configured a data port as your management interface. When integrating your firewall into your management network, follow the Administrative best practices to ensure that you're securing administrative access to your NGFWs and other security devices in a way that prevents successful attacks.*

After integrating the NGFWs into your network, learn how to perform the initial configuration steps that are necessary to integrate a new NGFW into the management network and deploy it in a basic security configuration.

The following topics describe how to integrate a single Palo Alto Networks NGFW into your network. However, for redundancy, consider deploying a pair of NGFWs in a high availability configuration.

Considerations for Business Continuity

Your business continuity plan should include provisions for how to connect to critical devices, including NGFWs and Panorama, during power outages and other events that prevent connecting to those devices over normal communication channels. The ability to connect to and manage devices on an out-of-band (OOB) network enables you to continue running your business when primary networks and power sources are down. Business continuity should be a core consideration of your network architecture.

An OOB network is a secure method of remotely accessing and managing devices and does not use the primary communication channels. Instead, OOB networks use separate communication channels that are always available if the primary channel fails and has a different source of power than the primary network. Depending on your network architecture, you may use both the primary network and the OOB network to access and manage devices in day-to-day operation.

The OOB network should never rely on a power source or network that could fail concurrently with the primary access network. How you architect OOB access to devices depends on your network architecture and your business considerations, so there is no “one size fits all” method of ensuring connectivity. However, there are guidelines that help you understand how to meet the goals of an OOB access network:

- **Power considerations**—Use a different power source (a separate circuit or a protected or battery-powered source) for the OOB network than you use for the regular access network. If you lose power to the regular network, you won’t lose power to the OOB network.

  Use power distribution unit (PDU) controls to remotely power devices on and off.

- **Secure connection method**—There are a number of ways to connect securely to an OOB network, for example, a terminal server device, a modem, or a serial console server. Examples of secure networks you can use for OOB access include LTE, dial-up, and broadband (separated from the normal broadband network) networks. The connection method you use depends on your business needs and network architecture.

  Regardless of the method you select, the connection must be secure, with strong encryption and authentication.

  You can connect into an OOB network remotely using SSH with strong authentication over an Ethernet LAN or you can dial in over a serial connection. The outbound connection will be serial.

To get started with the initial set up and configuration of your NGFWs, click here.

Perform the Initial Setup and Configuration for NGFWs

Where Can I Use This?	What Do I Need?
• NGFWs	□ No prerequisites needed for initial setup

Perform the initial configuration for your NGFW. You can perform these initial configuration tasks either from the MGT interface, even if you do not plan to use this interface for your NGFW management, or using a direct serial connection to the console port on the device.

The initial configurations need to be completed before you can begin onboarding your NGFW to your management system of choice.

The initial configurations for your NGFWs can be performed before you have decided on the management style of choice and will need to be done before you can proceed with onboarding.

For more information about what needs to be done before you can onboard to Strata Cloud Manager or Panorama, see the cheat sheet here.

By default, the PA-Series NGFW has:

□ An IP address of 192.168.1.1

□ A username/password of admin/admin

For security reasons, you must change these settings before continuing with other NGFW configuration tasks.

- Standard
- Air Gapped

Perform the Initial Setup and Configuration for NGFWs (Non-Air Gapped)

STEP 1 | Install your NGFW and connect power to it.

> *If your NGFW model has dual power supplies, connect the second power supply for redundancy. Refer to the* hardware reference guide *for your model for details.*

STEP 2 | Gather the required information from your network administrator.

- IP address and netmask (if the MGT port will have a static address)
- Default gateway (if the MGT port will have a static default gateway address)
- DNS server address

STEP 3 | Connect your computer to the NGFW.

You can connect to the device in one of the following ways:

- Connect a serial cable from your computer to the Console port and connect to the firewall using terminal emulation software (9600-8-N-1). Wait a few minutes for the boot-up sequence to complete; when the NGFW is ready, the prompt changes to the name of the firewall, for example `PA-220 login`.
- Connect an RJ-45 Ethernet cable from your computer to the MGT port on the NGFW. From a browser, go to **`https://192.168.1.1`**.

> *You may need to change the IP address on your computer to an address in the 192.168.1.0/24 network, such as 192.168.1.2, to access this URL.*

STEP 4 | When prompted, log in to the NGFW.

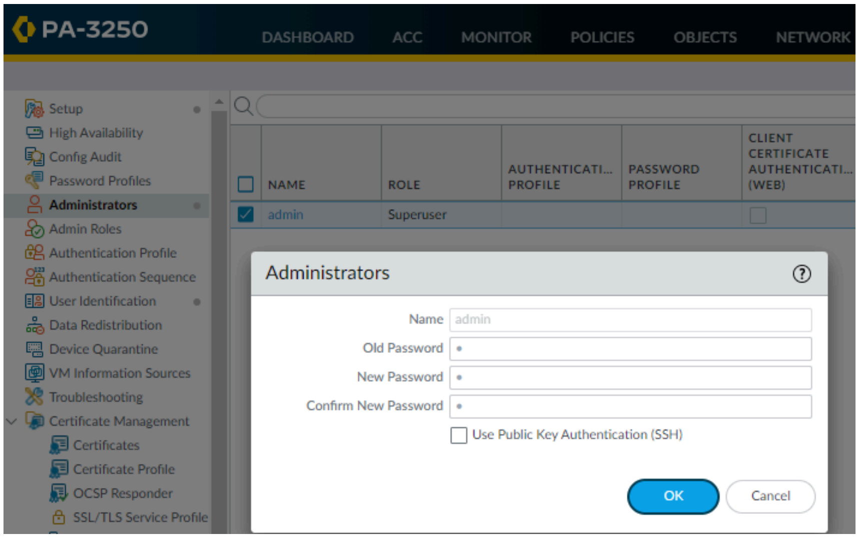
You must log in using the default username and password (admin/admin). The NGFW will begin to initialize.

STEP 5 | Set a secure username and password for the admin account.

The predefined, default administrator password (admin) must be changed on the first login on a device. The new password must be a minimum of eight characters and include a minimum of one lowercase and one uppercase character, as well as one number or special character. Although you don't have to configure a new username, it is a best practice to do so and to use unique usernames and passwords for each administrator. The login must include at least one alphabetical character or symbol (underscore, period, or hyphen, although a hyphen cannot be the first character in the username) and cannot be numbers only.

Be sure to use the best practices for password strength *to ensure a strict password and review the* minimum password complexity.

1. Select **Device** > **Administrators**.
2. Select the **admin** role.
3. Enter the current default password and the new password.



	NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)
☑	admin	Superuser			□

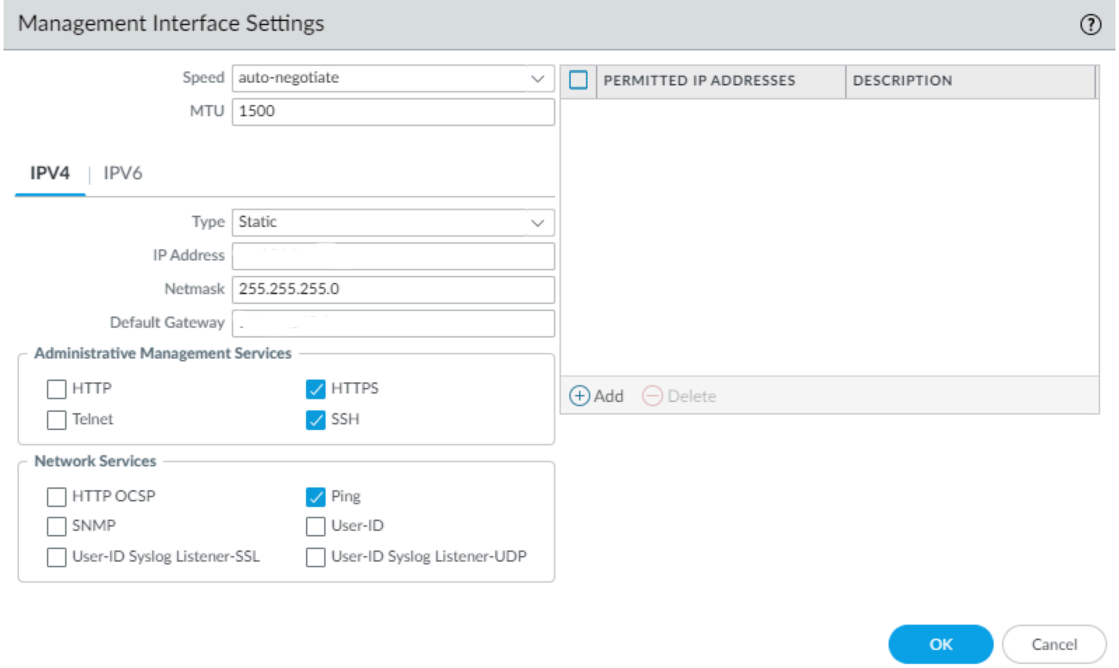
Administrators

Name: admin
Old Password: •
New Password: •
Confirm New Password: •
□ Use Public Key Authentication (SSH)

4. Click **OK** to save your settings.

STEP 6 | Configure the MGT interface.

1. Select **Device** > **Setup** > **Interfaces** and edit the **Management** interface.
2. Set the **Speed** to **auto-negotiate**.
3. Specify the **MTU** in bytes for packets sent on this interface.
4. Select **IPv4** or **IPv6**.
5. To configure IPv4 address settings for the MGT interface, select an address **Type**:
   - **Static**— Enter the **IP Address**, **Netmask**, and **Default Gateway**.
   - **DHCP Client**—To configure dynamic address settings, you must Configure the Management Interface as a DHCP Client.



Management Interface Settings

Speed: auto-negotiate

MTU: 1500

IPV4 | IPV6

Type: Static

IP Address:

Netmask: 255.255.255.0

Default Gateway: .

Administrative Management Services

☐ HTTP ☑ HTTPS

☐ Telnet ☑ SSH

Network Services

☐ HTTP OCSP ☑ Ping

☐ SNMP ☐ User-ID

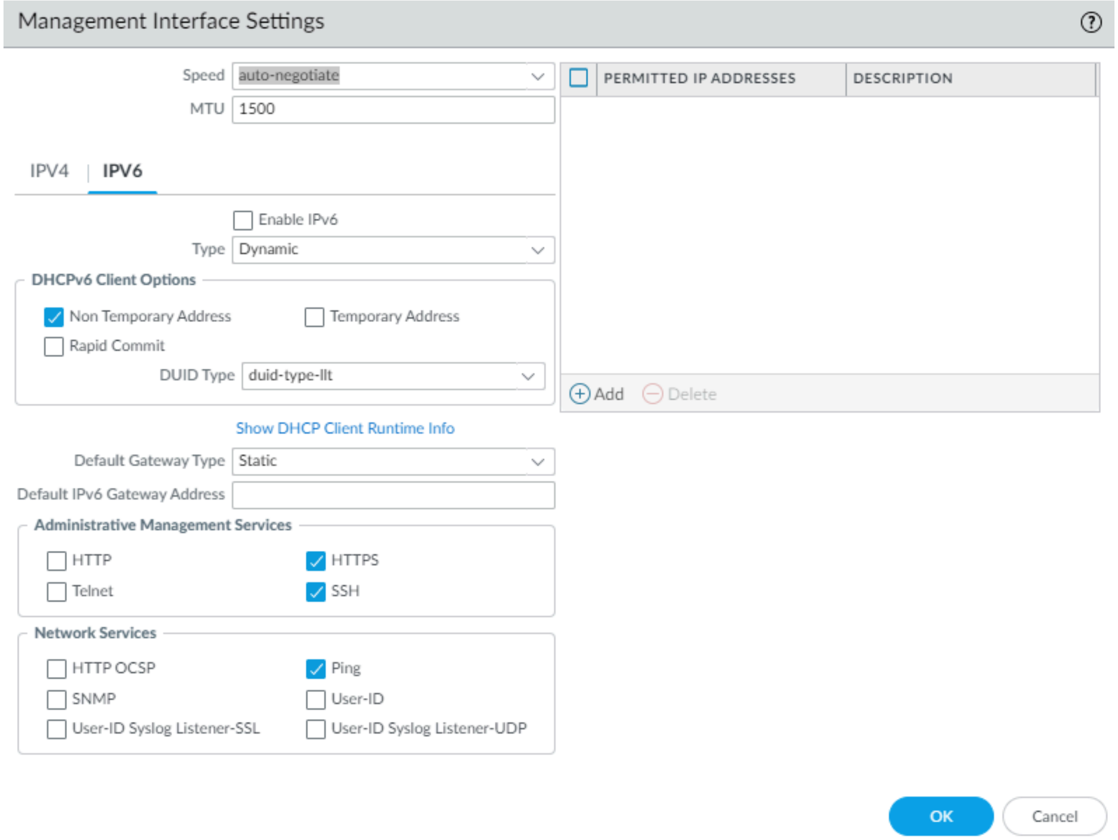
☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

☐	PERMITTED IP ADDRESSES	DESCRIPTION

6. To configure IPv6 address settings for the MGT interface, **Enable IPv6** and select an address **Type**:
   - **Static**— Enter the **IPv6 Address/Prefix Length**. Additionally, select a **Default Gateway Type**: **Static** (enter the **Default IPv6 Gateway Address**) or **Dynamic** (the NGFW learns

the default gateway address from the Router Advertisement message that the router sent).

- **DHCP Client**—To configure dynamic IPv6 address settings, you must Configure the Management Interface for Dynamic IPv6 Address Assignment.



Management Interface Settings

Speed: auto-negotiate
MTU: 1500

IPV4 | IPV6

□ Enable IPv6
Type: Dynamic

DHCPv6 Client Options
☑ Non Temporary Address □ Temporary Address
□ Rapid Commit
DUID Type: duid-type-llt

Show DHCP Client Runtime Info

Default Gateway Type: Static
Default IPv6 Gateway Address:

Administrative Management Services
□ HTTP ☑ HTTPS
□ Telnet ☑ SSH

Network Services
□ HTTP OCSP ☑ Ping
□ SNMP □ User-ID
□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION

7. To prevent unauthorized access to the management interface, it is a an administrative best practice to **Add** the **Permitted IP Addresses** from which an administrator can access the MGT interface.
8. Select which management services to allow on the interface.

   *Make sure **Telnet** and **HTTP** aren't selected because these services use plaintext and aren't as secure as the other services; they could compromise administrator credentials.*

9. Click **OK**.

STEP 7 | Specify the update server, and configure DNS settings and proxy server settings.

You must manually configure at least one DNS server on the NGFW or it won't be able to resolve hostnames; it won't use DNS server settings from another source, such as an ISP.

1. Select **Device** > **Setup** > **Services**.
    - For multi-virtual system platforms, select **Global** and edit the Services section.
    - For single virtual system platforms, edit the Services section.
2. On the **Services** tab, **Update Server** represents the IP address or host name of the server from which to download updates from Palo Alto Networks. The current value is

updates.paloaltonetworks.com. Don't change this setting unless instructed by technical support.

3. Select **Verify Update Server Identity**.

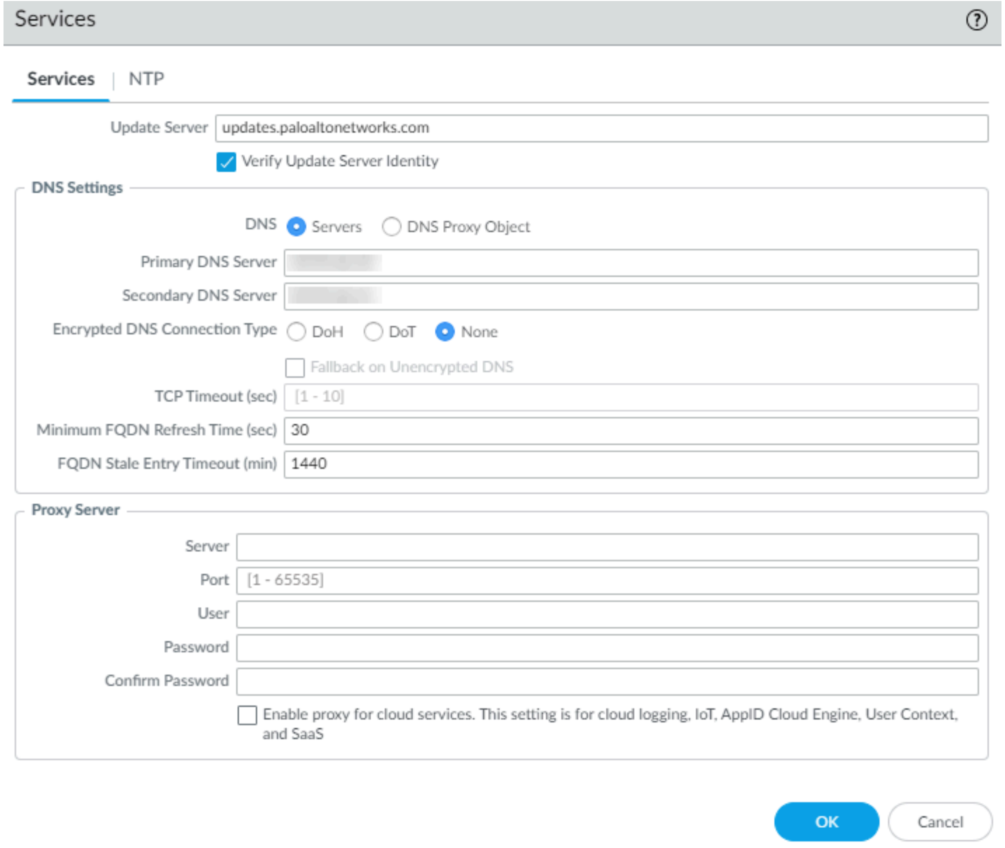
   It's a best practice to enable this option, which causes the firewall or Panorama to verify that the server from which the software or content package is downloaded has an SSL certificate signed by a trusted authority.

4. For **DNS**, select the way for the MGT interface to get DNS services:

   - **Servers**—Enter the **Primary DNS Server** address and **Secondary DNS Server** address.
   - **DNS Proxy Object**—From the drop-down, select the **DNS Proxy** that you want to use to configure global DNS services, or click **DNS Proxy** to configure a new DNS proxy object.

     Beginning with PAN-OS 11.2.1 and later releases, you can enable encrypted DNS on the MGT interface (whether the interface uses a DNS server or DNS proxy) by configuring DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT).

     - *To configure encrypted DNS when the MGT interface uses DNS servers, refer to the* Networking Administrator's Guide, Use Case 1: Firewall Requires DNS Resolution..
     - *To configure encrypted DNS when the MGT interface uses DNS proxy, refer to the* Networking Administrator's Guide, Configure a DNS Proxy Object.



Update Server: updates.paloaltonetworks.com

☑ Verify Update Server Identity

DNS Settings

DNS ● Servers ○ DNS Proxy Object

Primary DNS Server: [redacted]

Secondary DNS Server: [redacted]

Encrypted DNS Connection Type ○ DoH ○ DoT ● None

☐ Fallback on Unencrypted DNS

TCP Timeout (sec): [1 - 10]

Minimum FQDN Refresh Time (sec): 30

FQDN Stale Entry Timeout (min): 1440

Proxy Server

Server:

Port: [1 - 65535]

User:

Password:

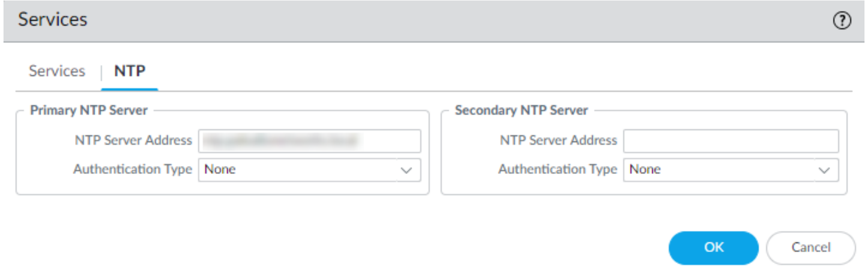
Confirm Password:

☐ Enable proxy for cloud services. This setting is for cloud logging, IoT, AppID Cloud Engine, User Context, and SaaS

5. Click **OK**.

STEP 8 | Configure date and time (NTP) settings.

1. Select **Device** > **Setup** > **Services**.
   - For multi-virtual system platforms, select **Global** and edit the Services section.
   - For single virtual system platforms, edit the Services section.
2. On the **NTP** tab, to use the virtual cluster of time servers on the Internet, enter the hostname `pool.ntp.org` as the **Primary NTP Server** or enter the IP address of your primary NTP server.



Services

Services | NTP

Primary NTP Server
NTP Server Address [redacted]
Authentication Type None

Secondary NTP Server
NTP Server Address
Authentication Type None

3. (Optional) Enter a **Secondary NTP Server** address.
4. (Optional) To authenticate time updates from the NTP server(s), for **Authentication Type**, select one of the following for each server:
   - **None**—(Default) Disables NTP authentication.
   - **Symmetric Key**—Firewall uses symmetric key exchange (shared secrets) to authenticate time updates.
     - **Key ID**—Enter the Key ID (1-65534).
     - **Algorithm**—Select the algorithm to use in NTP authentication (**MD5** or **SHA1**).
   - **Autokey**—NGFW uses autokey (public key cryptography) to authenticate time updates.
5. Click **OK**.

STEP 9 | (Optional) Configure general NGFW settings as needed.

1. Select **Device** > **Setup** > **Management** and edit the General Settings.
2. Enter a **Hostname** for the NGFW and enter your network **Domain** name. The domain name is just a label; it will not be used to join the domain.
3. Enter **Login Banner** text that informs users who are about to log in that they require authorization to access the NGFW management functions.

   As a best practice, avoid using welcoming verbiage. Additionally, you should ask your legal department to review the banner message to ensure it adequately warns that unauthorized access is prohibited.
4. Enter the **Latitude** and **Longitude** to enable accurate placement of the NGFW on the world map.
5. Click **OK**.

STEP 10 | Commit your changes.

When the configuration changes are saved, you lose connectivity to the web interface because the IP address has changed.

Click **Commit** at the top right of the web interface. The NGFW can take up to 90 seconds to save your changes.

STEP 11 | Connect the NGFW to your network.

1. Disconnect the NGFW from your computer.
2. (All NGFWs except for the PA-5450) Connect the MGT port to a switch port on your management network using an RJ-45 Ethernet cable. Make sure that the switch port you cable the device to is configured for auto-negotiation.
3. (PA-5450 only) Connect the MGT port to a switch port on your management network using a Palo Alto Networks certified SFP/SFP+ transceiver and cable.

STEP 12 | Open an SSH management session to the NGFW.

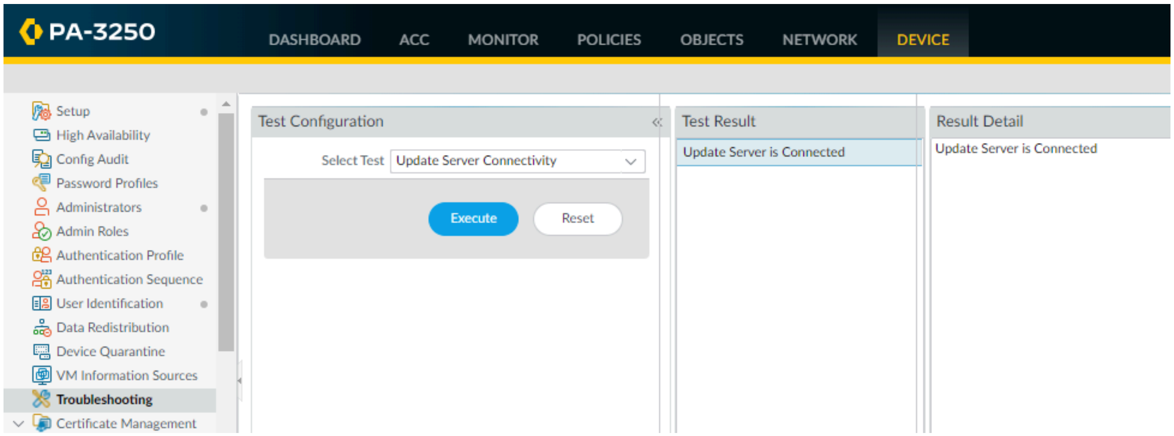
Using a terminal emulation software, such as PuTTY, launch an SSH session to the firewall using the new IP address you assigned to it.

STEP 13 | Verify network access to external services required for NGFW management, such as the Palo Alto Networks Update Server.

You can do this in one of the following ways:

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

1. Use update server connectivity test to verify network connectivity to the Palo Alto Networks Update server as shown in the following example:
    1. Select **Device** > **Troubleshooting**, and select **Update Server Connectivity** from the Select Test drop-down.
    2. **Execute** the update server connectivity test.



Select Test: Update Server Connectivity

Test Result: Update Server is Connected

Result Detail: Update Server is Connected

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

```
request support
check
```

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

```
Contact Us

https://www.paloaltonetworks.com/company/contact-us.html

Support Home

https://www.paloaltonetworks.com/support/tabs/overview.html

Device not found on this update server
```

Perform the Initial Setup and Configuration for NGFWs (Air Gapped)

The air gapped NGFW cannot connect to the Palo Alto Networks update server because an outbound internet connection is required. To activate licenses, upgrade the PAN-OS software version, and install dynamic content updates you must upload the relevant files to the air gapped NGFW manually.

STEP 1 | Gather the required information from your network administrator.

- □ Private IP address for the management (MGT) port
- □ Netmask
- □ Default gateway
- □ DNS server address
- □ NTP server address

STEP 2 | Install and power on the NGFW.

Review your NGFW hardware reference guide for details and best practices.

STEP 3 | Connect to the NGFW.

You must log in using the default **`admin`** username. You are immediately prompted to change the default `admin` password before you can continue. The new password must be a minimum of eight characters and include a minimum of one lowercase and one uppercase character, as well as one number or special character.

You can connect to the NGFW in one of the following ways:

- Connect a serial cable from your computer to the Console port and connect to the device using terminal emulation software (9600-8-N-1). Wait a few minutes for the boot-up sequence to complete; when the NGFW is ready, the prompt changes to the name of the NGFW, for example `PA-220 login`.
- Log in to the NGFW web interface by connecting an RJ-45 Ethernet cable from your computer to the MGT interface on the NGFW. From a browser, go to **`https://192.168.1.1`**.

You may need to change the IP address on your computer to an address in the 192.168.1.0/24 network, such as 192.168.1.2, to access this URL.

STEP 4 | (Best Practices) Disable Zero Touch Provisioning (ZTP).

ZTP can only be disabled from the firewall CLI. The NGFW reboots after you disable ZTP.

Continue to the next steps after the NGFW has rebooted and you can log back in.

- **PA-5400 Series, PA-3400 Series, PA-1400 Series, and PA-400 Series**

  ```
  admin> set system ztp disable
  ```

- **All Other NGFWs**

  ```
  admin> request disable-ztp
  ```

STEP 5 | Configure the network settings for the air gapped NGFW.

The following commands set the interface IP allocation to `static`, configures the IP address for the MGT interface, the Domain Name Server (DNS), and Network Time Protocol (NTP) server.

```
admin> configure
```

```
admin# set deviceconfig system type static
```

```
admin# set deviceconfig system ip-address <IP-Address> netmask
 <Netmask-IP> default-gateway <Gateway-IP>
```

```
admin# set deviceconfig system dns-settings servers primary <IP-
Address> secondary <IP-Address>
```

```
admin# set deviceconfig system ntp-servers primary-ntp-server ntp-
server-address <IP-Address>
```

```
admin# set deviceconfig system ntp-servers secondary-ntp-server
 ntp-server-address <IP-Address>
```

STEP 6 | Register the NGFW with the Palo Alto Networks Customer Support Portal (CSP).

1. Log in to the Palo Alto Networks CSP.
2. Click **Register a Device**.
3. Select **Register device using Serial Number** and click **Next**.
4. Enter the required `Device Information`.
   - Enter the NGFW **Serial Number**.
   - Check (enable) **Device will be used offline**.
   - Select the PAN-OS **OS Release** running on the NGFW.
5. Enter the required `Location Information`.
   - Enter the **City** the NGFW is located in,
   - Enter the **Postal Code** the NGFW is located in,
   - Enter the **Country** the NGFW is located in.
6. **Agree and Submit**.
7. **Skip this step** when prompted to generate the optional `Day 1 Configuration` config file.

STEP 7 | Download your NGFW license keys.

The license key files are required to activate your NGFW licenses when air gapped.

1. Log in to the Palo Alto Networks CSP.
2. Select **Product** > **Devices** and locate the NGFW you added.
3. Download all license keys files from the download links available `License` column.

   You must download a license key file for each license you want to active on the NGFW.

STEP 8 | Activate the NGFW licenses.

1. Log in to the firewall web interface.
2. Select **Device** > **Licenses** and **Manually upload license key**.

   Click **Choose File** to select the license key file you downloaded in the previous step and click **OK**.
3. Repeat this step to uploaded and activate all licenses.

STEP 9 | (Optional) Configure general NGFW settings as needed.

1. Select **Device** > **Setup** > **Management** and edit the General Settings.
2. Enter a **Hostname** for the NGFW and enter your network **Domain** name. The domain name is just a label; it will not be used to join the domain.
3. Enter **Login Banner** text that informs users who are about to log in that they require authorization to access the NGFW management functions.

   As a best practice, avoid using welcoming verbiage. Additionally, you should ask your legal department to review the banner message to ensure it adequately warns that unauthorized access is prohibited.

4. Enter the **Latitude** and **Longitude** to enable accurate placement of the device on the world map.
5. Click **OK**.
6. **Commit** your changes.

STEP 10 | Upgrade the NGFW PAN-OS and dynamic content versions.

Review the PAN-OS Upgrade Guide and PAN-OS Release Notes for detailed information about your target PAN-OS upgrade version.

1. Log in to the Palo Alto Networks CSP.
2. Download dynamic content updates.
   1. Select **Updates** > **Dynamic Updates**.
   2. Select the dynamic `Content type` you want to install.
   3. **Download** the dynamic content update to your local device.
   4. Repeat this step to download all required dynamic content updates.
3. Download a PAN-OS software update.
   1. Select **Updates** > **Software Updates**.
   2. For the `Content type`, select the NGFW model. For the `Release type`, select **All**(default) or **Preferred**.
   3. In the `Download` column, click the PAN-OS version to download the software image to your local device.
4. Log in to the NGFW web interface.
5. Select **Device** > **Dynamic Updates** and **Upload** the dynamic content updates you downloaded.

   Repeat this step to **Browse** and select all the dynamic content release versions.
6. **Install** the dynamic content updates.
7. Select **Device** > **Software** and **Upload** the PAN-OS software image you download.
8. **Install** the PAN-OS software version.

   The device needs to restart to finish installing the PAN-OS software upgrade.

STEP 11 | Connect the NGFW to your network.

1. Disconnect the device from your computer.
2. (All NGFWs except for the PA-5450) Connect the MGT port to a switch port on your management network using an RJ-45 Ethernet cable. Make sure that the switch port you cable the device to is configured for autonegotiation.
3. (PA-5450 only) Connect the MGT port to a switch port on your management network using a Palo Alto Networks certified SFP/SFP+ transceiver and cable.

STEP 12 | Verify the air gapped NGFW connectivity.

1. Log in to the NGFW web interface.
2. Select **Device** > **Troubleshooting**.
3. Verify the NGFW can reach required internal devices.
    1. For `Select Test`, select **ping**.
    2. For the `Host`, enter an internal IP address to verify the NGFW can reach a device in the air gapped network.
    3. Click **Execute** and wait for the test to complete.

       Click the `Test Result` when displayed to review the `Result Detail` to confirm the firewall can successfully ping the internal device.
    4. Repeat this step to verify the NGFW can reach all required internal devices.
4. Verify the NGFW cannot reach devices outside of the air gapped network.
    1. For `Select Test`, select **ping**.
    2. For the `Host`, enter an external IP address to verify the NGFW cannot reach devices outside of the air gapped network.
    3. Click **Execute** and wait for the test to complete.

       Click the `Test Result` when displayed to review the `Result Detail` to confirm the NGFW cannot ping the external device.

Set Up Network Access for External Services

Where Can I Use This?	What Do I Need?
• NGFWs	□ No prerequisites needed

By default, the NGFW uses the MGT interface to access remote services, such as DNS servers, content updates, and license retrieval. If you do not want to enable external network access to your management network, you must set up an in-band data port to provide access to required external services and set up service routes to instruct the NGFW what port to use to access the external services.

Do not enable management access from the internet or from other untrusted zones inside your enterprise security boundary. Follow the Administrative Access Best Practices *to ensure that you are properly securing your NGFW.*

This task requires familiarity with NGFW interfaces, zones, and policies. For more information on these topics, see Configure Interfaces and Zones *and* Set Up a Basic Security Policy.

STEP 1 | Decide which interface you want to use for access to external services and connect it to your switch or router port.

The interface you use must have a static IP address.

STEP 2 | Log in to the NGFW web interface.

Using a secure connection (https) from your web browser, log in using the new IP address and password you assigned during initial configuration (https://<IP address>). You will see a certificate warning; that is okay. Continue to the web page.

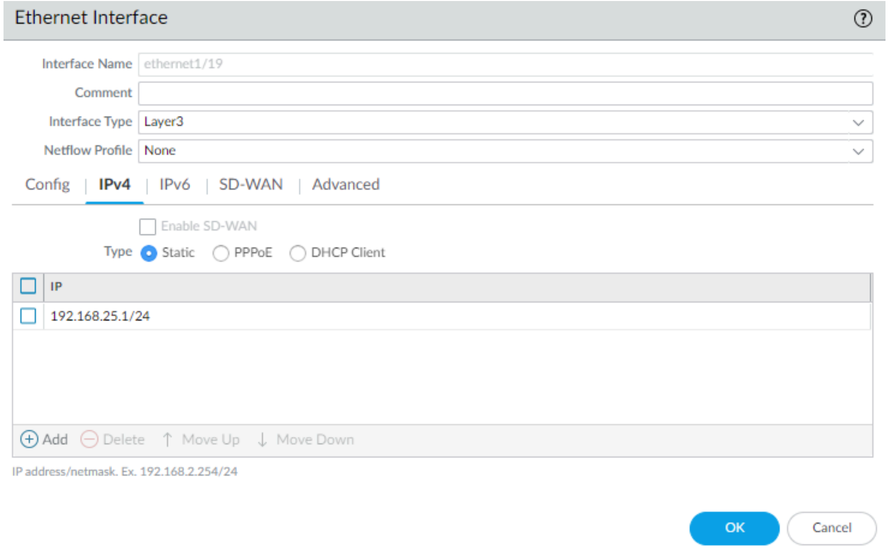
STEP 3 | (Optional) The NGFW comes preconfigured with a default virtual wire interface between ports Ethernet 1/1 and Ethernet 1/2 (and a corresponding default security policy and zones). If you do not plan to use this virtual wire configuration, you must manually delete the configuration to prevent it from interfering with other interface settings you define.

You must delete the configuration in the following order:

1. To delete the default security policy, select **Policies** > **Security**, select the rule, and click **Delete**.
2. To delete the default virtual wire, select **Network** > **Virtual Wires**, select the virtual wire and click **Delete**.
3. To delete the default trust and untrust zones, select **Network** > **Zones**, select each zone and click **Delete**.
4. To delete the interface configurations, select **Network** > **Interfaces** and then select each interface (ethernet1/1 and ethernet1/2) and click **Delete**.
5. **Commit** the changes.

STEP 4 | Configure the interface you plan to use for external access to management services.

1. Select **Network** > **Interfaces** and select the interface that corresponds to the interface you cabled in Step 1.
2. Select the **Interface Type**. Although your choice here depends on your network topology, this example shows the steps for **Layer3**.
3. On the **Config** tab, expand the **Security Zone** drop-down and select **New Zone**.
4. In the Zone dialog, enter a **Name** for new zone, for example Management, and then click **OK**.
5. Select the **IPv4** tab, select the **Static** radio button, and click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.1.254/24. You must use a static IP address on this interface.



Interface Name: ethernet1/19
Comment:
Interface Type: Layer3
Netflow Profile: None

□ Enable SD-WAN

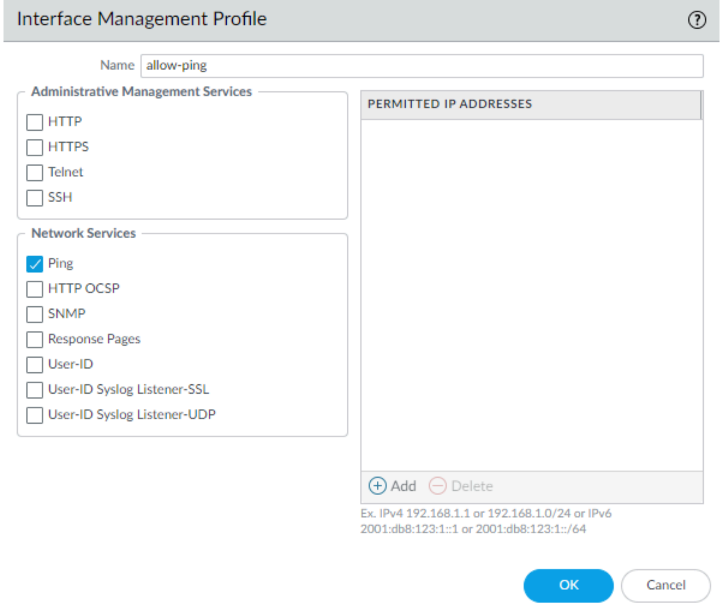
Type ● Static ○ PPPoE ○ DHCP Client

□	IP
□	192.168.25.1/24

IP address/netmask. Ex. 192.168.2.254/24

6. Select **Advanced** > **Other Info**, expand the **Management Profile** drop-down, and select **New Management Profile**.
7. Enter a **Name** for the profile, such as allow_ping, and then select the services you want to allow on the interface. For the purposes of allowing access to the external services, you probably only need to enable **Ping** and then click **OK**.

These services provide management access to the NGFW, so only select the services that correspond to the management activities you want to allow on this interface. For example, don't enable HTTP or Telnet because those protocols transmit in plaintext and therefore aren't secure. Or if you plan to use the MGT interface for NGFW configuration tasks through the web interface or CLI, you don't enable HTTP, HTTPS, SSH, or Telnet so that you prevent unauthorized access through the interface (if you must allow HTTPS or SSH in this scenario, limit access to a specific set of ***Permitted IP Addresses****). For details, see* Use Interface Management Profiles to Restrict Access.



Name allow-ping

Administrative Management Services

□ HTTP
□ HTTPS
□ Telnet
□ SSH

Network Services

☑ Ping
□ HTTP OCSP
□ SNMP
□ Response Pages
□ User-ID
□ User-ID Syslog Listener-SSL
□ User-ID Syslog Listener-UDP

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

8. To save the interface configuration, click **OK**.

STEP 5 | Configure the Service Routes.

By default, the NGFW uses the MGT interface to access the external services it requires. To change the interface the NGFW uses to send requests to external services, you must edit the service routes.

This example shows how to set up global service routes. For information on setting up network access to external services on a virtual system basis rather than a global basis, see Customize Service Routes to Services for Virtual Systems.

1. Select **Device** > **Setup** > **Services** > **Global** and click **Service Route Configuration**.

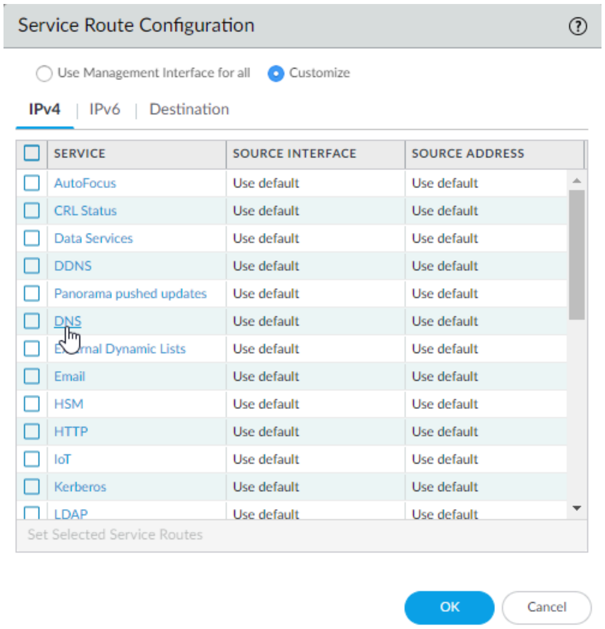
   For the purposes of activating your licenses and getting the most recent content and software updates, you will want to change the service route for ***DNS****,* ***Palo Alto Networks Services****,* ***URL Updates****, and* ***AutoFocus****.*

2. Click the **Customize** radio button, and select one of the following:

   - For a predefined service, select **IPv4** or **IPv6** and click the link for the service. To limit the drop-down list for Source Address, select **Source Interface** and select the interface you just configured. Then select a Source Address (from that interface) as the service route.

If more than one IP address is configured for the selected interface, the **Source Address** drop-down allows you to select an IP address.

- To create a service route for a custom destination, select **Destination**, and click **Add**. Enter a **Destination** IP address. An incoming packet with a destination address that matches this address will use as its source the Source Address you specify for this service route. To limit the drop-down for Source Address, select a **Source Interface**. If more than one IP address is configured for the selected interface, the **Source Address** drop-down allows you to select an IP address.



Service Route Configuration

○ Use Management Interface for all ● Customize

IPv4 | IPv6 | Destination

□	SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
□	AutoFocus	Use default	Use default
□	CRL Status	Use default	Use default
□	Data Services	Use default	Use default
□	DDNS	Use default	Use default
□	Panorama pushed updates	Use default	Use default
□	DNS	Use default	Use default
□	External Dynamic Lists	Use default	Use default
□	Email	Use default	Use default
□	HSM	Use default	Use default
□	HTTP	Use default	Use default
□	IoT	Use default	Use default
□	Kerberos	Use default	Use default
□	LDAP	Use default	Use default

3. Click **OK** to save the settings.
4. Repeat Steps 5.2 - 5.3 above for each service route you want to modify.
5. **Commit** your changes.

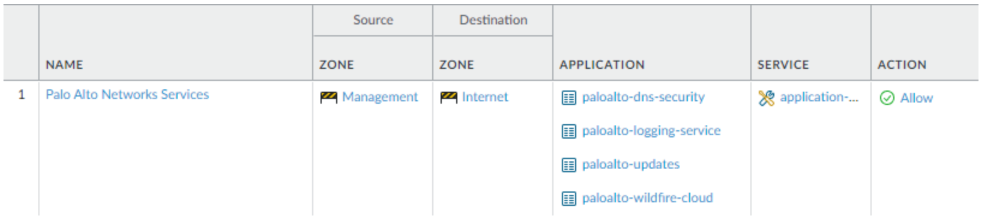
STEP 6 | Configure an external-facing interface and an associated zone and then create a security policy rule to allow the NGFW to send service requests from the internal zone to the external zone.

1. Select **Network** > **Interfaces** and then select the external-facing interface. Select **Layer3** as the **Interface Type**, **Add** the **IP** address (on the **IPv4** or **IPv6** tab), and create the

associated **Security Zone** (on the **Config** tab), such as Internet. This interface must have a static IP address; you do not need to set up management services on this interface.

2. To set up a security rule that allows traffic from your internal network to the Palo Alto Networks update server, select **Policies** > **Security** and click **Add**.

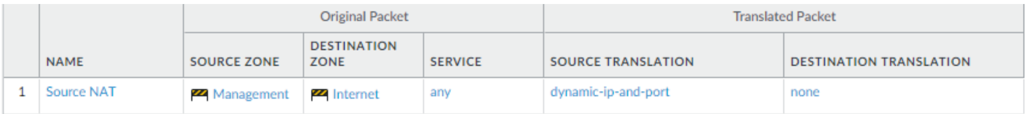
As a best practice when creating Security policy rules, use application-based rules instead of port-based rules to ensure that you are accurately identifying the underlying application regardless of the port, protocol, evasive tactics, or encryption in use. Always leave the ***Service*** *set to* ***application-default****. In this case, create a security policy rule that allows access to the update server (and other Palo Alto Networks services).*



		Source	Destination			
	NAME	ZONE	ZONE	APPLICATION	SERVICE	ACTION
1	Palo Alto Networks Services	Management	Internet	paloalto-dns-security paloalto-logging-service paloalto-updates paloalto-wildfire-cloud	application-...	✓ Allow

STEP 7 | Create a NAT policy rule.

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

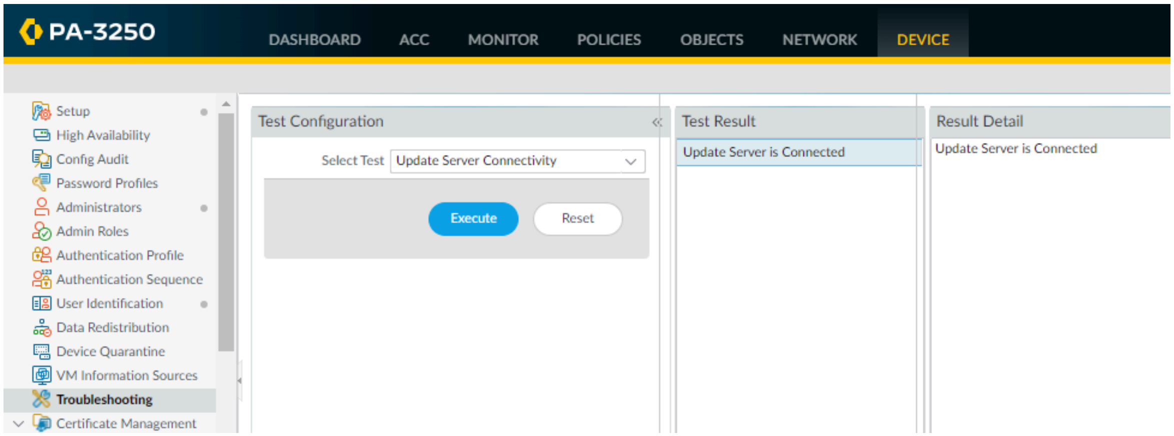


		Original Packet			Translated Packet	
	NAME	SOURCE ZONE	DESTINATION ZONE	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Source NAT	Management	Internet	any	dynamic-ip-and-port	none

STEP 8 | Select **Device** > **Troubleshooting** and verify that you have connectivity from the data port to the external services, including the default gateway, using the **Ping** connectivity test, and the Palo Alto Networks Update Server using the **Update Server Connectivity** test. In this example, the NGFW connectivity to the Palo Alto Networks Update Server is tested.

After you verify you have the required network connectivity, continue to Register the NGFW and Activate Subscription Licenses.

1. Select **Update Server** from the Select Test drop-down.
2. **Execute** the Palo Alto Networks Update Server connectivity test.



Select Test: Update Server Connectivity

Update Server is Connected

Update Server is Connected

3. Access the NGFW CLI, and use the following command to retrieve information on the support entitlement for the NGFW from the Palo Alto Networks update server:

```
request support
check
```

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

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

STEP 9 | **(Optional)** Install a Device Certificate if you plan to manage your NGFWs through Strata Cloud Manager.

STEP 10 | (Optional) Setup Device Telemetry if you plan to manage your NGFWs through Strata Cloud Manager.

1. Enable Strata Logging Service.
2. Navigate to **Device** > **Setup** > **Telemetry**.
3. In **Telemetry Destination**, select your region, if it is not automatically selected. If your organization is using Strata Logging Service, you must use the region that your Strata Logging Service is configured to use.
4. Click **OK**, and then commit your changes.

Beginning with PAN-OS 11.2.8 and later releases, the telemetry autoenablement feature *configures telemetry to be enabled by default on your devices. Upon onboarding a new device (Panorama or firewall), telemetry is automatically enabled with settings centrally controlled through Strata Cloud Manager. This centralized approach ensures consistent telemetry settings across your entire environment.*

Cheat Sheet: Onboard NGFWs to Panorama or Strata Cloud Manager

Where Can I Use This?	What Do I Need?
• NGFW	Onboarding Prerequisites: □ Prerequisites for Strata Cloud Manager □ Prerequisites for Panorama

Now that your initial setup and basic configuration are complete, the next optional step is onboarding your NGFWs to a centralized management platform. The transition from individual device management to a centralized management system significantly enhances your ability to maintain consistent security policies, streamline administrative tasks, and gain comprehensive visibility across your entire NGFW infrastructure. It also opens up the possibility of managing your NGFWs alongside Prisma Access deployments. Whether you choose Strata Cloud Manager for cloud-native management or Panorama for on-premises centralized control, onboarding your NGFWs establishes the foundation for scalable security management, automated policy deployment, and unified monitoring that grows with your organization's needs.

By following the comprehensive onboarding process, your NGFWs will be successfully integrated into centralized management, providing the foundation for efficient, scalable security administration across your network infrastructure.

You can find the detailed onboarding instructions in the respective product areas using this cheat sheet and the links below.

Onboarding NGFWs to Strata Cloud Manager

Before beginning the NGFW onboarding process to Strata Cloud Manager, ensure you have:

- A valid Strata Cloud Manager license and account
- Initial configuration is complete
- Administrative access to your NGFWs web interface or CLI
- DNS resolution configured on your NGFW
- Device Certificate installed on your device
- Device Telemetry has been enabled

For more information and detailed instructions for the activation and onboarding process for Strata Cloud Manager, click here.

Onboarding NGFWs to Panorama

Before beginning the NGFW onboarding process to Panorama, ensure you have:

- Panorama server is deployed and accessible

- Sufficient Panorama device licenses available
- Initial configuration is complete
- Administrative access to your NGFWs web interface or CLI

For more information and detailed instructions for the activation and onboarding process for Panorama, click here.

Segment Your Network for a Reduced Attack Surface

Where Can I Use This?	What Do I Need?
• NGFWs	□ No prerequisites needed

Traffic must pass through the NGFW in order for the NGFW to manage and control it. Physically, traffic enters and exits the NGFW through *interfaces*. The NGFW determines how to act on a packet based on whether the packet matches a *Security policy rule*. At the most basic level, each Security policy rule must identify where the traffic came from and where it is going.

On a Palo Alto Networks NGFWs, Security policy rules are applied between zones. A *zone* is a grouping of interfaces (physical or virtual) that represents a segment of your network that is connected to, and controlled by, the NGFW. Because traffic can only flow between zones if there is a Security policy rule to allow it, this is your first line of defense. The more granular the zones you create, the greater control you have over access to sensitive applications and data and the more protection you have against malware moving laterally throughout your network.

For example, you might want to segment access to the database servers that store your customer data into a zone called Customer Data. You can then define security policies that only permit certain users or groups of users to access the Customer Data zone, thereby preventing unauthorized internal or external access to the data stored in that segment.

The following diagram shows a very basic example of network segmentation using zones. The more granular you make your zones (and the corresponding security policy rules that allows traffic between zones), the more you reduce the attack surface on your network. This is because traffic can flow freely within a zone (intra-zone traffic), but traffic cannot flow between zones (inter-zone traffic) until you define a Security policy rule that allows it.

Additionally, an interface cannot process traffic until you have assigned it to a zone. Therefore, by segmenting your network into granular zones you have more control over access to sensitive applications or data and you can prevent malicious traffic from establishing a communication channel within your network, thereby reducing the likelihood of a successful attack on your network.

To start configuring zones and interfaces, click here.

Configure Interfaces and Zones

Where Can I Use This?	What Do I Need?
• NGFW	One of these licenses for Strata Cloud Manager managed NGFWs: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

After you identify how you want to segment your network and the zones you will need to create to achieve the segmentation (as well as the interfaces to map to each zone), you can begin configuring the interfaces and zones on the NGFW. Configure interfaces on the NGFW to support the topology of each part of the network you are connecting to. The following workflow shows how to configure Layer 3 interfaces and assign them to zones. For details on integrating the NGFW using a different type of interface deployments (for example as virtual wire interfaces or as Layer 2 interfaces), see the Networking Administration guide.

For more information about Zones, click here.

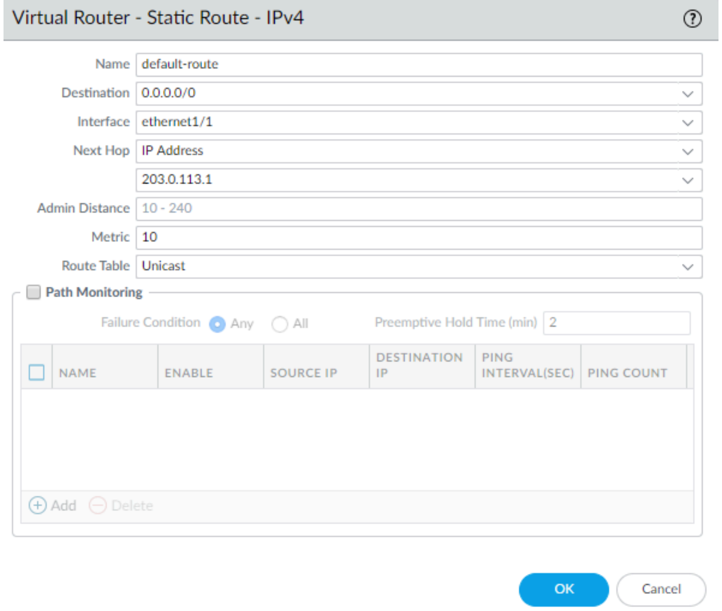
> *The NGFW comes preconfigured with a default virtual wire interface between ports Ethernet 1/1 and Ethernet 1/2 (and a corresponding default security policy and virtual router). If you do not plan to use the default virtual wire, you must manually delete the configuration and commit the change before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

- PAN-OS & Panorama
- Strata Cloud Manager

Configure Interfaces and Zones (PAN-OS)

STEP 1 | Configure a default route to your Internet router.

1. Select **Network** > **Virtual Router** and then select the **default** link to open the Virtual Router dialog.
2. Select the **Static Routes** tab and click **Add**. Enter a **Name** for the route and enter the route in the **Destination** field (for example, 0.0.0.0/0).
3. Select the **IP Address** radio button in the **Next Hop** field and then enter the IP address and netmask for your Internet gateway (for example, 203.0.113.1).



Virtual Router - Static Route - IPv4

Name	default-route
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	203.0.113.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast

□ Path Monitoring

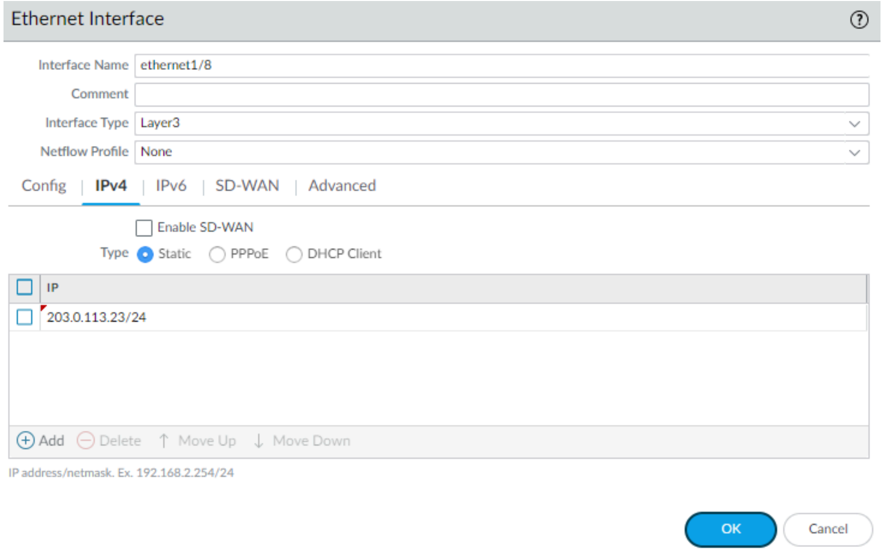
Failure Condition ● Any ○ All   Preemptive Hold Time (min) 2

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

4. Click **OK** twice to save the virtual router configuration.

STEP 2 | Configure the external interface (the interface that connects to the Internet).

1. Select **Network** > **Interfaces** and then select the interface you want to configure. In this example, we are configuring Ethernet1/8 as the external interface.
2. Select the **Interface Type**. Although your choice here depends on interface topology, this example shows the steps for **Layer3**.
3. On the **Config** tab, select **New Zone** from the **Security Zone** drop-down. In the Zone dialog, define a **Name** for new zone, for example Internet, and then click **OK**.
4. In the **Virtual Router** drop-down, select **default**.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 203.0.113.23/24.



Ethernet Interface

Interface Name	ethernet1/8
Comment	
Interface Type	Layer3
Netflow Profile	None

□ Enable SD-WAN

Type ● Static ○ PPPoE ○ DHCP Client

□	IP
□	203.0.113.23/24

IP address/netmask. Ex. 192.168.2.254/24

6. To enable you to ping the interface, select **Advanced** > **Other Info**, expand the **Management Profile** drop-down, and select **New Management Profile**. Enter a **Name** for the profile, select **Ping** and then click **OK**.
7. To save the interface configuration, click **OK**.

STEP 3 | Configure the interface that connects to your internal network.

In this example, the interface connects to a network segment that uses private IP addresses. Because private IP addresses cannot be routed externally, you have to configure NAT.

1. Select **Network** > **Interfaces** and select the interface you want to configure. In this example, we are configuring Ethernet1/15 as the internal interface our users connect to.
2. Select **Layer3** as the **Interface Type**.
3. On the **Config** tab, expand the **Security Zone** drop-down and select **New Zone**. In the Zone dialog, define a **Name** for new zone, for example Users, and then click **OK**.
4. Select the same Virtual Router you used previously, default in this example.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 192.168.1.4/24.
6. To enable you to ping the interface, select the management profile that you just created.
7. To save the interface configuration, click **OK**.

STEP 4 | Configure the interface that connects to your data center applications.

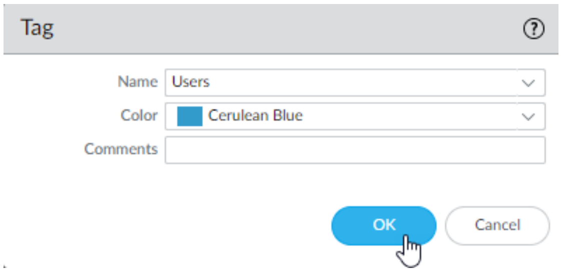
Make sure you define granular zones to prevent unauthorized access to sensitive applications or data and eliminate the possibility of malware moving laterally within your data center.

1. Select the interface you want to configure.
2. Select **Layer3** from the **Interface Type** drop-down. In this example, we are configuring Ethernet1/1 as the interface that provides access to your data center applications.
3. On the **Config** tab, expand the **Security Zone** drop-down and select **New Zone**. In the Zone dialog, define a **Name** for new zone, for example Data Center Applications, and then click **OK**.
4. Select the same Virtual Router you used previously, default in this example.
5. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 10.1.1.1/24.
6. To enable you to ping the interface, select the management profile that you created.
7. To save the interface configuration, click **OK**.

STEP 5 | (Optional) Create tags for each zone.

Tags allow you to visually scan policy rules.

1. Select **Objects** > **Tags** and **Add**.
2. Select a zone **Name**.
3. Select a tag **Color** and click **OK**.



Name: Users
Color: Cerulean Blue
Comments:

STEP 6 | Save the interface configuration.

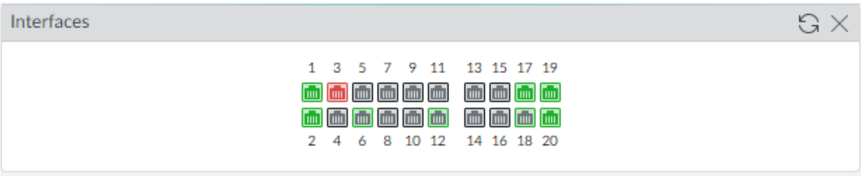
Click **Commit**.

STEP 7 | Cable the NGFW.

Attach straight through cables from the interfaces you configured to the corresponding switch or router on each network segment.

STEP 8 | Verify that the interfaces are active.

Select **Dashboard** and verify that the interfaces you configured show as green in the Interfaces widget.



Configure Interfaces and Zones (SCM)

Create an Interface

Interfaces serve as the fundamental building blocks of your firewall's network connectivity, defining how traffic enters, exits, and flows through your security infrastructure. In Strata Cloud Manager, you can create and configure various types of interfaces to match your specific network architecture and deployment requirements, whether you're implementing network segmentation, connecting to different network zones, or establishing connectivity between network segments. Each interface type serves distinct purposes and operates at different layers of the network stack, from simple traffic monitoring and forwarding to complex routing and switching functions.

The interface configuration determines how the firewall processes traffic, applies security policies, and integrates with your existing network infrastructure. Choose the appropriate interface type based on your network topology, traffic flow requirements, and the level of packet inspection and processing needed for your deployment:

- Routing and Interfaces
  - Configure a Layer 2 Interface
  - Configure a Layer 2 Interface

Create a Zone

Assign one or more firewall interfaces to a zone to segment your network to control protection for each zone individually.

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Configure your NGFW interfaces.

STEP 3 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Device Settings** > **InterfacesConfiguration** > **NGFW and Prisma Access** > **Device Settings** > **Interfaces** and select the Configuration Scope where you want to create the zone.

You can select a folder or firewall from your **Folders** or select **Snippets** to configure the zone in a snippet.

STEP 4 | **Add Zone**.

STEP 5 | Configure the zone.

1. Select the **Interface Type**.

   Select **Layer2** if you want to add Layer 2 interfaces to the zone or **Layer 3** to add Layer 3 interfaces.
2. **Add** one or more interfaces to the zone.
3. (Optional) Select a **Zone Protection Profile** to specify how the firewall responds to attack from this zone.

   Select **Create New** to create a new Zone Protection Profile inline.
4. (Optional) Confirm you want to **Enable Packet Buffer Protection**.

   This setting is enabled by default. The firewall applies Packet Buffer Protection to the ingress zone only to protect the zone from DoS attacks and aggressive sessions and sources.
5. (Optional) **Enable User ID ACL**.

   This setting is disabled by default. When disabled, the firewall applies user mapping information it discovers to all traffic of this zone for use in logs, reports, and policy rules. When enabled, the firewall
6. (Optional) **Enable Device ID ACL**.

   This setting is disabled by default.

STEP 6 | **Save**.

Set Up a Basic Security Policy

Where Can I Use This?	What Do I Need?
• NGFW	One of these licenses for Strata Cloud Manager managed NGFWs: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

Now that you defined some zones and attached them to interfaces, you are ready to begin creating your Security Policy. The NGFW will not allow any traffic to flow from one zone to another unless there is a Security policy rule that allows it. When a packet enters a NGFW interface, the NGFW matches the attributes in the packet against the Security policy rules to determine whether to block or allow the session based on attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service. The NGFW evaluates incoming traffic against the Security policy rulebase from left to right and from top to bottom and then takes the action specified in the first Security rule that matches (for example, whether to allow, deny, or drop the packet). This means that you must order the rules in your Security policy rulebase so that more specific rules are at the top of the rulebase and more general rules are at the bottom to ensure that the NGFW is enforcing policy as expected.

Even though a Security policy rule allows a packet, this does not mean that the traffic is free of threats. To enable the NGFW to scan the traffic that it allows based on a Security policy rule, you must also attach Security Profiles—including URL Filtering, Antivirus, Anti-Spyware, File Blocking, and WildFire Analysis—to each rule (the profiles you can use depend on which subscriptions you purchased). When creating your basic Security policy, use the predefined security profiles to ensure that the traffic you allow into your network is being scanned for threats. You can customize these profiles later as needed for your environment.

Use the following workflows to set up a very basic Security policy that enables access to the network infrastructure, to data center applications, and to the internet. This enables you to get the NGFW up and running so that you can verify that you have successfully configured the NGFW. However, this initial policy is not comprehensive enough to protect your network. After you verify that you successfully configured the NGFW and integrated it into your network, proceed with creating a best practice internet gateway security policy that safely enables application access while protecting your network from attack.

- Strata Cloud Manager
- PAN-OS & Panorama

Set Up a Basic Security Policy (SCM)

For more information about setting up Security Policy Rules in Strata Cloud Manager, click here.

STEP 1 | Add a rule.

1. Select **Configuration** > **NGFW and Prisma Access** > **Security Services** > **Security Policy** > **Add Rule** > **Security Rule** and select **Pre-Rule** and build your rule. Components marked with an asterisk(*) are mandatory.
2. In the **General** tab, enter a descriptive **Name** for the rule.
3. Give a **Description** for your rule's intent.
4. Add a **Tag** to your rules to group them using keywords or phrases.
5. Limit a security rule to specific times using a **Schedule**.

STEP 2 | Define the matching criteria for the source fields in the packet.

1. In the **Source** tab, select a **Source Zone**.
2. Specify a **Source IP Address** or leave the value set to **ny**.
3. You can search for specific **Users**or **User Groups** to enforce policy for individual users or a group of users. Specify the match criteria that define which users and user groups.
   - Sub string or partial string search is not supported for performance reasons.
   - Entire string search is possible when delimiters such as space and hyphen is present.
   - When number of users is more than 500 then string search use quotes with exact string

STEP 3 | Define the matching criteria for the destination fields in the packet.

1. In the **Destination** tab, set the **Zone**.
2. Specify a **Destination IP Address** or leave the value set to **any**.

STEP 4 | Specify the application that the rule will allow or block.

1. In the **Applications** tab, **Add** the **Application** you want to safely enable. You can select multiple applications or you can use application groups or application filters.
2. In the **Service/URL Category** tab, keep the service set to **application-default** to ensure that any applications that the rule allows are allowed only on their standard ports. An administrator can also use an existing App-ID signature and customize it to detect proprietary applications or to detect specific attributes of an existing application. Custom applications are defined in **Objects** > **Applications**

STEP 5 | (Optional) Specify a URL category as match criteria for the rule.

Select **URL Category** or **Tenant Restriction** to specify a specific TCP and/or UDP port number, a URL category, a tenant restriction as match criteria in the security rule. If you select a URL category, only web traffic will match the rule and only if the traffic is destined for that specified category.

STEP 6 | Define what action you want the firewall to take for traffic that matches the rule.

In the **Actions** tab, select an **Action**.

- **Allow**
- **Deny**
- **Drop**
- **Reset Client**
- **Reset Server**
- **Reset Both Client and Server**

STEP 7 | Configure the log settings.

- By default, the rule is set to **Log at Session End**. You can disable this setting if you don't want any logs generated when traffic matches this rule or you can select **Log at Session Start** for more detailed logging.
- Select a **Log Forwarding** profile.

STEP 8 | Attach security profiles to scan all allowed traffic for threats.

In **Actions** > **Profile Group**, select a **Profile Group** from the drop-down to attach to the rule.

STEP 9 | Select **Save** to save the security rule, then **Push Config** to your devices.

Set Up a Basic Security Policy (PAN-OS)

STEP 1 | (Optional) Delete the default Security policy rule.

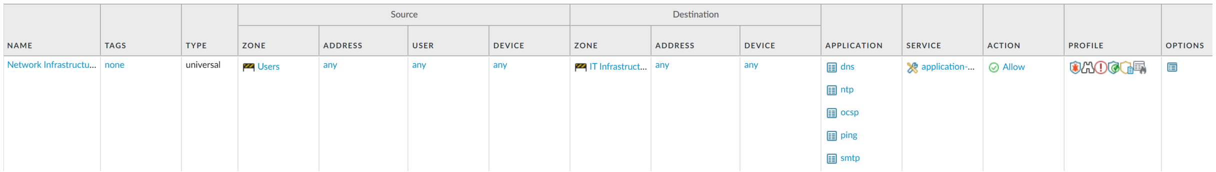
By default, the NGFW includes a Security policy rule named *rule1* that allows all traffic from Trust zone to Untrust zone. You can either delete the rule or modify the rule to reflect your zone-naming conventions.

STEP 2 | Allow access to your network infrastructure resources.

1. Select **Policies** > **Security** and click **Add**.
2. In the **General** tab, enter a descriptive **Name** for the rule.
3. In the **Source** tab, set the **Source Zone** to **Users**.
4. In the **Destination** tab, set the **Destination Zone** to **IT Infrastructure**.

   *As a best practice, use address objects in the **Destination Address** field to enable access to specific servers or groups of servers only, particularly for services such as DNS and SMTP that are commonly exploited. By restricting users to specific destination server addresses, you can prevent data exfiltration and command and control traffic from establishing communication through techniques such as DNS tunneling.*

5. In the **Applications** tab, **Add** the applications that correspond to the network services you want to safely enable. For example, select **dns**, **ntp**, **ocsp**, **ping**, and **smtp**.
6. In the **Service/URL Category** tab, keep the **Service** set to **application-default**.
7. In the **Actions** tab, set the **Action Setting** to **Allow**.
8. Set **Profile Type** to **Profiles** and select the following security profiles to attach to the policy rule:
   - For **Antivirus**, select **default**
   - For **Vulnerability Protection**, select **strict**
   - For **Anti-Spyware**, select **strict**
   - For **URL Filtering**, select **default**
   - For **File Blocking**, select **basic file blocking**
   - For **WildFire Analysis**, select **default**
9. Verify that **Log at Session End** is enabled. Only traffic that matches a Security policy rule will be logged.
10. Click **OK**.

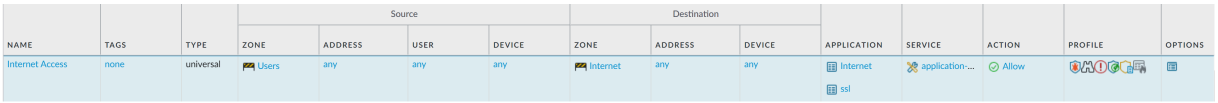


			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Network Infrastructu...	none	universal	Users	any	any	any	IT Infrastruct...	any	any	dns ntp ocsp ping smtp	application-...	Allow		

STEP 3 | Enable access to general internet applications.

This is a temporary rule that allows you to gather information about the traffic on your network. After you have more insight into which applications your users need to access, you can make informed decisions about which applications to allow and create more granular application-based rules for each user group.

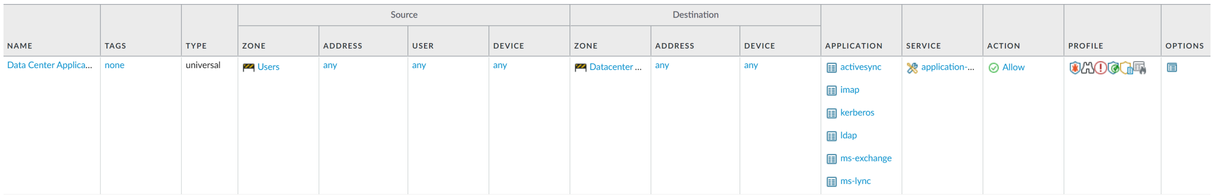
1. Select **Policies** > **Security** and **Add** a rule.
2. In the **General** tab, enter a descriptive **Name** for the rule.
3. In the **Source** tab, set the **Source Zone** to **Users**.
4. In the **Destination** tab, set the **Destination Zone** to **Internet**.
5. In the **Applications** tab, **Add** an **Application Filter** and enter a **Name**. To safely enable access to legitimate web-based applications, set the **Category** in the application filter to **general-internet** and then click **OK**. To enable access to encrypted sites, **Add** the **ssl** application.
6. In the **Service/URL Category** tab, keep the **Service** set to **application-default**.
7. In the **Actions** tab, set the **Action Setting** to **Allow**.
8. Set **Profile Type** to **Profiles** and select the following security profiles to attach to the policy rule:
   - For **Antivirus**, select **default**
   - For **Vulnerability Protection**, select **strict**
   - For **Anti-Spyware**, select **strict**
   - For **URL Filtering**, select **default**
   - For **File Blocking**, select **strict file blocking**
   - For **WildFire Analysis**, select **default**
9. Verify that **Log at Session End** is enabled. Only traffic that matches a security rule will be logged.
10. Click **OK**.



			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Internet Access	none	universal	Users	any	any	any	Internet	any	any	Internet ssl	application-...	Allow		

STEP 4 | Enable access to data center applications.

1. Select **Policies** > **Security** and **Add** a rule.
2. In the **General** tab, Enter a descriptive **Name** for the rule.
3. In the **Source** tab, set the **Source Zone** to **Users**.
4. In the **Destination** tab, set the **Destination Zone** to **Data Center Applications**.
5. In the **Applications** tab, **Add** the applications that correspond to the network services you want to safely enable. For example, select **activesync**, **imap**, **kerberos**, **ldap**, **ms-exchange**, and **ms-lync**.
6. In the **Service/URL Category** tab, keep the **Service** set to **application-default**.
7. In the **Actions** tab, set the **Action Setting** to **Allow**.
8. Set **Profile Type** to **Profiles** and select the following security profiles to attach to the policy rule:
   - For **Antivirus**, select **default**
   - For **Vulnerability Protection** select **strict**
   - For **Anti-Spyware** select **strict**
   - For **URL Filtering** select **default**
   - For **File Blocking** select **basic file blocking**
   - For **WildFire Analysis** select **default**
9. Verify that **Log at Session End** is enabled. Only traffic that matches a security rule will be logged.
10. Click **OK**.



			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Data Center Applica...	none	universal	Users	any	any	any	Datacenter ...	any	any	activesync imap kerberos ldap ms-exchange ms-lync	application-...	Allow		

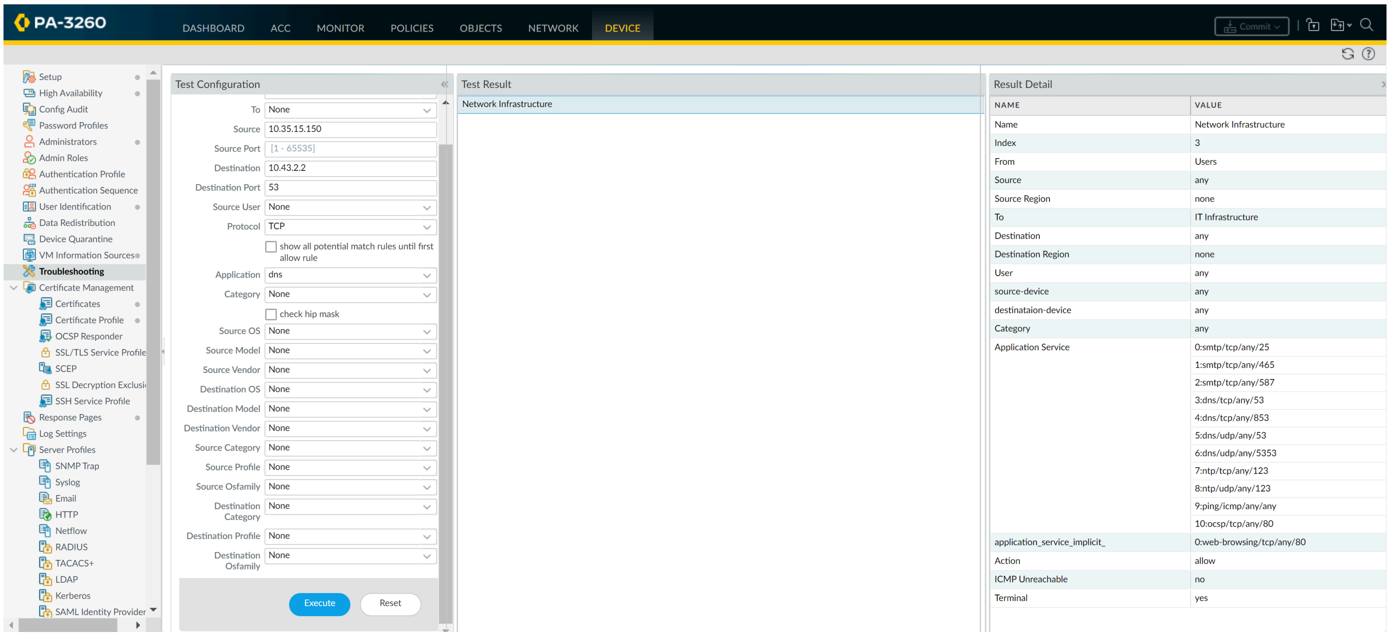
STEP 5 | Save your policy rules to the running configuration on the NGFW.

Click **Commit**.

STEP 6 | To verify that you have set up your basic policies effectively, test whether your Security policy rules are being evaluated and determine which Security policy rule applies to a traffic flow.

For example, to verify the policy rule that will be applied for a client in the user zone with the IP address 10.35.14.150 when it sends a DNS query to the DNS server in the data center:

1. Select **Device** > **Troubleshooting** and select **Security Policy Match** (**Select Test**).
2. Enter the **Source** and **Destination** IP addresses.
3. Enter the **Protocol**.
4. Select **dns** (**Application**)
5. **Execute** the Security policy match test.



Test Configuration

To	None
Source	10.35.15.150
Source Port	[1 - 65535]
Destination	10.43.2.2
Destination Port	53
Source User	None
Protocol	TCP
	□ show all potential match rules until first allow rule
Application	dns
Category	None
	□ check hip mask
Source OS	None
Source Model	None
Source Vendor	None
Destination OS	None
Destination Model	None
Destination Vendor	None
Source Category	None
Source Profile	None
Source Osfamily	None
Destination Category	None
Destination Profile	None
Destination Osfamily	None

Test Result

Network Infrastructure

Result Detail

NAME	VALUE
Name	Network Infrastructure
Index	3
From	Users
Source	any
Source Region	none
To	IT Infrastructure
Destination	any
Destination Region	none
User	any
source-device	any
destinataion-device	any
Category	any
Application Service	0:smtp/tcp/any/25 1:smtp/tcp/any/465 2:smtp/tcp/any/587 3:dns/tcp/any/53 4:dns/tcp/any/853 5:dns/udp/any/53 6:dns/udp/any/5353 7:ntp/tcp/any/123 8:ntp/udp/any/123 9:ping/icmp/any/any 10:ocsp/tcp/any/80
application_service_implicit_	0:web-browsing/tcp/any/80
Action	allow
ICMP Unreachable	no
Terminal	yes

Assess Network Traffic

Where Can I Use This?	What Do I Need?
• NGFW	One of these licenses for Strata Cloud Manager managed NGFWs: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

Maintaining optimal network health for your NGFWs is essential for ensuring robust security posture, reliable performance, and operational efficiency across your infrastructure. Regular assessment of NGFW health involves monitoring key performance indicators, analyzing system resource utilization, reviewing hardware and software status, and evaluating traffic processing capabilities to identify potential bottlenecks or security gaps before they impact your network. By establishing comprehensive health monitoring practices, administrators can proactively address issues such as high CPU utilization, memory constraints, interface congestion, and policy inefficiencies while ensuring that security services like threat prevention, URL filtering, and application identification continue to operate at peak effectiveness. Whether managing a single firewall or a distributed security architecture, systematic health assessment provides the visibility and insights necessary to optimize configuration settings, plan capacity requirements, and maintain the high availability and performance standards that modern networks demand.

- Strata Cloud Manager
- PAN-OS & Panorama

Assess Network Traffic (SCM)

Now that you have a basic security policy, you can review the statistics and data in the Strata Cloud Manager Command Center, Activity Insights, and its various dashboards.

Use this information to identify where you need to create more granular security policy rules:

- Use the Command Center

  In the Command Center, review the most used applications and the high-risk applications on your network. The Command Center is a visualized overview of your network and security infrastructure. It provides you with four different views, each with its own tracked data, metrics, and actionable insights to examine and interact with.

- Use Activity Insights

  Activity Insights gives you an in-depth view of your network activities across Prisma Access and NGFW deployments. Activity Insights unifies your network data such as network traffic, application usage, threats, and user activities in one place.

- Evaluate Your Security Policy

  You can use built-in security checks to evaluate the strength of your security rules and policy and determine if any of the following is needed:

  - Whether to allow web content based on schedule, users, or groups.
  - Allow or control certain applications or functions within an application.
  - Decrypt and inspect content.
  - Allow but scan for threats and exploits.
  - For information on refining your security policies and for attaching custom security profiles, see how to create a security policy rule and security profiles.

  For information on refining your security policies and for attaching custom security profiles, see how to create a security policy rule and security profiles.

- View Incidents

  Strata Cloud Manager provides a unified incidents and alerts framework. In one place, view, investigate, and address the alerts and incidents on your network, and jump to your logs to examine the associated activity.

- Monitor Your Network

  Monitor the health and security of everything on your network, and use the IoC Search to investigate the history of an artifact on your network and review global analysis findings. What you can monitor depends on your active security subscriptions.

Assess Network Traffic (PAN-OS)

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

- Use the Application Command Center and the automated correlation engine.

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

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

- Determine what updates/modifications are required for your network security policy rules and implement the changes.

  For example:

  - Evaluate whether to allow web content based on schedule, users, or groups.
  - Allow or control certain applications or functions within an application.
  - Decrypt and inspect content.
  - Allow but scan for threats and exploits.

  For information on refining your security policies and for attaching custom security profiles, see how to create a security policy rule and security profiles.

- View Logs.

  Specifically, view the traffic and threat logs (**Monitor** > **Logs**).

  Traffic logs are dependent on how your security policies are defined and set up to log traffic. The Application Usage widget in the **ACC***, however, records applications and statistics regardless of policy configuration; it shows all traffic that is allowed on your network, therefore it includes the inter-zone traffic that is allowed by policy and the same zone traffic that is allowed implicitly.*

- Configure Log Storage Quotas and Expiration Periods.

  Review the AutoFocus intelligence summary for artifacts in your logs. An *artifact* is an item, property, activity, or behavior associated with logged events on the NGFW. The intelligence summary reveals the number of sessions and samples in which WildFire detected the artifact. Use WildFire verdict information (benign, grayware, malware) and AutoFocus matching tags to look for potential risks in your network.

  AutoFocus tags created by Unit 42*, the Palo Alto Networks threat intelligence team, call attention to advanced, targeted campaigns and threats in your network.*

  From the AutoFocus intelligence summary, you can start an AutoFocus search for artifacts and assess their pervasiveness within global, industry, and network contexts.

- Monitor Web Activity of Network Users.

  Review the URL filtering logs to scan through alerts, denied categories/URLs. URL logs are generated when a traffic matches a security rule that has a URL filtering profile attached with an action of alert, continue, override or block.

Enable Free WildFire Fowarding on Your NGFW

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS)	No prerequisites needed

WildFire is a cloud-based virtual environment that analyzes and executes unknown samples (files and email links) and determines the samples to be malicious, phishing, grayware, or benign. With WildFire enabled, a Palo Alto Networks NGFW can forward unknown samples to WildFire for analysis. For newly-discovered malware, WildFire generates a signature to detect the malware, which is made available for retrieval in real-time for all NGFWs with an active WildFire subscription. This enables all Palo Alto next-generation NGFWs worldwide to detect and prevent malware found by a single NGFW. Malware signatures often match multiple variants of the same malware family, and as such, block new malware variants that the NGFW has never seen before. The Palo Alto Networks threat research team uses the threat intelligence gathered from malware variants to block malicious IP addresses, domains, and URLs.

A basic WildFire service is included as part of the Palo Alto Networks next-generation NGFW and does not require a WildFire subscription. With the basic WildFire service, you can enable the NGFW to forward portable executable (PE) files. Additionally, if you do not have a WildFire subscription, but you do have a Threat Prevention subscription, you can receive signatures for malware WildFire identifies every 24- 48 hours (as part of the Antivirus updates).

Beyond the basic WildFire service, a WildFire subscription is required for the NGFW to:

- Get the latest WildFire signatures in real-time.
- Prevent malicious PE (portable executables), ELF and MS Office files, and PowerShell and shell scripts from entering your network in real-time using WildFire Inline ML.
- Forward advanced file types and email links for analysis.
- Use the WildFire API.
- Use a WildFire appliance to host a WildFire private cloud or a WildFire hybrid cloud.

If you have a WildFire subscription, go ahead and get started with WildFire to get the most out of your subscription. Otherwise, take the following steps to enable basic WildFire forwarding:

STEP 1 | Confirm that your NGFW is registered and that you have a valid support account as well as any subscriptions you require.

1. Log in to the Palo Alto Networks Customer Support Portal (CSP) and on the left-hand side navigation pane, select **Assets** > **Devices**.
2. Verify that the NGFW is listed. If it is not listed, select **Register New Device** and continue to register the NGFW.
3. (Optional) If you have a Threat Prevention subscription, be sure to Activate Subscription Licenses.

STEP 2 | Log in to the NGFW and configure WildFire forwarding settings.

1. Select **Device** > **Setup** > **WildFire** and edit the General Settings.
2. Set the **WildFire Public Cloud** field to forward files to the WildFire global cloud (U.S.) at: **`wildfire.paloaltonetworks.com`**.

   You can also forward files to a WildFire regional cloud or a private cloud based on your location and your organizational requirements.
3. Review the **File Size Limits** for PEs the NGFW forwards for WildFire analysis. set the **Size Limit** for PEs that the NGFW can forward to the maximum available limit of 10 MB.

   *As a WildFire best practice, set the **Size Limit** for PEs to the maximum available limit of 10 MB.*
4. Click **OK** to save your changes.

STEP 3 | Enable the NGFW to forward PEs for analysis.

1. Select **Objects** > **Security Profiles** > **WildFire Analysis** and **Add** a new profile rule.
2. **Name** the new profile rule.
3. **Add** a forwarding rule and enter a **Name** for it.
4. In the **File Types** column, add **pe** files to the forwarding rule.
5. In the **Analysis** column, select **public-cloud** to forward PEs to the WildFire public cloud.
6. Click **OK**.

STEP 4 | Apply the new WildFire Analysis profile to traffic that the NGFW allows.

1. Select **Policies** > **Security** and either select an existing policy rule or create a new policy rule as described in Set Up a Basic Security Policy.
2. Select **Actions** and in the Profile Settings section, set the **Profile Type** to **Profiles**.
3. Select the **WildFire Analysis** profile you just created to apply that profile rule to all traffic this policy rule allows.
4. Click **OK**.

STEP 5 | Enable the NGFW to forward decrypted SSL traffic for WildFire analysis.

STEP 6 | Review and implement WildFire best practices to ensure that you are getting the most of WildFire detection and prevention capabilities.

STEP 7 | **Commit** your configuration updates.

STEP 8 | Verify that the NGFW is forwarding PE files to the WildFire public cloud.

Select **Monitor** > **Logs** > **WildFire Submissions** to view log entries for PEs the NGFW successfully submitted for WildFire analysis. The Verdict column displays whether WildFire found the PE to be malicious, grayware, or benign. (WildFire only assigns the phishing verdict to email links). The Action column indicates whether the NGFW allowed or blocked the sample. The severity column indicates how much of a threat a sample poses to an organization using the following values: critical, high, medium, low, information.

STEP 9 | (Threat Prevention subscription only) If you have a Threat Prevention subscription, but do not have a WildFire subscription, you can still receive WildFire signature updates every 24-48 hours.

1. Select **Device** > **Dynamic Updates**.
2. Check that the NGFW is scheduled to download, and install Antivirus updates.

Device Setup for Cloud Managed Devices

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager)	One of these licenses: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

Setting up a NGFWs for Strata Cloud Manager management requires careful configuration of essential device parameters to establish secure cloud connectivity and local management capabilities.

General Settings Configuration

The initial setup begins with configuring fundamental device parameters including hostname, domain settings, DNS servers, and NTP synchronization. These foundational elements ensure proper device identification and time synchronization critical for logging, certificate validation, and policy enforcement. Administrator accounts must be established with appropriate access levels, while timezone and locale settings provide accurate event correlation.

Management and Auxiliary Interfaces

Network connectivity configuration focuses on the management interface setup, including IP addressing, subnet configuration, and default gateway assignment. The management interface serves as the primary channel for Strata Cloud Manager communication. Auxiliary interfaces may be configured for out-of-band management or dedicated services. Proper VLAN tagging, interface speeds, and duplex settings ensure reliable connectivity to cloud services.

Local Configuration Management

While Strata Cloud Manager provides centralized policy distribution, local configuration elements remain device-specific. This includes emergency administrative access, local user authentication fallback, and critical network settings that must persist independently of cloud connectivity. Bootstrap configurations and device certificates facilitate initial cloud registration, while local backup configurations ensure operational continuity during network disruptions or maintenance windows.

Configure the Firewall General Settings

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager)	One of these licenses: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

After you successfully onboard your firewall to cloud management, you have the option to configure and specify the general firewall management settings. Configuring the general settings for a firewall isn't required but is recommended. You can configure some or all of the firewall general settings as needed.

STEP 1 | Log in to cloud management.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** > **Management Configuration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** > **Management**and select the Configuration Scope where you want to configure the general settings.

You can select a folder or firewall from your **Folders** or select **Snippets** to configure the general settings in a snippet.

STEP 3 | Click the cog wheel to edit the General Settings and **Customize**.

*If you modified the General Settings for a nested folder or individual device, you can **Revert to Inherited** to revert the General Settings configuration from the `Customized` configuration to that inherited from the parent folder of the nester folder or that inherited from the folder the firewall is associated with.*

STEP 4 | Enter the network **Domain** domain name for the firewall (up to 31 characters).

STEP 5 | Enter text to display in the **Login Banner** on the firewall web interface login page (up to 3,200 characters).

(Optional) Check (enable) **Force Admins to Acknowledge Login Banner** to force administrators to select **I Accept and Acknowledge the Statement Below** when logging in to the firewall web interface. This forces local firewall admins to acknowledge the login banner before they can log into the firewall web interface.

STEP 6 | Select or create a **SSL/TSL Service Profile** to specify a certificate and the SSL/TSL protocol settings allowed on the management interface.

The firewall uses this certificate to authenticate to administrators who access the web interface through the management (MGT) interface or through any other interface that supports HTTP/HTTPS management traffic. If you select **None**, the firewall uses a predefined certificate.

STEP 7 | Select the **Time Zone** where the firewall is located.

STEP 8 | Select the **Locale** where the firewall is located to specify the language for PDF reports generated locally on the firewall.

STEP 9 | Enter the **Latitude** (-90.0 to 90.0) and **Longitude** (-180.0 to 180.0) of the firewall.

STEP 10 | Check (enable) **Automatically Acquire Commit Lock** to automatically apply a commit lock when you change the candidate configuration.

Enable this setting so that other administrators can't make configuration changes until the first administrator commits their changes.

STEP 11 | Check (enable) **Certificate Expiration Check** to instruct the firewall to create a warning message when on-device certificates approach their expiration date.

STEP 12 | (VM-Series firewall only) Check (enable) **Use Hypervisor Assigned MAC Addresses** to have the VM-Series firewall use the MAC address that the hypervisor assigned, instead of generating a MAC address using the PAN-OS custom schema.

STEP 13 | Check (enable) **Tunnel Acceleration** to improve performance and throughput for traffic going through GRE tunnels, VXLAN tunnels, and GTP-U tunnels. This option is enabled by default.

If you disable or reenable Tunnel Acceleration and commit, you must reboot the firewall.

STEP 14 | Save.

STEP 15 | Push Config to push your configuration changes.

Configure the Management Interface Settings

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager)	One of these licenses: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

Configure the management interfaces settings to establish the connection settings, allowed services, and administrative access settings permitted over the management interface.

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** > **ManagementConfiguration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** > **Management** and select the Configuration Scope where you want to configure the management interface settings.

You can select a folder or firewall from your **Folders** or select **Snippets** to configure the management interface settings in a snippet.

STEP 3 | Click the cog wheel to edit the Management Interface Settings and **Customize**.

STEP 4 | Configure the management interface settings.

1. Set the **Speed** to **auto-negotiate**.
2. Specify the **MTU** in bytes for packets sent on this interface.
3. Configure the address settings for the MGT interface using one of the following methods:

   - To configure static IP address settings for the MGT interface, set the **IP Type** to **Static** and enter the **IP Address**, **Netmask**, and **Default Gateway**.
   - To dynamically configure the MGT interface address settings, set the **IP Type** to **DHCP Client**.

   To prevent unauthorized access to the management interface, it is a an administrative best practice to ***Add*** *the* ***Permitted IP Addresses*** *from which an administrator can access the MGT interface.*

4. Select which Administrative Management Services that you want to enable on the interface in order to access the firewall web interface and CLI.

   HTTP and **HTTPS** are the supported protocols to access the firewall web interface.

   Telnet and **SSH** are supported protocols to access the firewall CLI.

   Palo Alto Networks recommends enabling ***HTTPS*** *and* ***SSH*** *for management traffic on the interface rather than* ***HTTP*** *and* ***Telnet****. HTTP and Telnet both use plaintext, which isn't as secure as HTTPS and SSH.*

5. Select the Network Services that you want to enable on the interface.

   - **HTTP OCSP**—Configure the firewall as an Online Certificate Status Protocol (OCSP) responder.
   - **Ping**—Test connectivity with external services. For example, you can ping the interface to verify it can receive PAN-OS software and content updates from the Palo Alto Networks Update Server.

     In a high availability (HA) deployment, HA peers use ping to exchange heartbeat backup information.
   - **SNMP**—Process firewall statistics queries from an SNMP manager.
   - **User-ID**—Enable data redistribution of user mappings among firewalls.
   - **User-ID Syslog Listener-SSL**—Enable the PAN-OS integrated User-ID™ agent to collect syslog messages over SSL.
   - **User-ID Syslog Listener-UDP**—Enable the PAN-OS integrated User-ID agent to collect syslog messages over UDP.

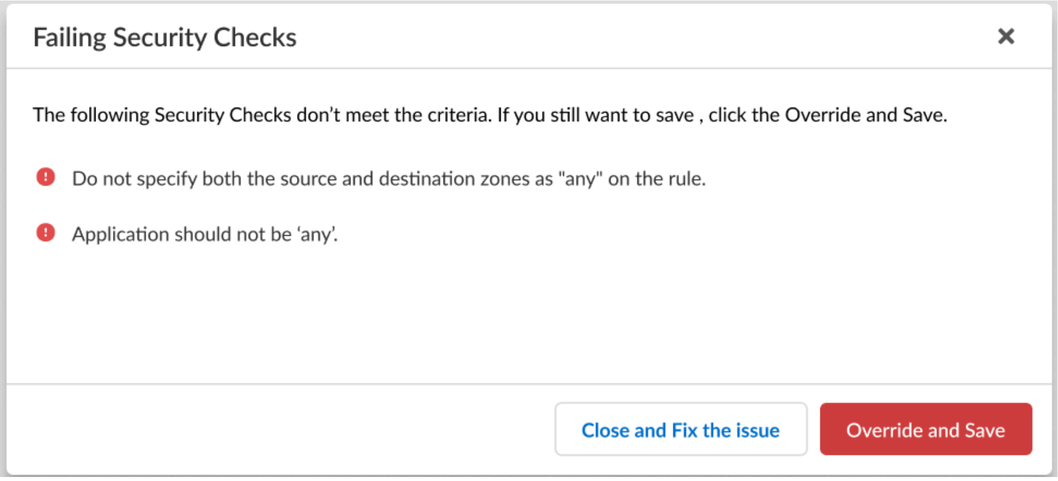
6. Add Permitted IP Addresses from which administrators can access the firewall through the interface.

   The list is empty by default. An empty Permitted IP Address list specifies that access is available from an IP address.

   To prevent unauthorized access, Palo Alto Networks recommends specifying IP addresses that are allowed to access the firewall through the management interface rather than leaving the Permitted IP Addresses empty.

STEP 5 | **Save**.

If the configuration you're trying to save doesn't meet the criteria to pass the compliance check, you'll have the option to remediate the issue or override the warning and save the configuration anyway.



Failing Security Checks

The following Security Checks don't meet the criteria. If you still want to save , click the Override and Save.

- Do not specify both the source and destination zones as "any" on the rule.
- Application should not be 'any'.

STEP 6 | **Push Config** to push your configuration changes.

Configure the Auxiliary Interface Settings

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager)	One of these licenses: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

PA-5200 Series firewalls include two multipurpose auxiliary (Aux1 and Aux2) SFP+ ports that can be configured for high availability (HA) and management functions. You can configure the auxiliary interfaces settings to establish the connection settings, allowed services, and administrative access settings permitted over the Aux1 and Aux2 interfaces.

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** > **ManagementConfiguration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** > **Management** and select the Configuration Scope where you want to configure the auxiliary interface settings.

You can select a folder or firewall from your **Folders** or select **Snippets** to configure the auxiliary interface settings in a snippet.

STEP 3 | Click the cog wheel to edit the Aux Interface Settings and **Customize**.

STEP 4 | Configure the auxiliary interface settings.

1. **Enable Interface**.
2. Assign an IPv4 or IPv6 **IP Address** to the interface.
3. Enter the **Netmask**.
4. Enter the **Default Gateway** IP address.

   The gateway must be on the same subnet as the interface IP address.
5. Enter the **MTU** (maximum transmission unit) in bytes for packets sent on this interface.

   Range is **`576`** to **`1,500`**. Default is `1,500`.
6. Select which Administrative Management Services that you want to enable on the interface in order to access the firewall web interface and CLI.

   HTTP and **HTTPS** are the supported protocols to access the firewall web interface.

   Telnet and **SSH** are supported protocols to access the firewall CLI.

   *Palo Alto Networks recommends enabling **HTTPS** and **SSH** for management traffic on the interface rather than **HTTP** and **Telnet**. HTTP and Telnet both use plaintext, which isn't as secure as HTTPS and SSH.*
7. Select the Network Services that you want to enable on the interface.
   - **HTTP OCSP**—Configure the firewall as an Online Certificate Status Protocol (OCSP) responder.
   - **Ping**—Test connectivity with external services. For example, you can ping the interface to verify it can receive PAN-OS software and content updates from the Palo Alto Networks Update Server.

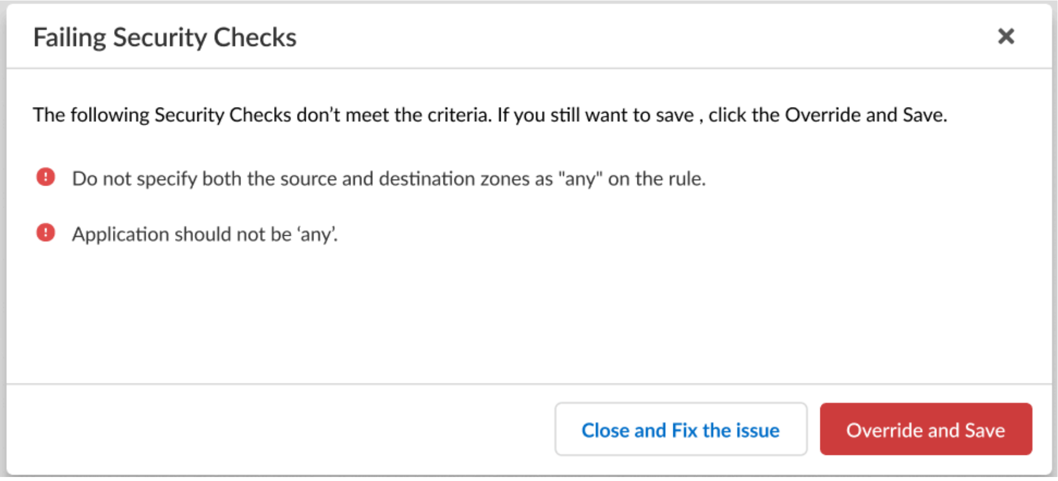
     In a high availability (HA) deployment, HA peers use ping to exchange heartbeat backup information.
   - **SNMP**—Process firewall statistics queries from an SNMP manager.
   - **User-ID**—Enable data redistribution of user mappings among firewalls.
   - **User-ID Syslog Listener-SSL**—Enable the PAN-OS integrated User-ID™ agent to collect syslog messages over SSL.
   - **User-ID Syslog Listener-UDP**—Enable the PAN-OS integrated User-ID agent to collect syslog messages over UDP.
8. Add Permitted IP Addresses from which administrators can access the firewall through the interface.

   The list is empty by default. An empty Permitted IP Address list specifies that access is available from an IP address.

   To prevent unauthorized access, Palo Alto Networks recommends specifying IP addresses that are allowed to access the firewall through the auxiliary interface rather than leaving the Permitted IP Addresses empty.

STEP 5 | **Save**.

If the configuration you're trying to save doesn't meet the criteria to pass the compliance check, you'll have the option to remediate the issue or override the warning and save the configuration anyway.



Failing Security Checks

The following Security Checks don't meet the criteria. If you still want to save , click the Override and Save.

- Do not specify both the source and destination zones as "any" on the rule.
- Application should not be 'any'.

STEP 6 | **Push Config** to push your configuration changes.

Manage a Local Firewall Configuration

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager)	One of these licenses: □ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

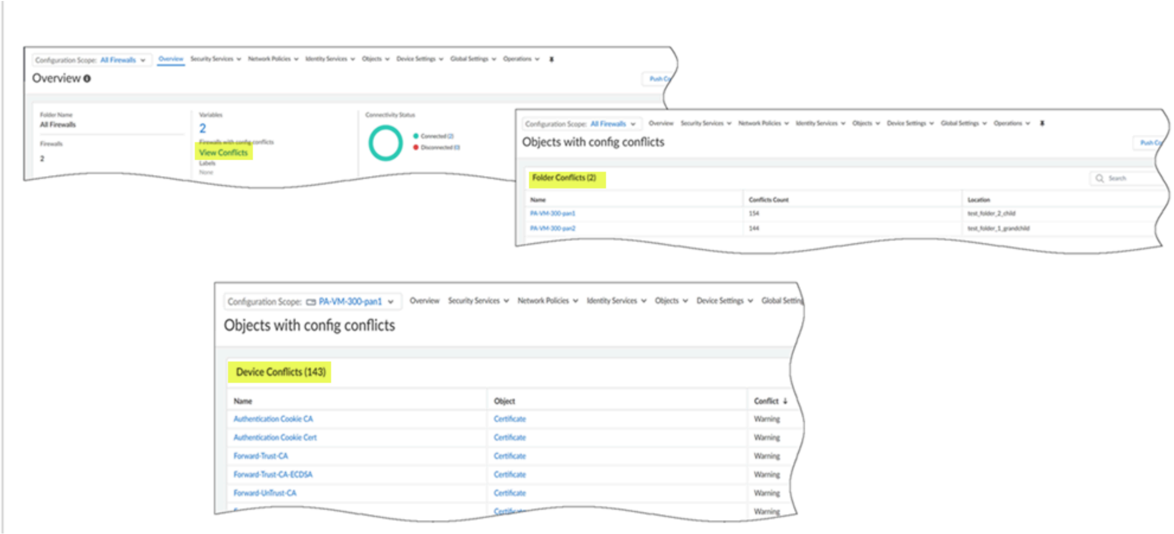
The local configuration management feature eliminates the need for context switching from central management to individual firewalls for managing local configurations. This feature enhances readability, simplifies troubleshooting, and reduces manual effort by providing visibility and control over local firewall configurations through Strata Cloud Manager. Additionally, it identifies any conflicting or overridden objects between local and pushed configurations, making it easier to troubleshoot.

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **OverviewConfiguration** > **NGFW and Prisma Access** > **Overview** and select the configuration Scope.

STEP 3 | Select a folder or specific firewall from your **Folders** to view any conflicting configurations.

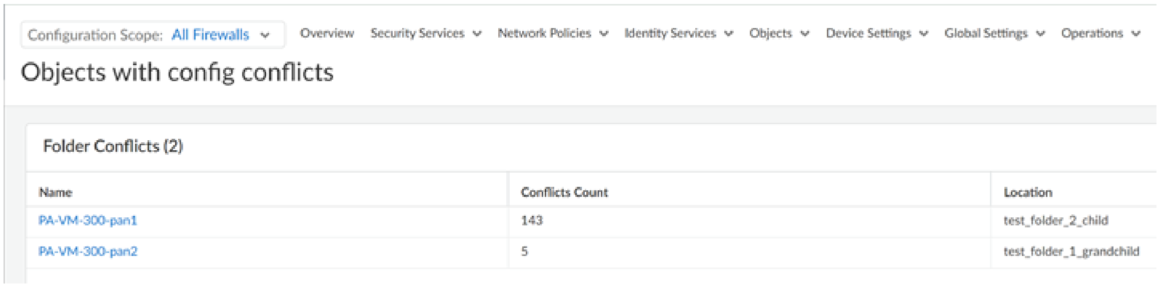
- **Firewalls with config conflicts** shows the number of firewalls with conflicts. **View Conflicts** to see conflicts for all firewalls and their respective locations. Click the individual firewall to further investigate device-level conflicts.



Name	Conflicts Count	Location
PA-VM-300-pan1	154	test_folder_2_child
PA-VM-300-pan2	144	test_folder_1_grandchild

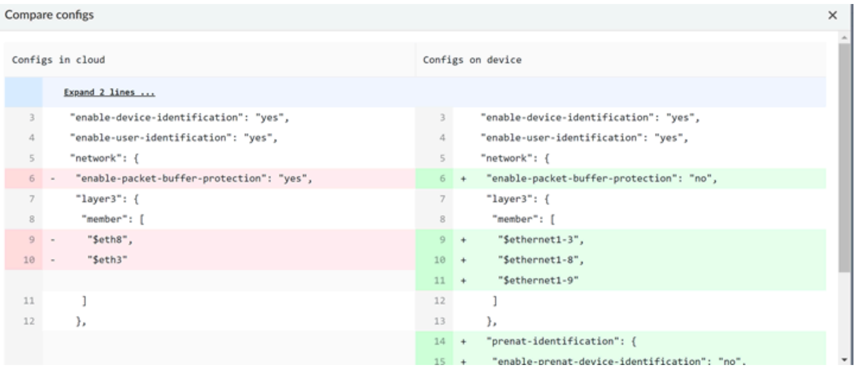
Name	Object	Conflict ↓
Authentication Cookie CA	Certificate	Warning
Authentication Cookie Cert	Certificate	Warning
Forward-Trust-CA	Certificate	Warning
Forward-Trust-CA-ECDSA	Certificate	Warning
Forward-UnTrust-CA	Certificate	Warning

- **Objects with config conflicts** shows the number of conflicts per firewall. Click the number to view the conflicted objects and their corresponding types specific to that firewall. Click the object to get the granular details on the conflict.



Name	Conflicts Count	Location
PA-VM-300-pan1	143	test_folder_2_child
PA-VM-300-pan2	5	test_folder_1_grandchild

- Select objects such as zones and interfaces to view any conflicts with the local device configuration.
- Use the **Show Config Diff** option to compare configurations between the Strata Cloud Manager and the firewall.



Configs in cloud

```
  "enable-device-identification": "yes",
  "enable-user-identification": "yes",
  "network": {
-  "enable-packet-buffer-protection": "yes",
   "layer3": {
    "member": [
-     "$eth8",
-     "$eth3"
    ]
   },
```

Configs on device

```
  "enable-device-identification": "yes",
  "enable-user-identification": "yes",
  "network": {
+  "enable-packet-buffer-protection": "no",
   "layer3": {
    "member": [
+     "$ethernet1-3",
+     "$ethernet1-8",
+     "$ethernet1-9"
    ]
   },
+  "prenat-identification": {
+   "enable-prenat-device-identification": "no",
```

Manage Your NGFWs

Where Can I Use This?	What Do I Need?
• NGFW	

Effective resource management on NGFWs encompasses the entire lifecycle of the security appliance, from initial registration through operational monitoring to eventual decommissioning. The resource management process begins during implementation, where administrators must register NGFWs with Palo Alto Networks to activate subscriptions, enable updates, and access support services. This registration associates the NGFW's serial number with a customer account, enabling features like threat intelligence updates and software upgrades while establishing the device's identity within the support ecosystem.

During operational use, monitoring hardware resource consumption becomes essential for maintaining security efficacy and performance. Administrators should regularly assess CPU utilization, memory usage, session table capacity, and disk storage—particularly for logging and reporting functions. Each hardware model has specific capacity limitations, and exceeding these thresholds can trigger resource exhaustion, potentially causing packet drops, increased latency, or security bypass. Implementing appropriate alerting thresholds for resource metrics provides early warning of developing issues, while capacity planning helps ensure appropriate hardware sizing as network traffic patterns and security requirements evolve.

The resource lifecycle concludes with proper decommissioning procedures when NGFWs reach end-of-life or require replacement. Decommissioning involves several critical steps: backing up configurations, securely erasing sensitive data through factory reset functions, unregistering the device from support systems, and revoking any certificates or credentials associated with the NGFW. For organizations with centralized management through Panorama or Strata Cloud Manager, this process also includes removing the device from the management console and ensuring that any shared policies or objects are properly migrated to replacement systems. Proper decommissioning not only protects sensitive configuration data but also ensures accurate license management and inventory tracking across the security infrastructure.

Register Your NGFW

Where Can I Use This?	What Do I Need?
• NGFW	

Before you can activate support and other licenses and subscriptions, you must first register the NGFW. Before you can register a NGFW, though, you must first have an active support account. Perform one of the following tasks depending on whether you have an active support account:

- If you don't have an active support account, then .
- If you already have an active support account, then you are ready to .
- on a registered NGFW.
- If your NGFW uses line cards such as an NPC (Network Processing Card), then .

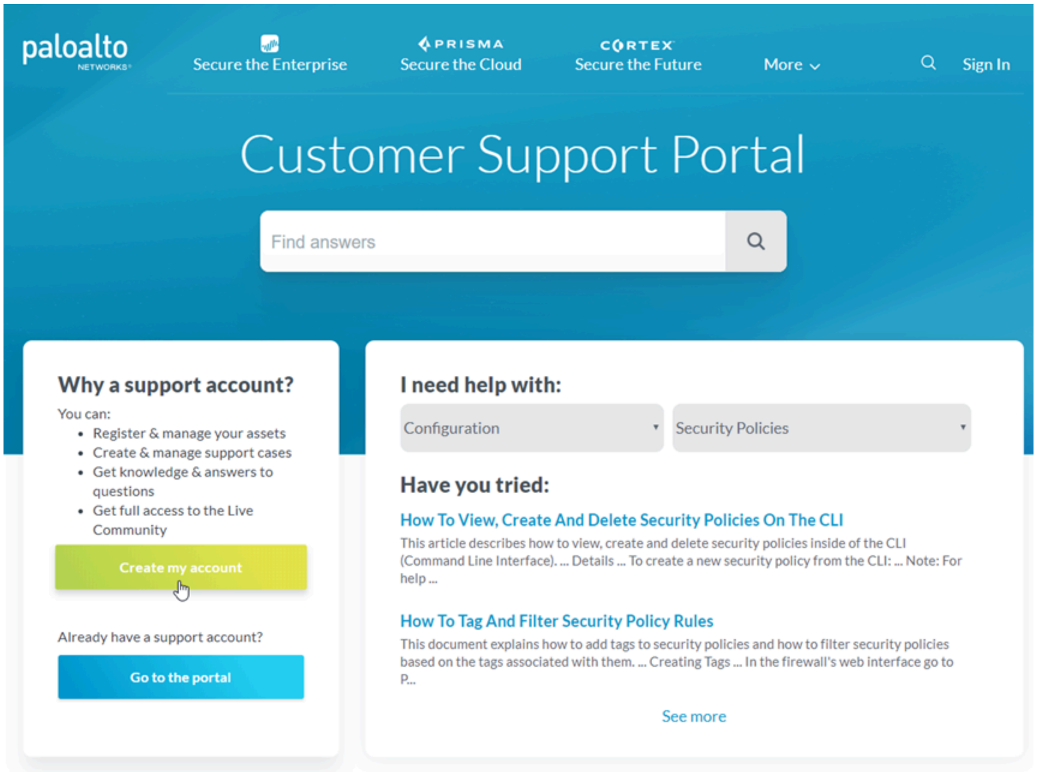
If you are registering a VM-Series NGFW, *refer to the* VM-Series Deployment Guide *for instructions.*

Create a New Support Account and Register an NGFW

If you do not already have an active Palo Alto Networks support account, then you need to register your NGFW when you create your new support account.

STEP 1 | Go to the Palo Alto Networks Customer Support Portal.

STEP 2 | Click **Create my account**.



Customer Support Portal

Why a support account?

You can:

- Register & manage your assets
- Create & manage support cases
- Get knowledge & answers to questions
- Get full access to the Live Community

Already have a support account?

I need help with:

Have you tried:

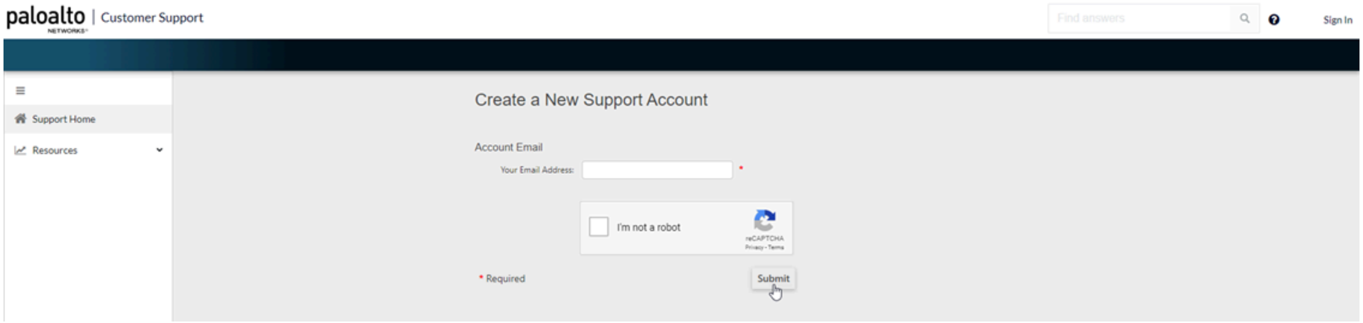
How To View, Create And Delete Security Policies On The CLI

This article describes how to view, create and delete security policies inside of the CLI (Command Line Interface). ... Details ... To create a new security policy from the CLI: ... Note: For help ...

How To Tag And Filter Security Policy Rules

This document explains how to add tags to security policies and how to filter security policies based on the tags associated with them. ... Creating Tags ... In the firewall's web interface go to P...

STEP 3 | Enter **Your Email Address**, check **I'm not a robot**, and click **Submit**.



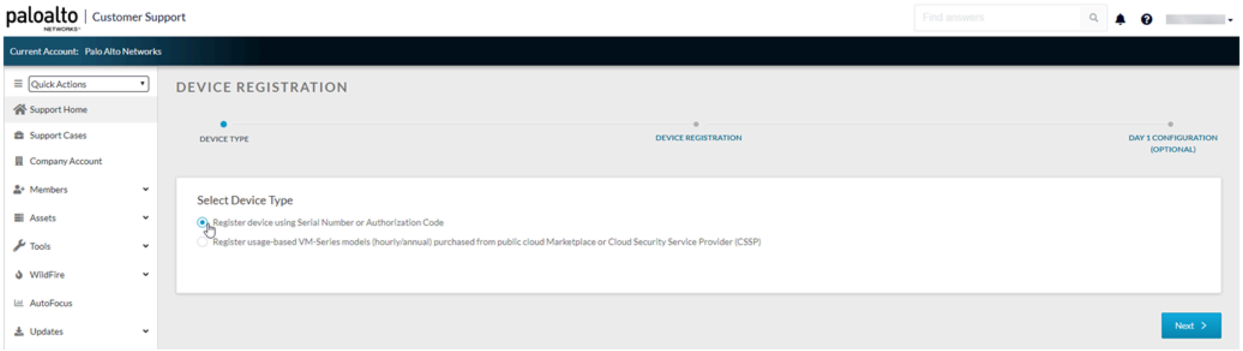
Create a New Support Account

Account Email

Your Email Address: *

* Required

STEP 4 | Select **Register device using Serial Number or Authorization Code** and click **Next**.



DEVICE REGISTRATION

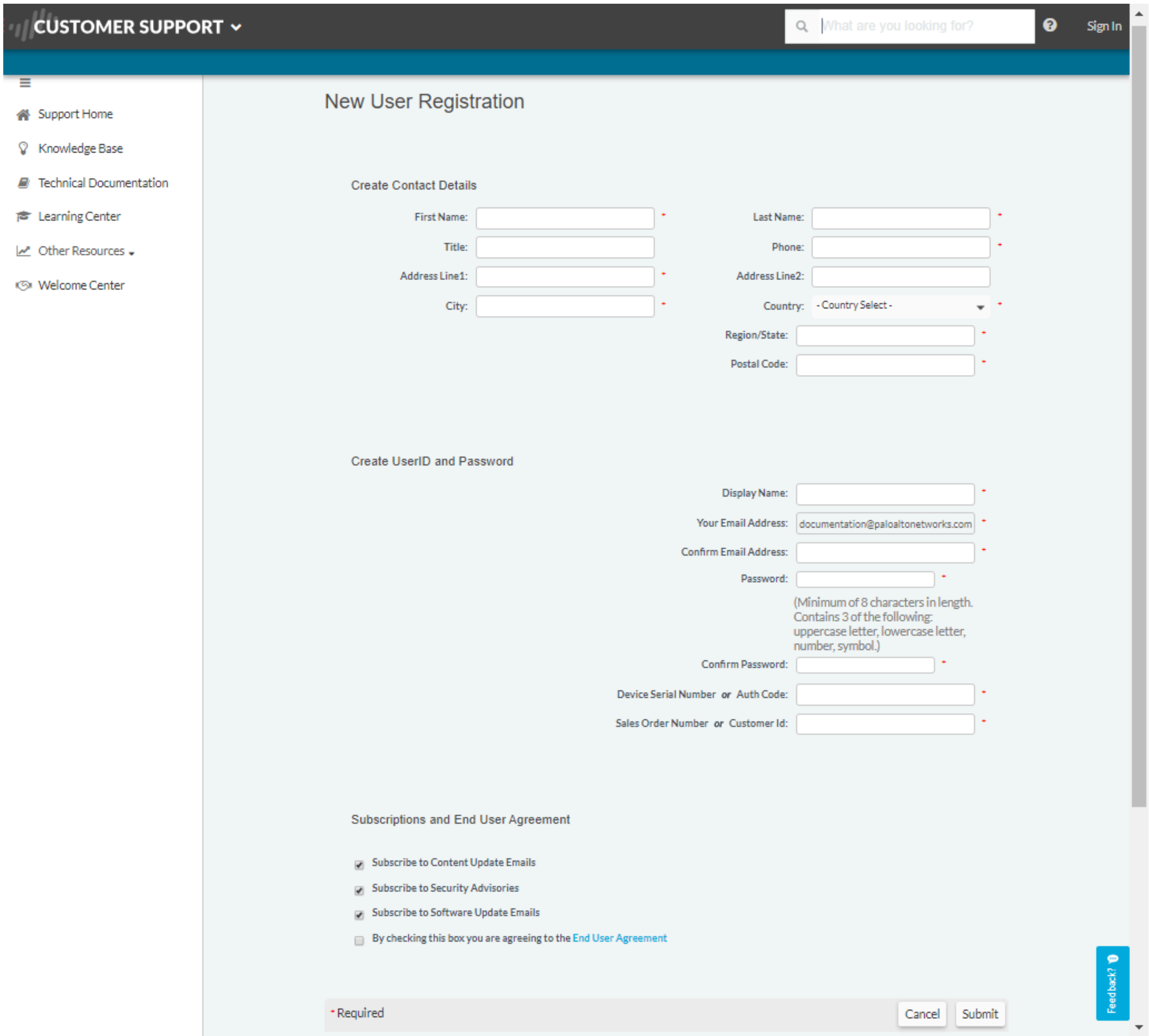
Select Device Type

● Register device using Serial Number or Authorization Code

○ Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)

STEP 5 | Complete the registration form.

1. Enter your contact details. Required fields are indicated by red asterisks.
2. Create a UserID and Password for the account. Required fields are indicated by red asterisks.
3. Enter the **Device Serial Number** or **Auth Code**.
4. Enter your **Sales Order Number** or **Customer Id**.
5. To ensure that you are always alerted to the latest updates and security advisories, **Subscribe to Content Update Emails**, **Subscribe to Security Advisories**, and **Subscribe to Software Update Emails**.
6. Select the check box to agree to the End User Agreement and **Submit**.



New User Registration

Create Contact Details

First Name: *
Last Name: *
Title:
Phone: *
Address Line1: *
Address Line2:
City: *
Country: - Country Select - *
Region/State: *
Postal Code: *

Create UserID and Password

Display Name: *
Your Email Address: documentation@paloaltonetworks.com *
Confirm Email Address: *
Password: *
(Minimum of 8 characters in length. Contains 3 of the following: uppercase letter, lowercase letter, number, symbol.)
Confirm Password: *
Device Serial Number or Auth Code: *
Sales Order Number or Customer Id: *

Subscriptions and End User Agreement

☑ Subscribe to Content Update Emails
☑ Subscribe to Security Advisories
☑ Subscribe to Software Update Emails
☐ By checking this box you are agreeing to the End User Agreement

* Required

Cancel Submit

Register an NGFW

If you already have an active Palo Alto Networks Customer Support account, perform the following task to register your NGFW.

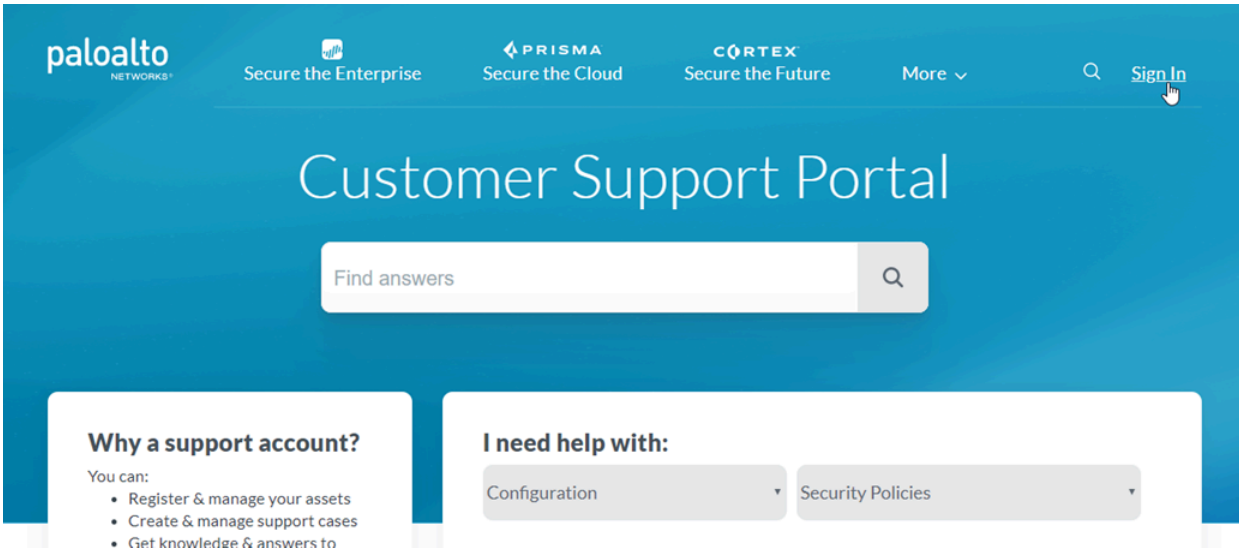
STEP 1 | Log in to the NGFW web interface.

Using a secure connection (HTTPS) from your web browser, log in using the new IP address and password you assigned during initial configuration (https://<IP address>).

STEP 2 | Locate your serial number and copy it to the clipboard.

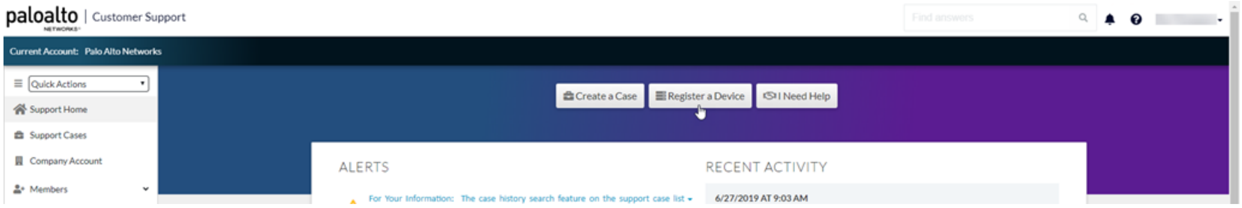
On the **Dashboard**, locate your **Serial Number** in the General Information section of the screen.

STEP 3 | Go to the Palo Alto Networks Customer Support Portal and, if not already logged in, **Sign In** now.

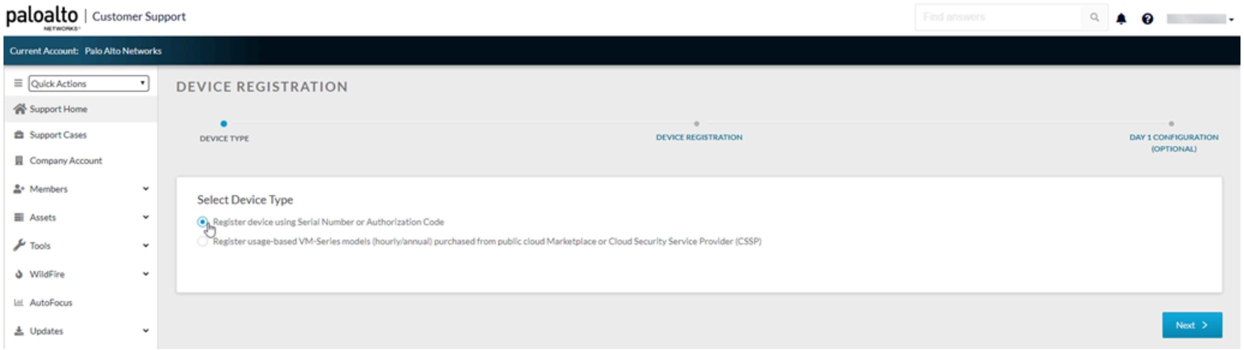


STEP 4 | Register the NGFW.

1. On the Support Home page, click **Register a Device**.



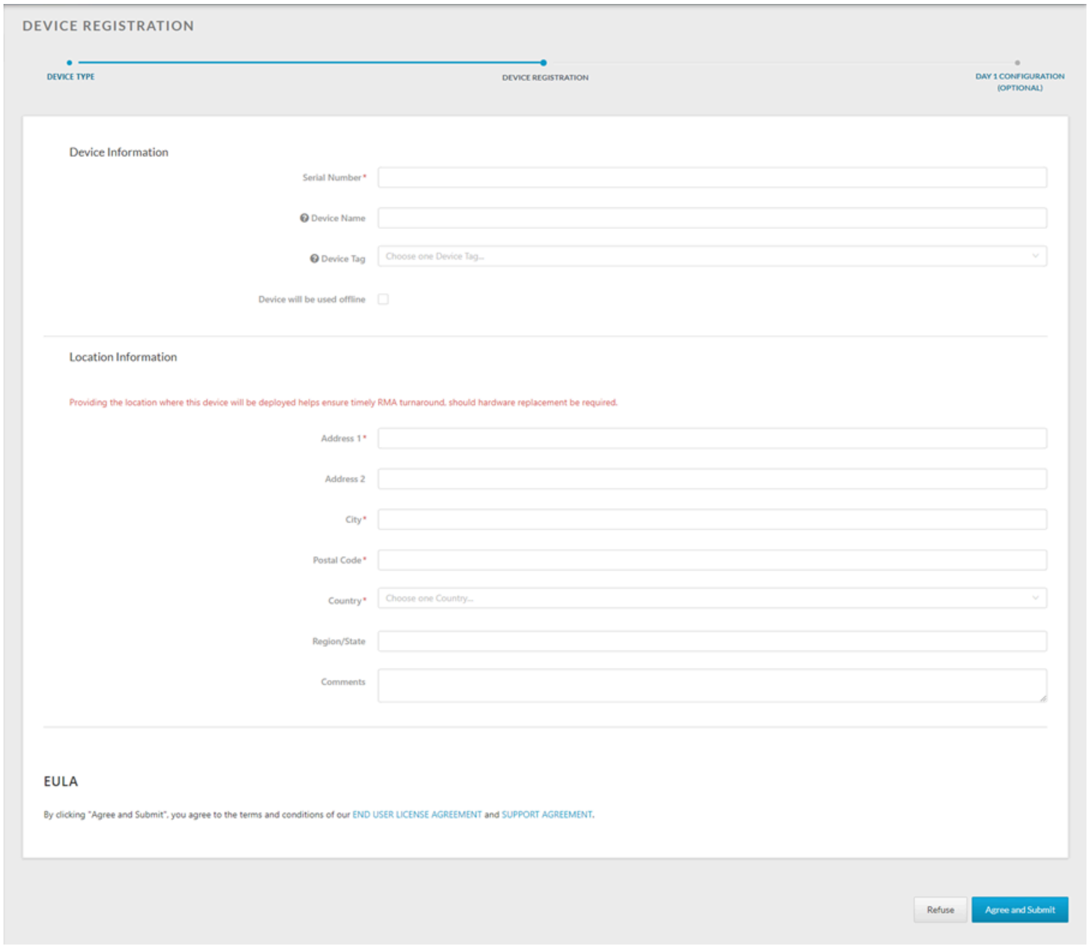
2. Select **Register device using Serial Number or Authorization Code**, and then click **Next**.


paloalto NETWORKS | Customer Support
Find answers
Current Account: Palo Alto Networks
Quick Actions
Support Home
Support Cases
Company Account
Members
Assets
Tools
WildFire
AutoFocus
Updates
DEVICE REGISTRATION
DEVICE TYPE
DEVICE REGISTRATION
DAY 1 CONFIGURATION (OPTIONAL)
Select Device Type
Register device using Serial Number or Authorization Code
Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)
Next >

3. Enter the NGFW **Serial Number** (you can copy and paste it from the NGFW Dashboard).
4. (Optional) Enter the **Device Name** and **Device Tag**.
5. (Optional) If the device will not have a connection to the internet, select the **Device will be used offline** check box and then, from the drop-down, select the **OS Release** you plan to use.
6. Provide information about the physical location where you plan to deploy the NGFW including the **Address**, **City**, **Postal Code**, and **Country**.

   The physical location of the NGFW is set on the Customer Support Portal. There is no command on the NGFW to set the physical location.

7. Read the End User License Agreement (EULA) and the Support Agreement, then **Agree and Submit**.



DEVICE REGISTRATION

Device Information

Serial Number*

Device Name

Device Tag: Choose one Device Tag...

Device will be used offline □

Location Information

Providing the location where this device will be deployed helps ensure timely RMA turnaround, should hardware replacement be required.

Address 1*

Address 2

City*

Postal Code*

Country*: Choose one Country...

Region/State

Comments

EULA

By clicking "Agree and Submit", you agree to the terms and conditions of our END USER LICENSE AGREEMENT and SUPPORT AGREEMENT.

You can search for and manage the NGFW you just registered from the **Network Security** page.

STEP 5 | (Firewalls with line cards) To ensure that you receive support for your NGFW's line cards, make sure to register the NGFW line cards.

(Optional) Perform Day 1 Configuration

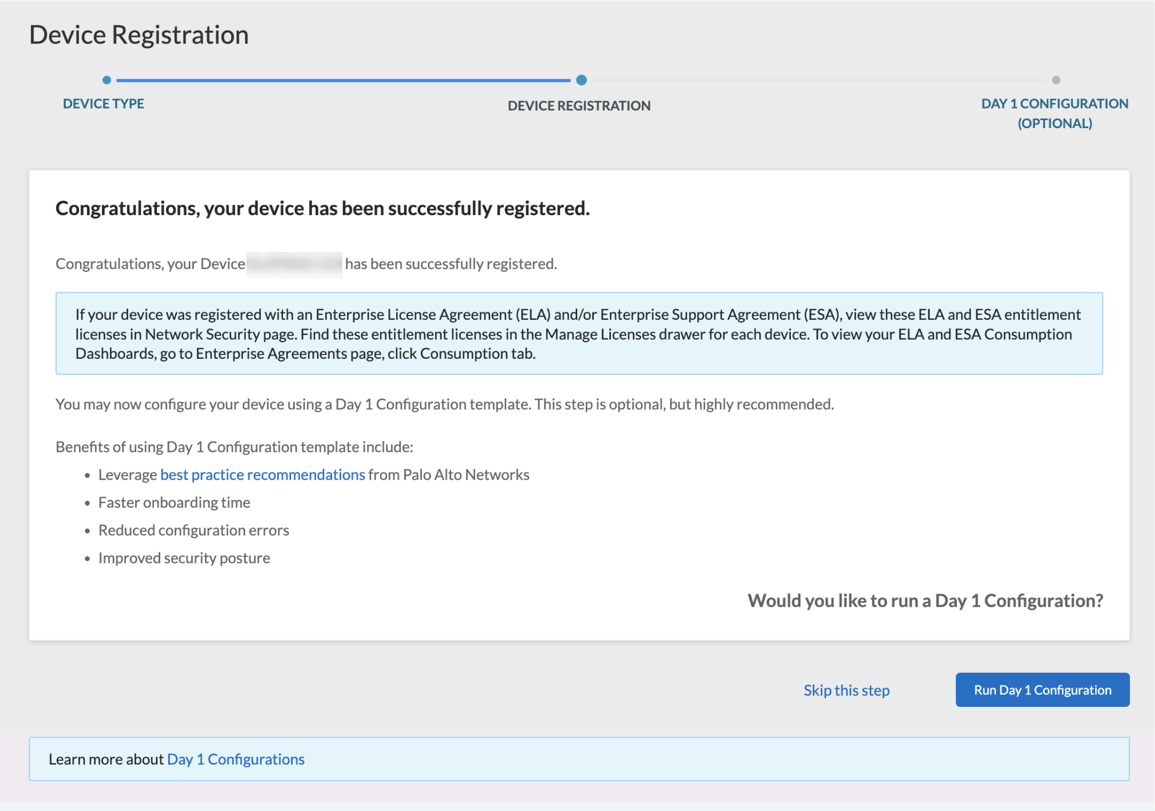
After you register your NGFW, you have the option of running Day 1 Configuration. The Day 1 Configuration tool provides configuration templates informed by Palo Alto Networks best practices, which you can use as a starting point to build the rest of your configuration.

The benefits of Day 1 Configuration templates include:

- Faster implementation time
- Reduced configuration errors
- Improved security posture

Perform Day 1 Configuration by following these steps:

STEP 1 | From the page that displays after you have registered your NGFW, select **Run Day 1 Configuration**.



Congratulations, your device has been successfully registered.

Congratulations, your Device [redacted] has been successfully registered.

If your device was registered with an Enterprise License Agreement (ELA) and/or Enterprise Support Agreement (ESA), view these ELA and ESA entitlement licenses in Network Security page. Find these entitlement licenses in the Manage Licenses drawer for each device. To view your ELA and ESA Consumption Dashboards, go to Enterprise Agreements page, click Consumption tab.

You may now configure your device using a Day 1 Configuration template. This step is optional, but highly recommended.

Benefits of using Day 1 Configuration template include:

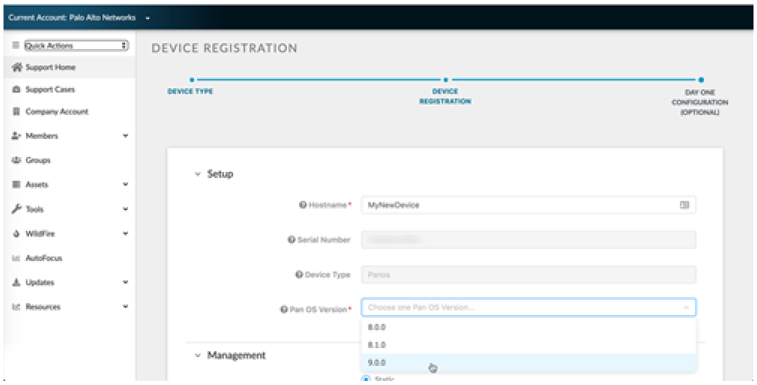
- Leverage best practice recommendations from Palo Alto Networks
- Faster onboarding time
- Reduced configuration errors
- Improved security posture

Would you like to run a Day 1 Configuration?

Learn more about Day 1 Configurations

If you've already registered your NGFW but haven't run Day 1 Configuration, you can also run it from the Customer Support Portal home page by selecting ***Tools*** *>* ***Run Day 1 Configuration.***

STEP 2 | Enter the **Hostname** and **Pan OS Version** for your new device, and optionally, the **Serial Number** and **Device Type**.



Hostname* MyNewDevice

Serial Number [redacted]

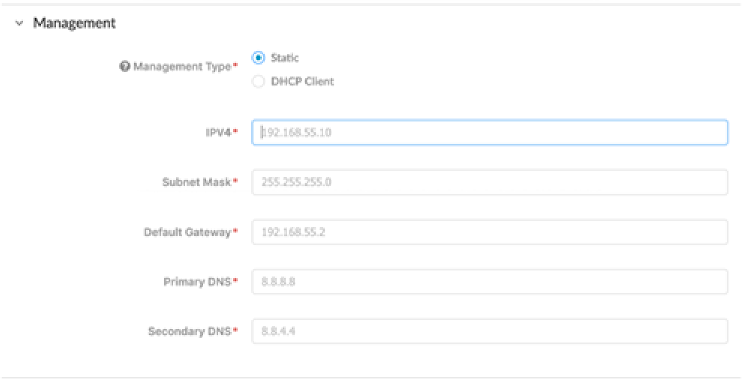
Device Type Panos

Pan OS Version* Choose one Pan OS Version...

8.0.0
8.1.0
9.0.0

STEP 3 | Under **Management**, select either **Static** or **DHCP Client** for your **Management Type**.

Selecting **Static** will require you fill out the **IPV4**, **Subnet Mask**, and **Default Gateway** fields.



Management

Management Type* ● Static ○ DHCP Client

IPV4* 192.168.55.10

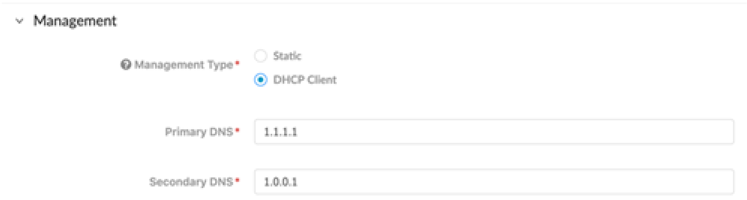
Subnet Mask* 255.255.255.0

Default Gateway* 192.168.55.2

Primary DNS* 8.8.8.8

Secondary DNS* 8.8.4.4

Selecting **DHCP Client** only requires that you enter the **Primary DNS** and **Secondary DNS**. A device configured in DHCP client mode will ensure the management interface receives an IP address from the local DHCP server, or it will fill out all the parameters if they are known.



Management

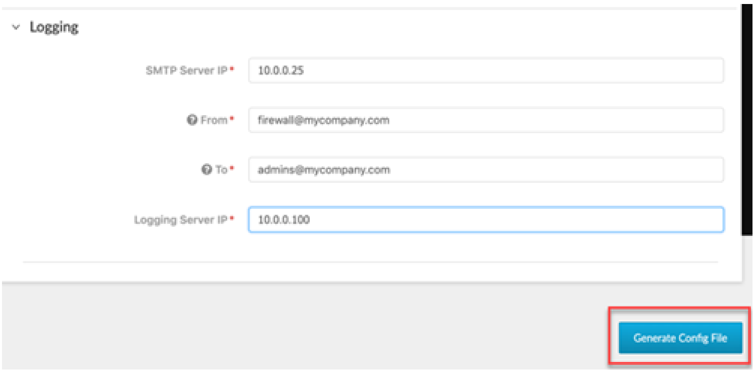
Management Type* ○ Static ● DHCP Client

Primary DNS* 1.1.1.1

Secondary DNS* 1.0.0.1

STEP 4 | Fill out all fields under **Logging**.

STEP 5 | Click **Generate Config File**.



Logging

SMTP Server IP* 10.0.0.25

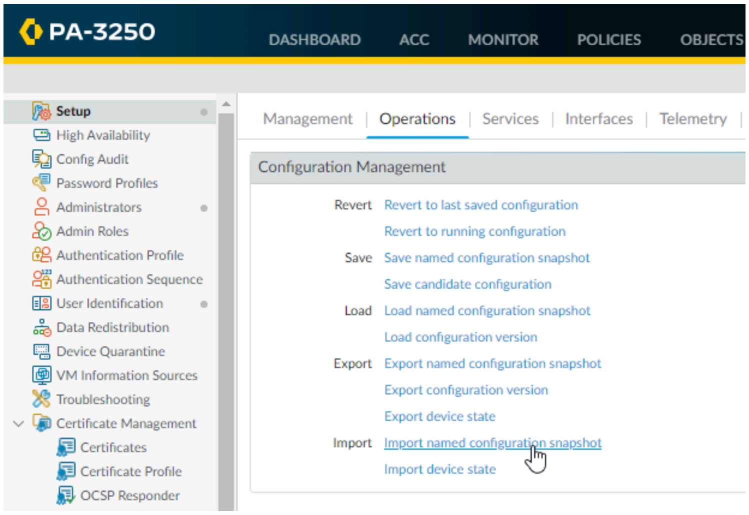
From* firewall@mycompany.com

To* admins@mycompany.com

Logging Server IP* 10.0.0.100

STEP 6 | To import and load the Day 1 Configuration file you just downloaded to your NGFW:

1. Log into your NGFW web interface.
2. Select **Device** > **Setup** > **Operations**.
3. Click **Import named configuration snapshot**.
4. Select the file.



Register the NGFW Line Cards

The following NGFWs use line cards that must be registered to receive support with troubleshooting and returns:

- PA-7000 Series NGFWs
- PA-5450 NGFW

Return to these instructions after creating your Customer Support account and registering your NGFW.

STEP 1 | Go to the Palo Alto Networks Customer Support Portal and, if not already logged in, **Sign In** now.

STEP 2 | Select **Assets** > **Line Cards/Optics/FRUs**.

STEP 3 | **Register Components**.

STEP 4 | Enter the Palo Alto Networks Sales Order Number of the line cards into the **Sales Order Number** field to display the line cards eligible for registration.

STEP 5 | Register the line cards to your NGFW by entering its chassis serial number in the **Serial Number** field. The **Location Information** below auto-populates based on the registration information of your NGFW.

STEP 6 | Click **Agree and Submit** to accept the legal terms. The system updates to display the registered line cards under **Assets** > **Line Cards/Optics/FRUs**.

Manage Hardware Consumption

Where Can I Use This?	What Do I Need?
• NGFW	

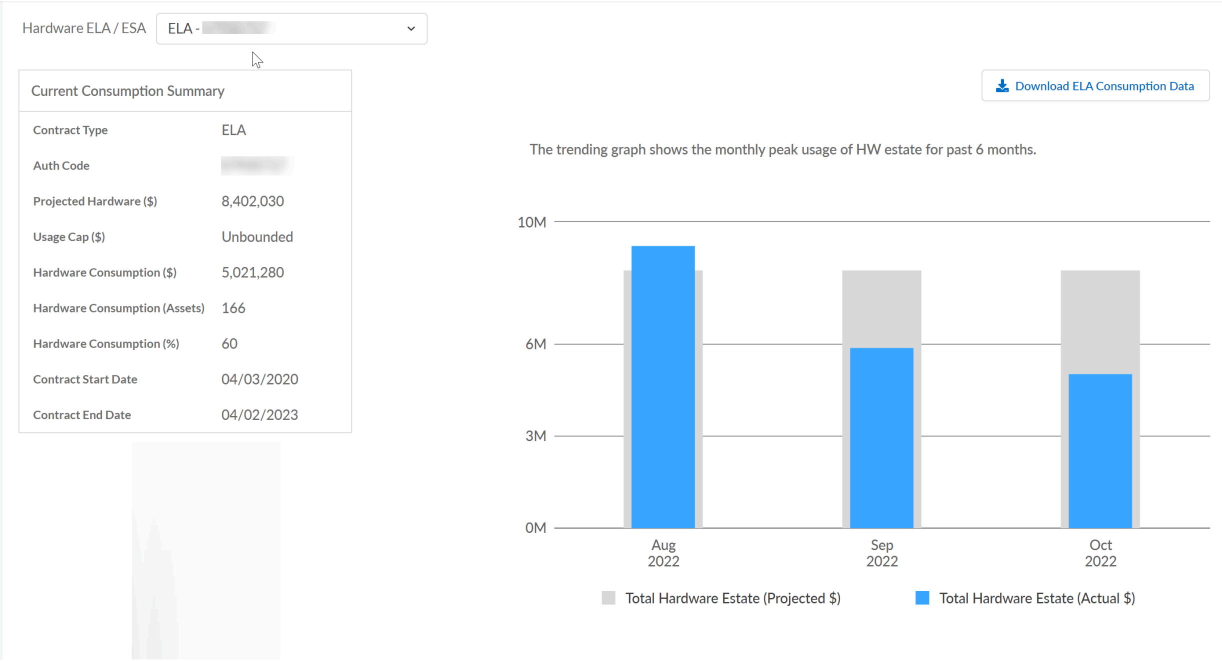
If you have an Enterprise Agreement, you can manage your PA-Series hardware consumption on the Customer Support Portal.

To learn about managing hardware consumption on Strata Cloud Manager managed NGFWs, click here.

STEP 1 | Log in to the Customer Support Portal.

STEP 2 | To view your consumption data, select **Assets** > **Enterprise Agreements** > **Consumption**.

Based on the ELA/ESA, view your consumption summary and associated CSP accounts. Changes to assets for activations and decommissions over the past six months are reflected in the summary and associated usage chart. You can also download a CSV file with the consumption data for the account.



Hardware ELA / ESA ELA - [redacted]

Current Consumption Summary

Contract Type	ELA
Auth Code	[redacted]
Projected Hardware ($)	8,402,030
Usage Cap ($)	Unbounded
Hardware Consumption ($)	5,021,280
Hardware Consumption (Assets)	166
Hardware Consumption (%)	60
Contract Start Date	04/03/2020
Contract End Date	04/02/2023

The trending graph shows the monthly peak usage of HW estate for past 6 months.

Download ELA Consumption Data
10M
6M
3M
0M
Aug 2022
Sep 2022
Oct 2022
Total Hardware Estate (Projected $)
Total Hardware Estate (Actual $)

STEP 3 | To manage the assets, select **Assets** > **Network Security**, then filter to view **NGFW**.

STEP 4 | Manage assets through **Account Actions**.

You can take the following actions:

- **Activate Asset**—Register your new NGFW.
- **Deactivate License**—Deactivate hardware feature licensing or VM feature licensing and support entitlements.
- **Decommissioned Assets**—View a list of assets you've decommissioned for your Enterprise Agreement.
- **Device Tags**—Add new device tags or search for existing device tags.
- **Download CSV**—Download a CSV file of all the assets associated with the account.
- **Incoming Transfers**—Accept or Reject asset transfers to the account.

Decommission Your NGFW

Where Can I Use This?	What Do I Need?
• NGFW	

Decommissioning NGFWs is a critical operational process that requires systematic planning and execution to maintain security integrity and proper asset management. When NGFWs reach end-of-life, undergo replacement, or are removed from service, administrators must follow specific procedures to protect sensitive configuration data, ensure secure data destruction, and properly update licensing and inventory systems.

Two primary decommissioning methods and available to accommodate different operational needs: Single Asset decommissioning for individual NGFW removals, which walks administrators through a step-by-step process for safely retiring a specific device; and Bulk Asset decommissioning for large-scale projects, allowing security teams to efficiently process multiple NGFWs simultaneously when performing data center migrations, hardware refresh cycles, or organizational restructuring. Both approaches ensure that sensitive data is securely erased, support entitlements are properly adjusted, and the NGFWs are completely removed from management systems like Panorama or Strata Cloud Manager, maintaining the integrity of the remaining security infrastructure while properly concluding the asset life cycle.

- Single Asset
- Bulk Assets

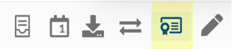
Decommission Your NGFW (Single Asset)

Use the Asset Actions to decommission a single asset.

STEP 1 | Log in to the Customer Support Portal.

STEP 2 | Select **Assets** > **Network Security**, then filter to view **NGFW**.

STEP 3 | Select **Licenses/Subscriptions** in **Actions** for the asset you want to decommission.



Review the asset details in the **Licenses & Subscriptions** panel.

STEP 4 | **Decommission Asset**.

STEP 5 | Select the reason to decommission the asset.

- Lost or stolen
- Customer Request

STEP 6 | **Decommission** the asset.

STEP 7 | **Agree and Submit** to decommission the assets listed.

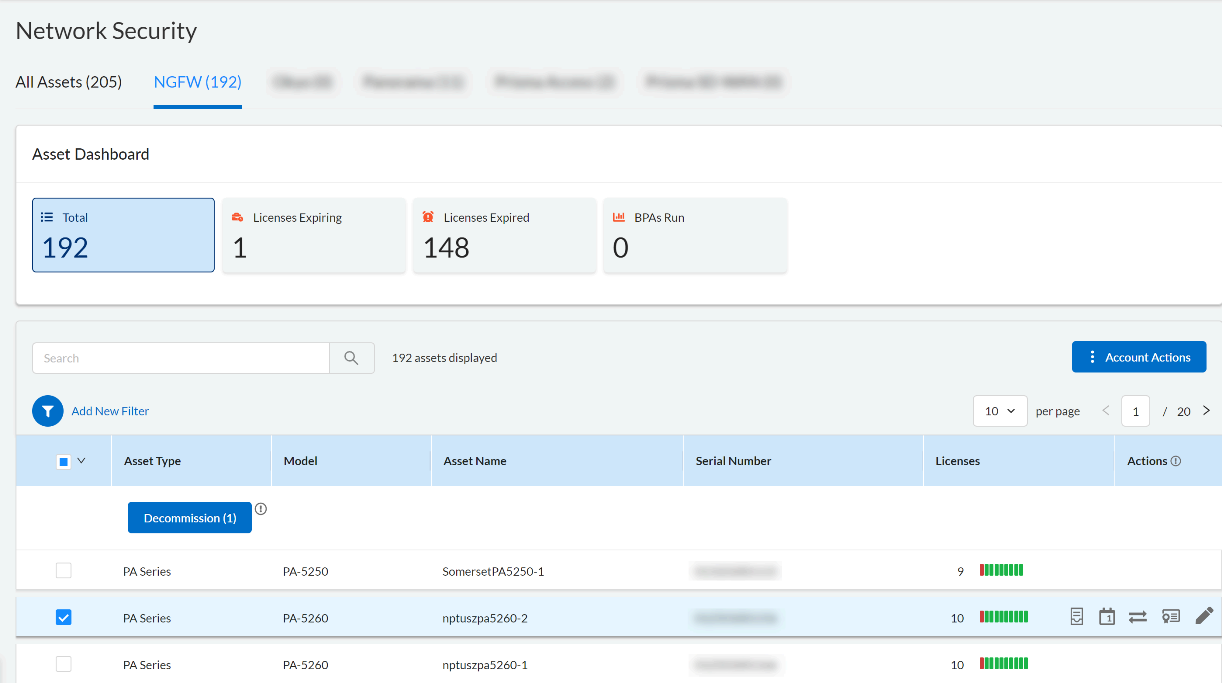
Decommissioning assets is a permanent operation.

STEP 8 | View the decommissioned assets through **Account Actions** > **Decommissioned Assets**.

Decommission Your NGFW (Bulk)

STEP 1 | Log in to the Customer Support Portal.

STEP 2 | Select **Assets** > **Network Security**, then filter to view **NGFW**.



Network Security

All Assets (205) | NGFW (192) | [redacted]

Asset Dashboard

Total	Licenses Expiring	Licenses Expired	BPAs Run
192	1	148	0

Search | 192 assets displayed | Account Actions

Add New Filter | 10 per page | 1 / 20

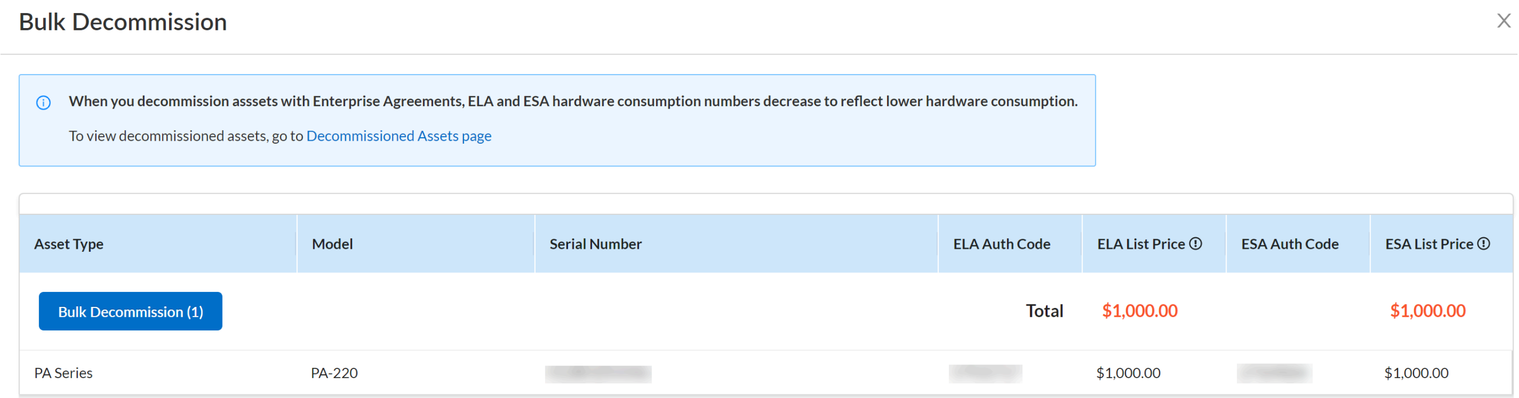
■	Asset Type	Model	Asset Name	Serial Number	Licenses	Actions
	Decommission (1)					
☐	PA Series	PA-5250	SomersetPA5250-1	[redacted]	9	
☑	PA Series	PA-5260	nptuszpa5260-2	[redacted]	10	
☐	PA Series	PA-5260	nptuszpa5260-1	[redacted]	10	

STEP 3 | Select the assets you want to decommission.

STEP 4 | **Decommission** the selected assets.

Review the assets in the Bulk Decommission list.

STEP 5 | **Bulk Decommission** the assets.



Bulk Decommission

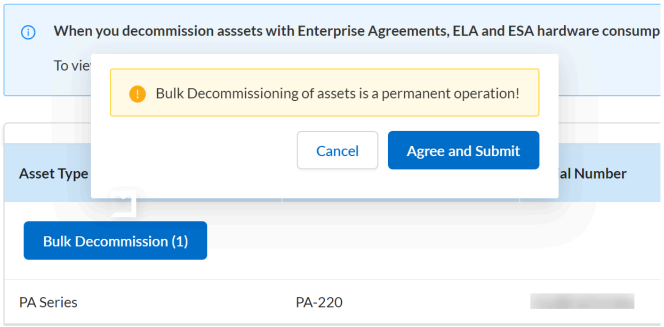
When you decommission assets with Enterprise Agreements, ELA and ESA hardware consumption numbers decrease to reflect lower hardware consumption.

To view decommissioned assets, go to Decommissioned Assets page

Asset Type	Model	Serial Number	ELA Auth Code	ELA List Price ⓘ	ESA Auth Code	ESA List Price ⓘ
Bulk Decommission (1)			Total	$1,000.00		$1,000.00
PA Series	PA-220	[redacted]	[redacted]	$1,000.00	[redacted]	$1,000.00

STEP 6 | **Agree and Submit** to decommission the assets listed.

Decommissioning assets is a permanent operation.

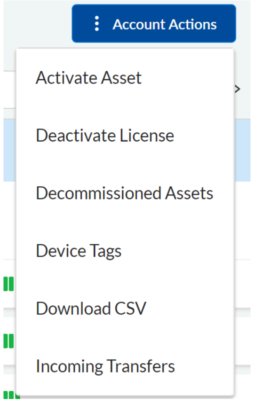


When you decommission assets with Enterprise Agreements, ELA and ESA hardware consump

To vie

Bulk Decommissioning of assets is a permanent operation!

STEP 7 | View the decommissioned assets through **Account Actions** > **Decommissioned Assets**.



Update NGFWs Managed by Strata Cloud Manager

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager)	□ Strata Cloud Manager Essentials □ Strata Cloud Manager Pro

Group and schedule PAN-OS software and dynamic content updates for your firewalls:

□ Create a software update grouping rule so you can group sets of firewalls and schedule PAN-OS software upgrades for sets of firewalls. A firewall can only be associated with a single software update grouping rule. When you create a new software update grouping rule, only firewalls not already associated with an existing software update grouping rule are displayed as Target Devices.

□ To ensure that you’re always protected from the latest threats, including those that haven’t yet been discovered, you must ensure that you keep your firewalls up to date with the latest content and software updates published by Palo Alto Networks.

To install the latest Antivirus, Applications and Threats, and WildFire dynamic content updates on your firewalls, you can schedule a recurring update schedule to specify which dynamic content update to install. A Dynamic Update schedule can be configured at the snippet, folder, or firewall level. A Dynamic Update schedule created at the folder level is inherited by all nested folders and associated firewalls but can be modified for the nested folder or individual firewall.

□ Schedule a PAN-OS software update to upgrade or downgrade your firewalls to a target PAN-OS version at a date and time of your choosing. Firewalls require an outbound internet connection in order to successfully download and install the PAN-OS software version from the Palo Alto Networks Update Server configured by default on the firewall. A software update schedule is a one time event to schedule updates to a specific PAN-OS version and aren’t reoccurring.

Create a Software Update Grouping Rule

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Select **Workflows** > **Upgrades** > **NGFW - Scheduler** > **Software Update Grouping RulesInsights** > **Upgrade Recommendations** and **Add Software Upgrade Grouping Rule**.

STEP 3 | Configure the General settings for software update grouping rule.

1. Enter a **Name**.
2. (Optional) Enter a **Description** for the software update grouping rule.
3. Specify the **Position** of the update upgrade grouping rule.

   You can select **Before** or **After** an existing software update grouping rule. The position of the software update grouping rule determines which firewalls are `Target Devices`.

   Based on the rule position and Match Criteria, firewalls aren't displayed as `Target Devices` if they're already associated with a rule positioned before the rule you're creating.

STEP 4 | Configure the Match Criteria to filter and specify target firewalls associated with the software update grouping rule.

1. Specify the **Folders** the firewalls you want to target are associated with.

   - **Any** (default)—Include all folders and the associated firewalls.
   - **Match**—Select one or more folder names to match and include in the filtered target firewalls.
   - **Exclude (Negate)**—Select one or more folder names to match and exclude from the filtered target firewalls.
2. Specify the firewall **Models** you want to target.

   All supported NGFW models are listed and not just the firewall models associated with the filtered **Folders**.

   - **Any** (default)—Include all firewall models.
   - **Match**—Select one or more firewall models to match and include in the filtered target firewalls.
   - **Exclude (Negate)**—Select one or more firewall models to match and exclude from the filtered target firewalls.
3. Specify one or more firewall **Label** you want to target.

   If you specify multiple labels, use the **And**, **Or**, and **Not** operators to further filter the target firewalls.
4. (Optional) **Exclude Devices** from the list of `Target Devices`.
5. Review the list of `Target Devices` to confirm all the firewalls you want to include in the software update grouping rule are included.

   If not all the firewalls you want to include are listed, go back and modify the Match Criteria until all the firewalls you want included are listed as `Target Devices`.

STEP 5 | **Save**.

STEP 6 | Schedule a Software Update.

Schedule Dynamic Content Updates

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Device Settings** > **Device SetupConfiguration** > **NGFW and Prisma Access** > **Device Settings** > **Device Setup** and select the Configuration Scope where you want to create the Dynamic Updates schedule.

You can select a folder or firewall from your **Folders** or select **Snippets** to configure the Dynamic Update schedule in a snippet.

STEP 3 | Click the cog wheel to edit the Management Interface Settings and **Customize**.

If you modified the Dynamic Updates Scheduler for a nested folder or individual device, you can ***Revert to Inherited*** *to revert the Dynamic Updates Scheduler configuration from the* `Customized` *configuration to that inherited from the parent folder of the nester folder or that inherited from the folder the firewall is associated with.*

STEP 4 | Configure the **Antivirus** and **Application and Threats** dynamic content update schedule.

1. Configure the Recurrence the firewall checks for Antivirus and Application and Threats dynamic content updates.

   - **None**—No new dynamic content updates are retrieved or installed.
   - (Application and Threats only) **Every 30 Minutes**—Firewall checks for new dynamic content updates every 30 minutes and installs a new content update if available.

     Specify how many **Minutes Past Half-Hour** the firewall should check for new dynamic content updates (between **0** and **29**).
   - **Hourly**—Firewall checks for new content updates every hour and installs a new dynamic content update if available.

     Specify how many **Minutes Past Hour** the firewall should check for new dynamic content updates (between **0** and **59**).
   - **Daily**—Firewall checks for new dynamic content updates every day and installs a new dynamic content update if available.

     Specify the **Time** of day the firewall should check for new dynamic content updates.
   - **Weekly**—Firewall checks for new dynamic content updates every week and installs a new dynamic content update if available.

     Specify the **Day** and **Time** the firewall should check for new dynamic content updates.
2. Configure the Action the firewall takes when a new dynamic content update is available.

   - **None**—Firewall doesn't download or install the new dynamic content update.
   - **Download Only**—Firewall only downloads the new dynamic content update but doesn't install.

     If you select **Download Only**, you must log in to the firewall web interface and install the dynamic content update.
   - **Download and Install**—Firewall downloads and installs the new dynamic content update.
3. Configure the dynamic content update Threshold.

   This specifies the dynamic content update must be this many hours old in order for the Action to be taken (between (**1** and **336** hours).
4. (Application and Threats only) Configure the New App-ID Threshold.

   This specifies the amount of time the firewall waits to install a dynamic content update that contains a new App-ID (between (**1** and **336** hours).
5. (HA only) Check (enable) **Sync to Peer** to also install the Antivirus and Application and Threats dynamic content update on the firewall HA peer.

STEP 5 | Configure the **WildFire** dynamic content update schedule.

1. Configure the Recurrence the firewall checks for WildFire dynamic content updates.
   - **None**—No new dynamic content updates are retrieved or installed.
   - **Every Minute**—Firewall checks for new dynamic content updates every minute and installs a new content update if available.
   - **Every 15 Minutes**—Firewall checks for new dynamic content updates every 15 minutes and installs a new content update if available.

     Specify how many **Minutes Past Quarter-Hour** the firewall should check for new dynamic content updates (between **0** and **14**).
   - **Every 30 Minutes**—Firewall checks for new dynamic content updates every 30 minutes and installs a new content update if available.

     Specify how many **Minutes Past Half-Hour** the firewall should check for new dynamic content updates (between **0** and **29**).
   - **Every Hour**—Firewall checks for new content updates every hour and installs a new dynamic content update if available.

     Specify how many **Minutes Past Hour** the firewall should check for new dynamic content updates (between **0** and **59**).
2. Configure the Action the firewall takes when a new dynamic content update is available.
   - **None**—Firewall doesn't download or install the new dynamic content update.
   - **Download Only**—Firewall only downloads the new dynamic content update but doesn't install.

     If you select **Download Only**, you must log in to the firewall web interface and install the dynamic content update.
   - **Download and Install**—Firewall downloads and installs the new dynamic content update.
3. (HA only) Check (enable) **Synchronize content with HA peer after download/install** to also install the WildFire dynamic content update on the firewall HA peer.

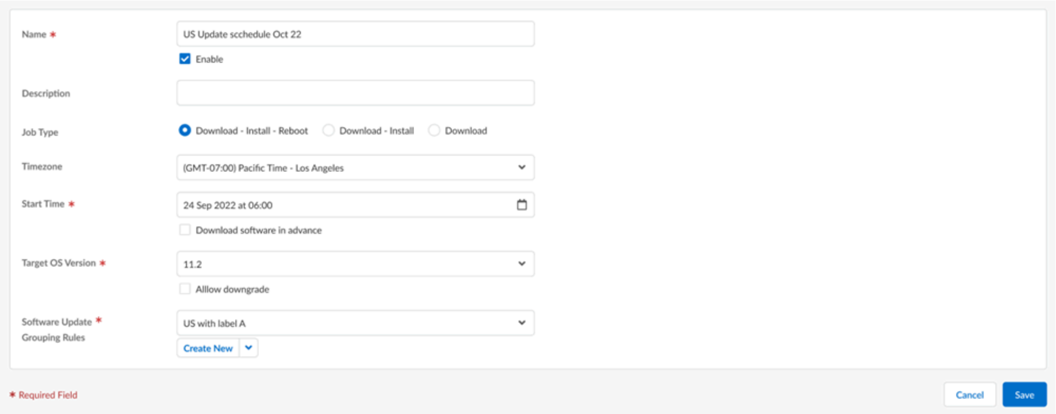
STEP 6 | **Save**.

Schedule a Software Update

STEP 1 | Log in to Strata Cloud Manager.

STEP 2 | Create a Software Update Grouping Rule.

STEP 3 | Select **Workflows** > **Upgrades** > **NGFW - Scheduler** > **SchedulesInsights** > **Upgrade Recommendations** and **Add Schedule**.



Name *	US Update scchedule Oct 22
	☑ Enable
Description	
Job Type	● Download - Install - Reboot ○ Download - Install ○ Download
Timezone	(GMT-07:00) Pacific Time - Los Angeles
Start Time *	24 Sep 2022 at 06:00
	☐ Download software in advance
Target OS Version *	11.2
	☐ Alllow downgrade
Software Update * Grouping Rules	US with label A

STEP 4 | Enter a **Name**.

STEP 5 | (Optional) Enter a **Description**.

STEP 6 | (Optional) Select the scope of the software upgrade:

- ☐ **Download-Install-Reboot** to go through the full update process.
- ☐ **Download-Install** to skip the reboot and avoid downtime.
- ☐ **Download** to skip the installation and reboot and manage these manually.

For upgrades that skip the install or reboot process, you can follow up on these actions from **Device Management**.

STEP 7 | Select the **Timezone** for the software install time.

STEP 8 | Specify the **Software Install Time** using the calendar tool to indicate the date and time you want the PAN-OS software download and install to occur.

Apply the date and time you want the update to occur.

STEP 9 | (Optional) Check (enable) **Download software in advanced** to specify a date and time you want the PAN-OS software version to be downloaded on the target firewalls.

Use the calendar tool to indicate the date and time you want the PAN-OS software version to be downloaded before install and **Apply**. The date and time must occur before the **Software Install Time**.

STEP 10 | Select the **Target OS Version** you want to update the firewall to.

(PAN-OS Software Downgrades only) If you're downgrading to an older PAN-OS, you must check (enable) ***Allow downgrade****. The downgrade fails if this setting isn't enabled.*

STEP 11 | Select **Device Grouping Rules** to associate firewalls with the software update schedule.

You can select multiple device grouping rules to update multiple sets of firewalls.

STEP 12 | **Save**.

NGFW Compatible Subscriptions

Where Can I Use This?	What Do I Need?
• NGFW	

The following Palo Alto Networks subscriptions unlock certain NGFW features or enable the NGFW to leverage a Palo Alto Networks cloud-delivered service (or both). Here you can read more about each service or feature that requires a subscription to work with the NGFW. To enable a subscription, you must first activate subscription licenses; once active, most subscription services can use Dynamic Content Updates to provide new and updated functionality to the NGFW.

Subscriptions You Can Use With the Firewall	
Strata Cloud Manager	Manage your Palo Alto Networks Next-Generation Firewalls (NGFW) from Strata Cloud Manager. This cloud-delivered, AI-powered security solution allows seamless management of your advanced ML-powered NGFWs, alongside Prisma Access deployments, through a single, streamlined user interface. Strata Cloud Manager has two licensing tiers: Strata Cloud Manager Essentials and Strata Cloud Manager Pro. This unified structure streamlines the deployment of network security offerings, including AIOps for NGFW, Autonomous Digital Experience Management (ADEM), cloud management functionality, and Strata Logging Service. • Get Started with Strata Cloud Manager • Strata Cloud Manager License
IoT Security	The IoT Security solution works with next-generation NGFWs to dynamically discover and maintain a real-time inventory of the IoT devices on your network. Through AI and machine-learning algorithms, the IoT Security solution achieves a high level of accuracy, even classifying IoT device types encountered for the first time. And because it’s dynamic, your IoT device inventory is always up to date. IoT Security also provides the automatic generation of policy recommendations to control IoT device traffic, as well as the automatic creation of IoT device attributes for use in NGFW policies. • Get Started with IoT Security.
SD-WAN	Provides intelligent and dynamic path selection on top of the industry-leading security that PAN-OS software already delivers. Managed by Panorama, the SD-WAN implementation includes:

Subscriptions You Can Use With the Firewall	
	• Centralized configuration management • Automatic VPN topology creation • Traffic distribution • Monitoring and troubleshooting • Get Started with SD-WAN
Threat Prevention	Threat Prevention provides: • Antivirus, anti-spyware (command-and-control), and vulnerability protection. • Built-in external dynamic lists that you can use to secure your network against malicious hosts. • Ability to identify infected hosts that try to connect to malicious domains. • Get Started with Threat Prevention
Advanced Threat Prevention	In addition to all of the features included with Threat Prevention, the Advanced Threat Prevention subscription provides an inline cloud-based threat detection and prevention engine, leveraging deep learning models trained on high fidelity threat intelligence gathered by Palo Alto Networks, to defend your network from evasive and unknown command-and-control (C2) threats by inspecting all network traffic. • Get Started with Advanced Threat Prevention
DNS Security	Provides enhanced DNS sinkholing capabilities by querying DNS Security, an extensible cloud-based service capable of generating DNS signatures using advanced predictive analytics and machine learning. This service provides full access to the continuously expanding DNS-based threat intelligence produced by Palo Alto Networks. To set up DNS Security, you must first purchase and install a Threat Prevention license. • Get Started with DNS Security
Advanced DNS Security	In addition to all of the features included with DNS Security, the Advanced DNS Security subscription provides access to the Advanced DNS Security cloud, which operates cloud-based domain detection engines that inspect changes to DNS responses. This enables NGFWs to detect and categorize hijacked and misconfigured domains in real-time to block malicious activity. • Get Started with Advanced DNS Security

Subscriptions You Can Use With the Firewall	
URL Filtering	Provides the ability to not only control web-access, but how users interact with online content based on dynamic URL categories. You can also prevent credential theft by controlling the sites to which users can submit their corporate credentials. To set up URL Filtering, you must purchase and install a subscription for the supported URL filtering database, PAN-DB. With PAN-DB, you can set up access to the PAN-DB public cloud or to the PAN-DB private cloud. *URL Filtering is no longer available as a standalone subscription. All URL Filtering features are included with the Advanced URL Filtering subscription.* • Get Started with URL Filtering
Advanced URL Filtering	Advanced URL Filtering uses a cloud-based ML-powered web security engine to perform ML-based inspection of web traffic in real-time. This reduces reliance on URL databases and out-of-band web crawling to detect and prevent advanced, file-less web-based attacks including targeted phishing, web-delivered malware and exploits, command-and-control, social engineering, and other types of web attacks. • Get Started with Advanced URL Filtering
WildFire	Although basic WildFire® support is included as part of the Threat Prevention license, the WildFire subscription service provides enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding (APK, PDF, Microsoft Office, and Java Applet), as well as the ability to upload files using the WildFire API. A WildFire subscription is also required if your NGFWs will be forwarding files to an on-premise WF-500 appliance. • Get Started with WildFire
Advanced WildFire	Advanced WildFire is a subscription offering that provides access to Intelligent Run-time Memory Analysis: a cloud-based advanced analysis engine that complements static and dynamic analysis, to detect and prevent evasive malware threats. 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. • Get Started with Advanced WildFire

Subscriptions You Can Use With the Firewall	
AutoFocus	Provides a graphical analysis of NGFW traffic logs and identifies potential risks to your network using threat intelligence from the AutoFocus portal. With an active license, you can also open an AutoFocus search based on logs recorded on the NGFW. • Get Started with AutoFocus
Strata Logging Service	Provides cloud-based, centralized log storage and aggregation. The Strata Logging Service is required or highly-recommended to support several other cloud-delivered services, including Cortex XDR, IoT Security, and Prisma Access, and Traps management service. • Get Started with Strata Logging Service
GlobalProtect Gateway	Provides mobility solutions and/or large-scale VPN capabilities. By default, you can deploy GlobalProtect portals and gateways (without HIP checks) without a license. If you want to use advanced GlobalProtect features (HIP checks and related content updates, the GlobalProtect Mobile App, IPv6 connections, or a GlobalProtect Clientless VPN) you will need a GlobalProtect Gateway license for each gateway. • Get Started with GlobalProtect
Virtual Systems	This is a perpetual license, and is required to enable support for multiple virtual systems on PA-3200 Series NGFWs. In addition, you must purchase a Virtual Systems license if you want to increase the number of virtual systems beyond the base number provided by default on PA-400 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, and PA-7000 Series NGFWs (the base number varies by platform). The PA-220 and PA-800 Series NGFWs do not support virtual systems. (PAN-OS 11.1.2 and earlier releases)The multiple virtual systems are not supported on VM- Series NGFWs. (PAN-OS 11.1.3 and later releases)The multiple virtual systems are supported on VM-Series NGFWs. • Get Started with Virtual Systems
Enterprise Data Loss Prevention (DLP)	Provides cloud-based protection against unauthorized access, misuse, extraction, and sharing of sensitive information. Enterprise DLP provides a single engine for accurate detection and consistent policy enforcement for sensitive data at rest and in motion using machine learning-based data classification, hundreds of data patterns using regular expressions or keywords, and data profiles using Boolean logic to scan for collective types of data.

Subscriptions You Can Use With the Firewall	
	• Get Started with Enterprise DLP
SaaS Security Inline	The SaaS Security solution works with Strata Logging Service to discover all of the SaaS applications in use on your network. SaaS Security Inline can discover thousands of Shadow IT applications and their users and usage details. SaaS Security Inline also enforces SaaS policy rule recommendations seamlessly across your existing Palo Alto Networks NGFWs. App-ID Cloud Engine (ACE) also requires SaaS Security Inline. • Get Started with SaaS Security Inline

Activate Subscription Licenses

Where Can I Use This?	What Do I Need?
• NGFW	

Follow these steps to activate a new license on the NGFW.

The Decryption Mirroring feature requires you to activate a free license to unlock feature functionality. For those features, you should instead follow the steps to activate a free license for Decryption features.

STEP 1 | Locate the activation codes for the licenses you purchased.

When you purchased your subscriptions you should have received an email from Palo Alto Networks customer service listing the activation code associated with each subscription. If you cannot locate this email, contact Customer Support to obtain your activation codes before you proceed.

STEP 2 | Activate your Support license.

You will not be able to update your PAN-OS software if you do not have a valid Support license.

1. Log in to the web interface and then select **Device** > **Support**.
2. Click **Activate support using authorization code**.
3. Enter your **Authorization Code** and then click **OK**.

STEP 3 | Activate each license you purchased.

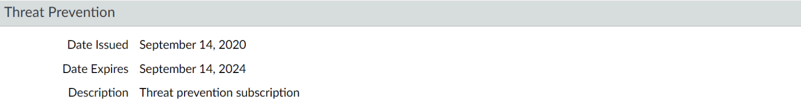
Select **Device** > **Licenses** and then activate your licenses and subscriptions in one of the following ways:

- **Retrieve license keys from license server**—Use this option if you activated your license on the Customer Support portal.
- **Activate feature using authorization code**—Use this option to enable purchased subscriptions using an authorization code for licenses that have not been previously activated on the support portal. When prompted, enter the **Authorization Code** and then click **OK**.
- **Manually upload license key**—Use this option if your NGFW does not have connectivity to the Palo Alto Networks Customer Support Portal. In this case, you must download a license key file from the support site on an internet-connected computer and then upload to the NGFW.

To automate activation using the Customer Support Portal API, see the process to Activate Licenses. This process works for both the hardware and VM-Series NGFWs.

STEP 4 | Verify that the license is successfully activated

On the **Device** > **Licenses** page, verify that the license is successfully activated. For example, after activating the WildFire license, you should see that the license is valid:



Threat Prevention

Date Issued September 14, 2020
Date Expires September 14, 2024
Description Threat prevention subscription

STEP 5 | (WildFire, Advanced URL Filtering, and DNS Security subscriptions only) **Commit** configuration changes to complete subscription activation.

After activating a WildFire, Advanced URL Filtering, or DNS Security subscription license, a commit is required for the NGFW to begin processing their corresponding traffic and data types based on the security profile configurations. You should:

- Commit any pending changes. If you do not have pending changes, which prevents you from committing any configuration updates, you can: issue a commit force command through the CLI or make an update that writes to the candidate configuration, which enables the commit option.

  Use the following CLI configuration mode command to initiate a commit force:

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

  A commit force bypasses some of the validation checks that normally occur with a normal commit operation. Make sure your configuration is valid and is semantically and syntactically correct before issuing a commit force update.

- WildFire only Check that the WildFire Analysis profile rules include the advanced file types that are now supported with the WildFire subscription. If no change to any of the rules is required, make a minor edit to a rule description and perform a commit.

What Happens When Licenses Expire?

Where Can I Use This?	What Do I Need?
• NGFW	

Palo Alto Networks subscriptions provide the NGFW with added functionality and/or access to a Palo Alto Networks cloud-delivered service. When a license is within 30 days of expiration, a warning message displays in the system log daily until the subscription is renewed or expires. Upon license expiration, some subscriptions continue to function in a limited capacity, and others stop operating completely. Here you can find out what happens when each subscription expires.

The precise moment of license expiry is at the beginning of the following day at 12:00 AM (GMT). For example, if your license is scheduled to end on 1/20 you will have functionality for the remainder of that day. At the start of the new day on 1/21 at 12:00 AM (GMT), the license will expire. All license-related functions operate on Greenwich Mean Time (GMT), regardless of the configured time zone on the NGFW.

(Panorama license) If the support license expires, Panorama can still manage NGFWs and collect logs, but software and content updates will be unavailable. The software and content versions on Panorama must be the same as or later than the versions on the managed NGFWs, or else errors will occur. For details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

Subscription	Expiry Behavior
Advanced Threat Prevention / Threat Prevention	Alerts appear in the System Log indicating that the license has expired. **You can still:** • Use signatures that were installed at the time the license expired, unless you install a new Applications-only content update either manually or as part of an automatic schedule. If you do, the update will delete your existing threat signatures and you will no longer receive protection against them. • Use and modify Custom App-ID™ and threat signatures. **You can no longer:** • Install new signatures. • Roll signatures back to previous versions. • Detect and prevent unknown threats using real-time, ML-based detection engines provided by Advanced Threat Prevention.
DNS Security	**You can still:**

Subscription	Expiry Behavior
	• Use local DNS signatures if you have an active Threat Prevention license. **You can no longer:** • Get new DNS signatures.
Advanced URL Filtering / URL Filtering	**You can still:** • Enforce policy using custom URL categories. **You can no longer:** • Get updates to cached PAN-DB categories. • Connect to the PAN-DB URL filtering database. • Get PAN-DB URL categories. • Analyze URL requests in real-time using advanced URL filtering.
WildFire	**You can still:** • Forward PEs for analysis. • Get signature updates every 24-48 hours if you have an active Threat Prevention subscription. **You can no longer:** • Get five-minute updates through the WildFire public and private clouds. • Forward advanced file types such as APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. • Use the WildFire API. • Use the WildFire appliance to host a WildFire private cloud or a WildFire hybrid cloud.
AutoFocus	**You can still:** • Use an external dynamic list with AutoFocus data for a grace period of three months. **You can no longer:** • Access the AutoFocus portal. • View the AutoFocus Intelligence Summary for Monitor log or ACC artifacts.
Strata Logging Service	**You can still:**

Subscription	Expiry Behavior
	• Store log data for a 30-day grace period, after which it is deleted. • Forward logs to Strata Logging Service until the end of the 30-day grace period.
GlobalProtect	**You can still:** • Use the app for endpoints running Windows and macOS. • Configure single or multiple internal/external gateways. **You can no longer:** • Access the Linux OS app and mobile app for iOS, Android, Chrome OS, and Windows 10 UWP. • Use IPv6 for external gateways. • Run HIP checks. • Use Clientless VPN. • Enforce split tunneling based on destination domain, client process, and video streaming application.
VM-Series	See the VM-Series Deployment Guide.
Support	**You can no longer:** • Receive software updates. • Download VM images. • Benefit from technical support.

Enhanced Application Logs for Palo Alto Networks Cloud Services

Where Can I Use This?	What Do I Need?
- NGFW	

The NGFW can collect data that increases visibility into network activity for Palo Alto Networks apps and services, like Cortex XDR and Internet of Things (IoT) Security. These Enhanced Application logs are designed strictly for Palo Alto Networks apps and services to consume and process; you cannot view Enhanced Application logs on the NGFW or Panorama. Only NGFWs sending logs to the logging service can generate Enhanced Application logs.

Enabling Enhanced Application Logging (EAL) can cause undesired logging behavior, such as the generation of URL Filtering logs for traffic to allowed categories. This can impact storage capacity and performance. Disable EAL to reduce undesired logs.

Follow these procedures to enable log forwarding of Enhanced Application logs for Cortex XDR and IoT Security:

Cortex XDR

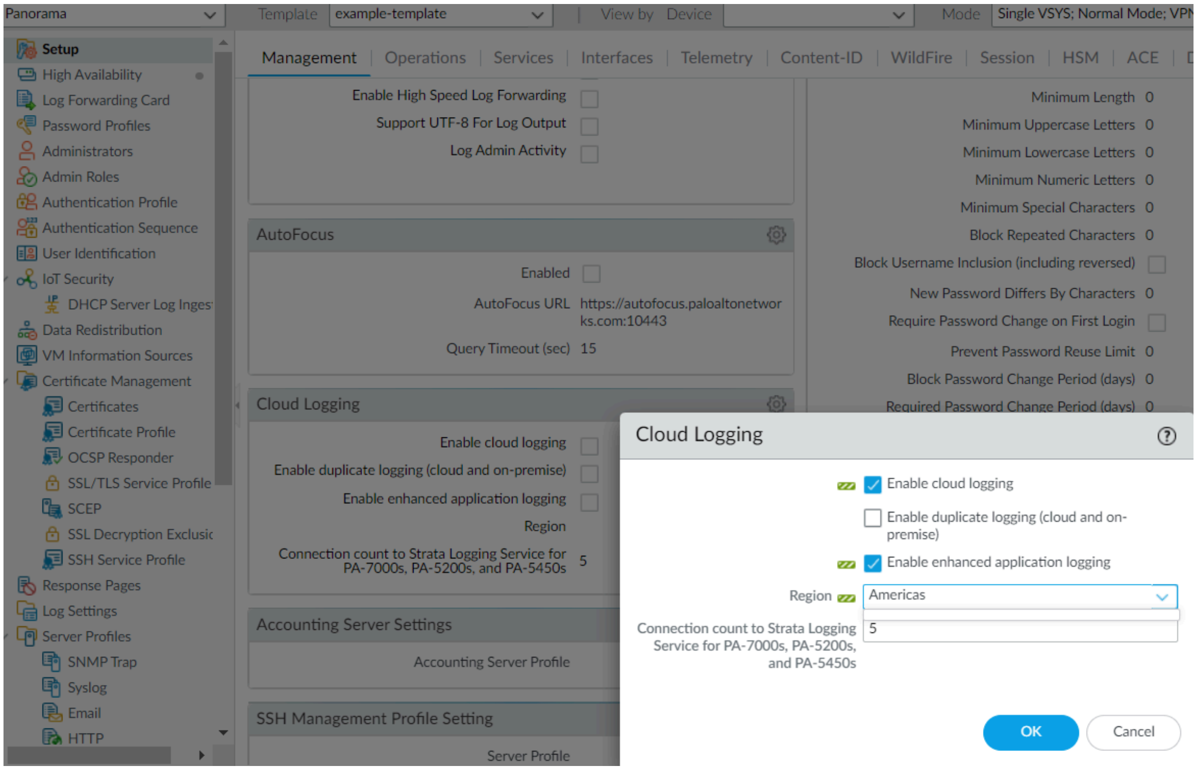
The types of data that Enhanced Application logs gather include records of DNS queries, the HTTP header User Agent field that specifies the web browser or tool used to access a URL, and information about DHCP automatic IP address assignment. With DHCP information, for example, Cortex XDR™ can alert on unusual activity based on hostname instead of IP address. This allows the security analyst using Cortex XDR to meaningfully assess whether the user's activity is within the scope of their role, and if not, to more quickly take action to stop the activity.

To benefit from the most comprehensive set of Enhanced Application logs, enable User-ID; deployments for the Windows-based User-ID agent and the PAN-OS integrated User-ID agent both collect some data that is not reflected in the NGFW User-ID logs but that is useful toward associating network activity with specific users.

To start forwarding Enhanced Application logs to the Strata Logging Service, turn on Enhanced Application Logging (EAL) globally, and then enable it on a per-security rule basis (using a Log Forwarding profile). The global setting is required and captures data for traffic that is not session-based (ARP requests, for example). The per-security policy rule setting is strongly recommended; the majority of Enhanced Application logs are gathered from the session-based traffic that your Security policy rules enforce.

STEP 1 | Enhanced Application Logging requires a Strata Logging Service subscription. User-ID is also recommended. Here are steps to get started with Strata Logging Service and enable User-ID.

STEP 2 | To **Enable Enhanced Application Logging** on the NGFW, select **Device** > **Setup** > **Management** > **Cloud Logging** and edit Settings.



Panorama
Template example-template
View by Device
Mode Single VSYS; Normal Mode; VPN
Setup
High Availability
Log Forwarding Card
Password Profiles
Administrators
Admin Roles
Authentication Profile
Authentication Sequence
User Identification
IoT Security
DHCP Server Log Inges
Data Redistribution
VM Information Sources
Certificate Management
Certificates
Certificate Profile
OCSP Responder
SSL/TLS Service Profile
SCEP
SSL Decryption Exclusic
SSH Service Profile
Response Pages
Log Settings
Server Profiles
SNMP Trap
Syslog
Email
HTTP
Management
Operations
Services
Interfaces
Telemetry
Content-ID
WildFire
Session
HSM
ACE
Enable High Speed Log Forwarding
Support UTF-8 For Log Output
Log Admin Activity
AutoFocus
Enabled
AutoFocus URL https://autofocus.paloaltonetworks.com:10443
Query Timeout (sec) 15
Cloud Logging
Enable cloud logging
Enable duplicate logging (cloud and on-premise)
Enable enhanced application logging
Region
Connection count to Strata Logging Service for PA-7000s, PA-5200s, and PA-5450s 5
Accounting Server Settings
Accounting Server Profile
SSH Management Profile Setting
Server Profile
Minimum Length 0
Minimum Uppercase Letters 0
Minimum Lowercase Letters 0
Minimum Numeric Letters 0
Minimum Special Characters 0
Block Repeated Characters 0
Block Username Inclusion (including reversed)
New Password Differs By Characters 0
Require Password Change on First Login
Prevent Password Reuse Limit 0
Block Password Change Period (days) 0
Required Password Change Period (days) 0
OK
Cancel

Cloud Logging

☑ Enable cloud logging

☐ Enable duplicate logging (cloud and on-premise)

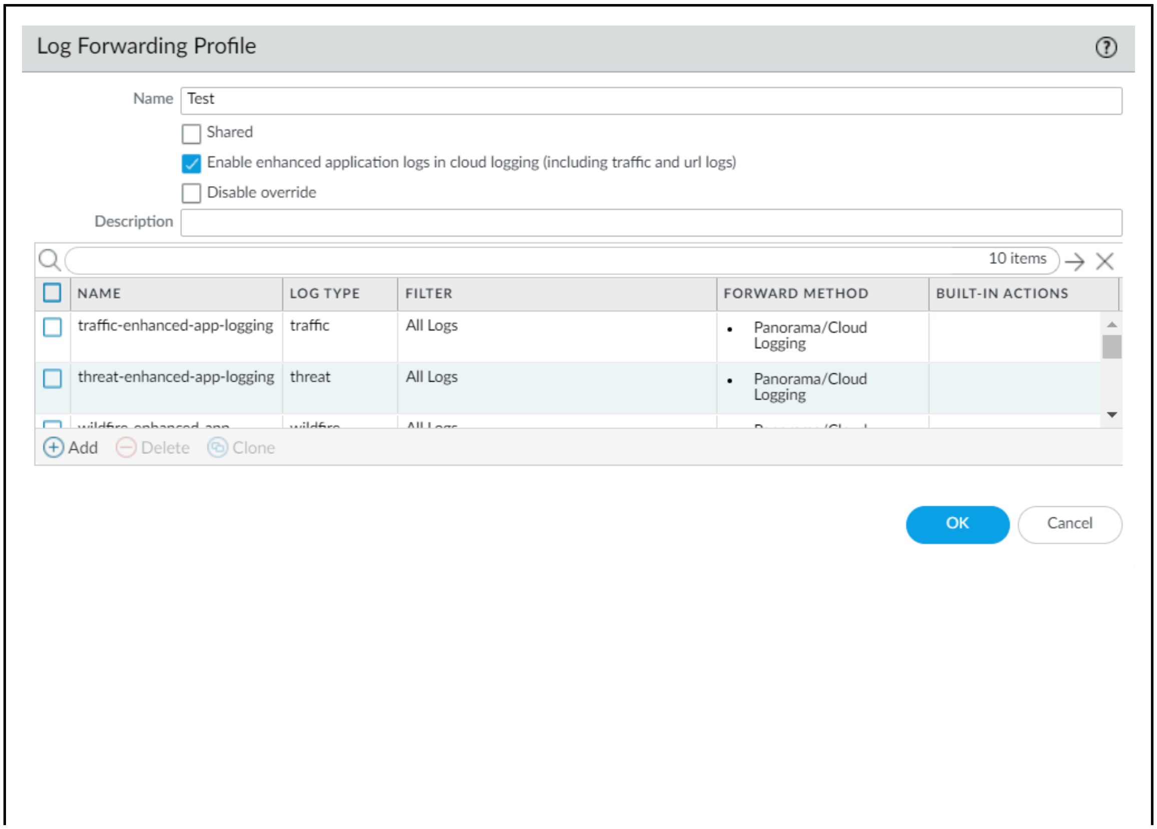
☑ Enable enhanced application logging

Region: Americas

Connection count to Strata Logging Service for PA-7000s, PA-5200s, and PA-5450s: 5

STEP 3 | Continue to enable EAL in the Security policy rules that control the traffic into which you want extended visibility.

1. Select **Objects** > **Log Forwarding** and **Add** or modify a Log Forwarding profile.
2. Update the profile to **Enable enhanced application logs in cloud logging (including traffic and url logs)**.



Name: Test

□ Shared

☑ Enable enhanced application logs in cloud logging (including traffic and url logs)

□ Disable override

Description:

10 items

□	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
□	traffic-enhanced-app-logging	traffic	All Logs	• Panorama/Cloud Logging	
□	threat-enhanced-app-logging	threat	All Logs	• Panorama/Cloud Logging	
□	wildfire-enhanced-app	wildfire	All Logs	Panorama/Cloud	

Notice that when you enable EAL in a Log Forwarding profile, match lists that specify the log types required for EAL are automatically added to the profile.

3. Click **OK** to save the profile and continue to update as many profiles as needed.
4. Ensure that the Log Forwarding profile that you've updated is attached to a Security policy rule, to trigger log generation and forwarding for the traffic matched to the rule.

   1. To view the profiles attached to each Security policy rule, select **Policies** > **Security**.
   2. To update the Log Forwarding profile attached to a rule, **Add** or edit a rule and select **Policies** > **Security** > **Actions** > **Log Forwarding** and select the Log Forwarding profile enabled with EAL.

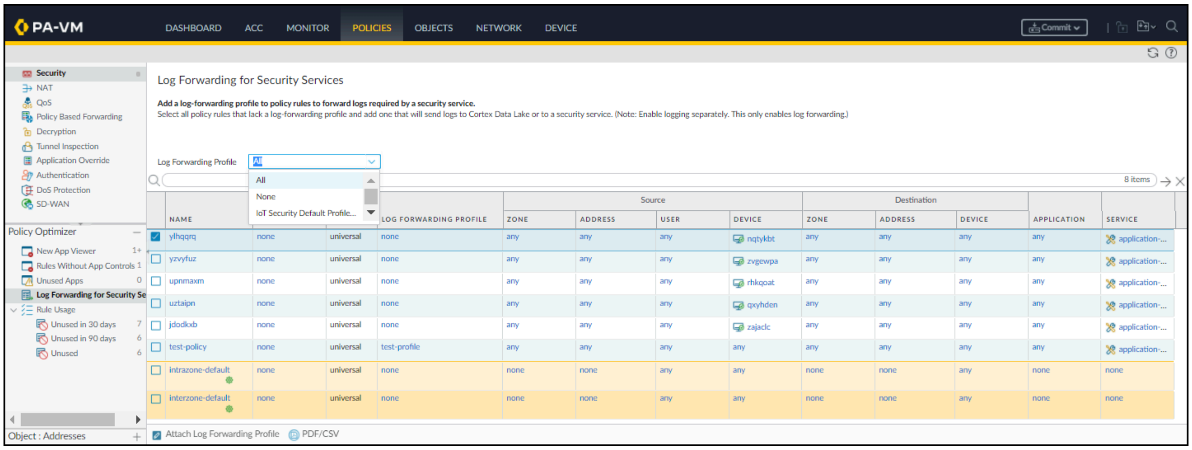
IoT Security

One part of the NGFW setup for IoT Security involves creating a Log Forwarding profile and applying it to Security policy rules. Although you can apply a profile to each rule individually, a simpler approach is to select a predefined Log Forwarding profile and apply it to as many rules as you like in bulk. The following steps explain this approach to adding the predefined Log Forwarding profile to Security policy rules in bulk.

To use this workflow, you must have already configured security policy rules, enabled logging on the rules, and enabled logging services with Enhanced Application Logging (EAL).

STEP 1 | Apply a Log Forwarding profile for IoT Security to Security policy rules.

1. Log in to your next-generation NGFW and select **Policies** > **Log Forwarding for Security Services** in the Policy Optimizer section.
2. To view all your Security policy rules—including those with a Log Forwarding profile and those without—choose **All** for **Log Forwarding Profile**.



Log Forwarding for Security Services

Add a log-forwarding profile to policy rules to forward logs required by a security service.
Select all policy rules that lack a log-forwarding profile and add one that will send logs to Cortex Data Lake or to a security service. (Note: Enable logging separately. This only enables log forwarding.)

Log Forwarding Profile: All

- All
- None
- IoT Security Default Profile...

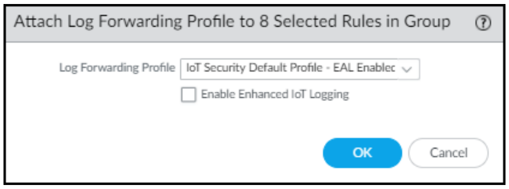
8 items

					Source				Destination				
	NAME			LOG FORWARDING PROFILE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
☑	ylhqqrq	none	universal	none	any	any	any	nqtykbt	any	any	any	any	application-...
□	yzvyfuz	none	universal	none	any	any	any	zvgewpa	any	any	any	any	application-...
□	upnmaxm	none	universal	none	any	any	any	rhkqoat	any	any	any	any	application-...
□	uztaipn	none	universal	none	any	any	any	qxyhden	any	any	any	any	application-...
□	jdodkxb	none	universal	none	any	any	any	zajaclc	any	any	any	any	application-...
□	test-policy	none	universal	test-profile	any	any	any	any	any	any	any	any	application-...
□	intrazone-default	none	universal	none	none	none	any	any	none	none	any	none	none
□	interzone-default	none	universal	none	none	none	any	any	none	none	any	none	none

3. Select the rules for which you want to forward logs to the logging service.
4. **Attach Log Forwarding Profile** at the bottom of the page.
5. To apply the default Log Forwarding profile to your rules, choose **IoT Security Default Profile - EAL Enabled** and **OK**.

   The default profile is preconfigured to provide IoT Security with all the log types it requires, including Enhanced Application logs.

   *You don't have to **Enable Enhanced IoT Logging** because EAL is already enabled on the IoT Security Default Profile.*



Attach Log Forwarding Profile to 8 Selected Rules in Group

Log Forwarding Profile: IoT Security Default Profile - EAL Enablec

□ Enable Enhanced IoT Logging

or

To forward Enhanced Application logs to an existing Log Forwarding profile that doesn't already have it, choose it from the **Log Forwarding Profile** list, select **Enable Enhanced IoT Logging** and then **OK**.

*When you **Enable Enhanced IoT Logging**, PAN-OS updates the chosen Log Forwarding profile itself and thereby enables enhanced log forwarding on all rules that use the same Log Forwarding profile.*

PAN-OS adds the chosen Log Forwarding profile to those rules that don't already have one and replaces previously assigned profiles with this one.

STEP 2 | **Commit** your changes.

Best Practices for Getting Started with NGFWs

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama)	

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

- □ Follow the Adminstrative Access Best Practices to make sure you are properly securing the management interfaces.
- □ Configure a best-practice security policy rulebase to safely enable applications and protect your network from attack. Go to the Best Practices page and select security policy best practice for your NGFW deployment.
- □ Set up High Availability—High availability (HA) is a configuration in which two NGFWs are placed in a group and their configuration and session tables are synchronized to prevent a single point to failure on your network. A heartbeat connection between the NGFW peers ensures seamless failover in the event that a peer goes down. Setting up a two-NGFW cluster provides redundancy and allows you to ensure business continuity.
- □ Enable User Identification (User-ID)—User-ID is a Palo Alto Networks next-generation NGFW feature that allows you to create policies and perform reporting based on users and groups rather than individual IP addresses.
- □ Enable Decryption—Palo Alto Networks NGFWs provide the capability to decrypt and inspect traffic for visibility, control, and granular security. Use decryption on a NGFW to prevent malicious content from entering your network or sensitive content from leaving your network concealed as encrypted or tunneled traffic.
- □ Follow the Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions.
- □ Share Threat Intelligence with Palo Alto Networks —Permit the NGFW to periodically collect and send information about applications, threats, and device health to Palo Alto Networks. Telemetry includes options to enable passive DNS monitoring and to allow experimental test signatures to run in the background with no impact to your security policy rules, NGFW logs, or NGFW performance. All Palo Alto Networks customers benefit from the intelligence gathered from telemetry, which Palo Alto Networks uses to improve the threat prevention capabilities of the NGFW.