CONFIGURING INITIAL FIREWALL SETTINGS

A JOURNEY OF A THOUSAND MILES BEGINS WITH … CONFIGURING YOUR MANAGEMENT NETWORK

- Initial system access
- Configure management network settings
- Activate a firewall, and manage licenses and software

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

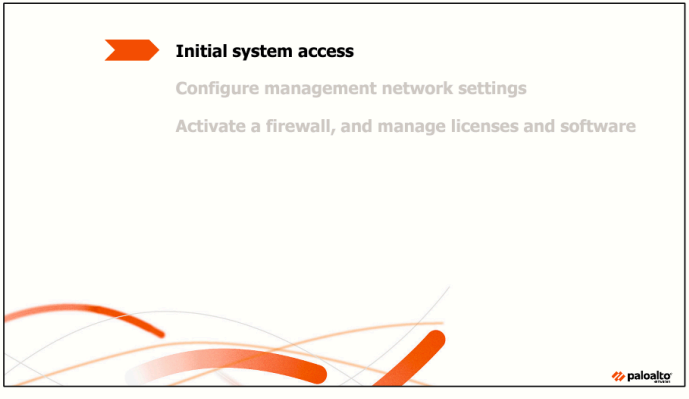
After you complete this module, you should be able to:

- Identify available firewall management interfaces and the methods to access them
- Configure firewall management interface network settings and services
- Identify the purpose and location of the firewall licenses and how to manage licenses
- Identify how to update the PAN-OS® software

This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

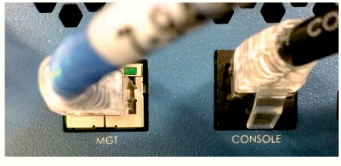
- Identify available firewall management interfaces and the methods to access them
- Configure firewall management interface network settings and services
- Identify the purpose and location of the firewall licenses and how to manage licenses
- Identify how to update the PAN-OS® software



This section introduces how to connect to a firewall and access a management interface so that you can begin to configure a firewall for your environment.

Initial Access to the Firewall

- Initial configuration must be performed using either:
  - Dedicated out-of-band management Ethernet interface (MGT)
  - Serial console connection
- Default MGT IP addressing:
  - Most firewall models: 192.168.1.1/24
  - VM-Series firewalls: DHCP client
- Predefined administrator:
  - Username: admin
  - Password: admin

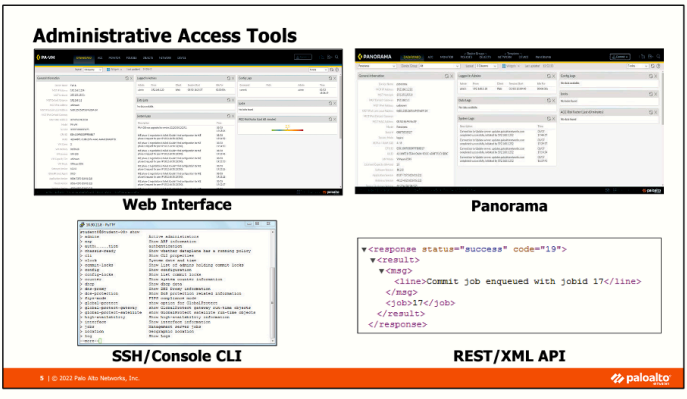


Palo Alto Networks firewalls are built with a dedicated out-of-band Ethernet network management interface labeled MGT. This interface passes only management traffic for the firewall and cannot be configured as a standard traffic interface. It is used for direct connectivity to the management plane of the firewall. You can configure the firewall to allow management traffic over the standard, in-band traffic interfaces.

For most models of firewalls, the MGT port has a factory default IP address of 192.168.1.1. For VM-Series firewalls starting with PAN-OS version 8.0, the MGT port is configured as a DHCP client. You can also configure the MGT port of any firewall model to use DHCP.

You accomplish the initial configuration of the firewall by connecting to the MGT port or the serial console port on the firewall. The serial console port is an RJ-45 connection on all firewalls. It has default configuration values of 9600-8-N-1.

The factory default for each firewall is to have a single administrative account named admin with a password of admin. Starting with PAN-OS 9.0.3, the firewall requires you to change the predefined admin account password at first login. The local admin password is stored in the firewall's XML configuration file but is encrypted using the firewall's master key.



There are four ways to access firewall management. Administrators often configure and monitor the firewall through the web-based interface, which provides detailed administrative and reporting tools in an intuitive browser-based format.

The Palo Alto Networks firewall can be configured and managed centrally using the Panorama management appliance, the Palo Alto Networks centralized security management system. If you have multiple firewalls deployed in your network, use Panorama to manage configurations, policies, and software and dynamic content updates. Panorama also will aggregate data from all managed firewalls and give you visibility into the information about all the traffic on your network.

The PAN-OS CLI enables you to access the firewall, display status and configuration information, and modify the configuration. Access to the PAN-OS CLI is provided through SSH or Telnet or directly through the serial console.

External systems and applications can execute commands remotely on a Palo Alto Networks firewall using the REST-based XML API. For example, you can use the REST-based interface to access operational status, reports, and packet captures or configure the firewall. The PAN-OS XML API can also capture login events and send them to the firewall. The XML API is implemented using HTTP/HTTPS requests and responses. Palo Alto Networks also provides an API browser on the firewall at https://<firewall>/api, where <firewall> is the hostname or IP address of the firewall. For more information about the PAN-OS 10.2 XML API, log into Live and search for "PAN-OS and Panorama API Usage Guide" or see https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-panorama-api.html.

Initial Login to the Web Interface

- Required to change predefined admin password at first login
- Predefined admin password complexity requirements:
  - Minimum of:
    - Eight characters
    - One uppercase character
    - One lowercase character
    - One numeral or special character
- These requirements:
  - Cannot be changed
  - Are not applied to other administrator accounts

Starting with PAN-OS 9.0.3, the firewall requires you to change the predefined admin account password at first login. The password complexity requirements are a minimum of eight characters in length, at least one uppercase character, one lowercase character, and one numeral or special character. These requirements apply only to the predefined administrator account and not to any additional firewall administrator accounts.

Navigate in the web interface to **Device > Setup > Management > Minimum Password Complexity** to define global password complexity and aging requirements for any other firewall administrator accounts that you create. You can also create per-administrator account password-aging requirements by navigating to **Device > Password Profiles** and creating a Password Profile. Any password-aging profiles that you create can be associated with specific administrator accounts and override any global password-aging settings.

Reset to Factory Configuration

- From the CLI with a *known* admin user password:

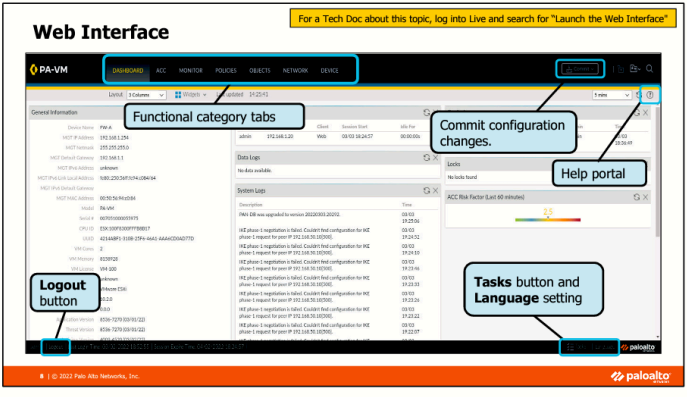
  `> request system private-data-reset`

  - Erases all logs
  - Resets all settings, including IP addressing, which causes loss of connectivity
  - Saves a default configuration after the MGT IP address is changed
- During bootup with an *unknown* admin user password:
  - From the console port, type **`maint`** during bootup.
  - Choose **Reset to Factory Default**.
  - Load a previous configuration file if the admin password has changed or is invalid.

For a Tech Doc about this topic, log into Live and search for "Reset Firewall to Factory Default Settings"

You can reset a firewall to its factory default settings. You can use the CLI operational command request system private-data-reset if you know the admin account password.

If you do not know the admin account password, you first must boot the firewall into maintenance mode. As the firewall is booting up, type the operational command **`maint`** into the CLI through the serial console port. After some time has elapsed, you can choose to have the firewall reset to its factory default settings, which includes setting the default admin password or loading a previous configuration file if the admin password has been inadvertently changed or an invalid config has been loaded.



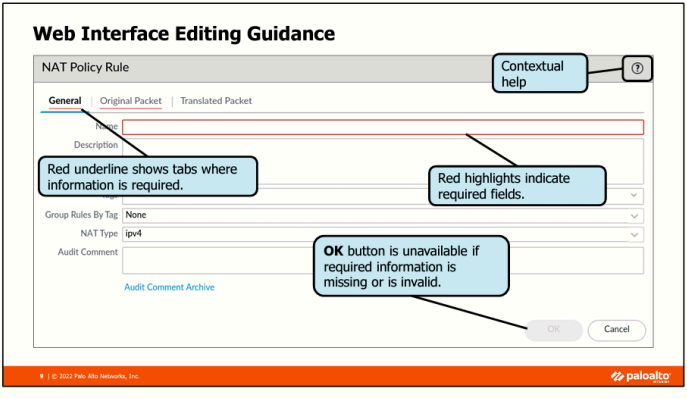
The PAN-OS web interface provides a common management interface across all Palo Alto Networks' physical and virtual firewall models. The web interface is supported on Internet Explorer 7+, Firefox 3.6+, Safari 5+, and Chrome 11+.

The management tools are grouped according to functional categories, which are listed as tabs at the top of the interface to ease switching between administrative tasks.

The **Help** button opens an HTML-formatted version of an administrator's guide in a separate browser tab. Click this searchable manual to get information about the options shown in a window or panel.

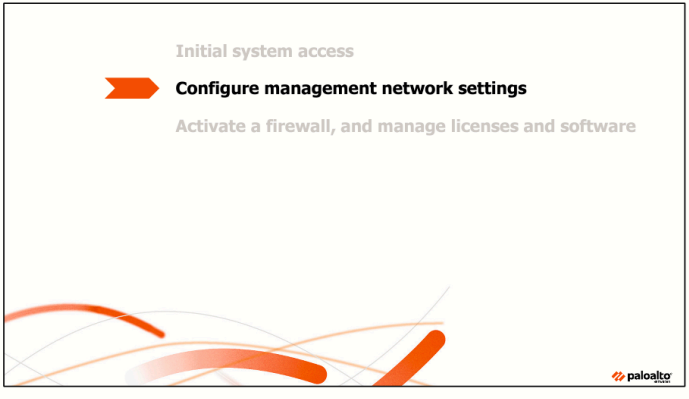
The **Tasks** button at the bottom right of the window provides a list of running and completed tasks for this firewall. This button is handy for verifying that configuration changes have been completed.

The web interface defaults to U.S. English, but it can be set to Traditional Chinese, Simplified Chinese, French, Japanese, or Spanish.

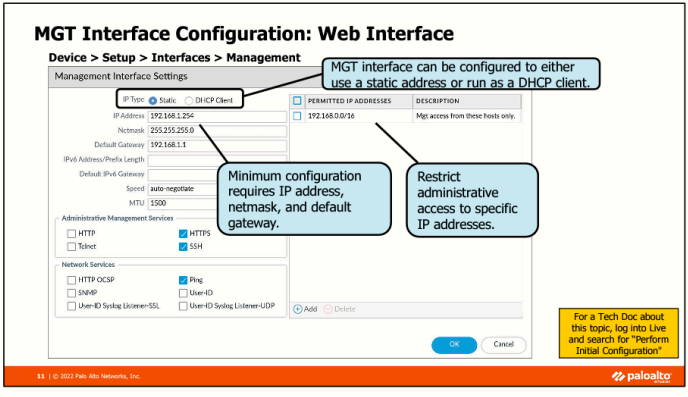


The web interface guides the configuration of the firewall:

- Red underlines or outlines indicate tabs that contain information that must be completed.
- Red highlights indicate required fields.
- The **OK** button is unavailable if required information is missing or is invalid.



This section provides an overview of the management network settings.



You can configure the MGT interface through the web interface. To connect your system or laptop to the MGT port so that you can use the web interface, complete the following steps:

1. Configure your system or laptop Ethernet interface in the 192.168.1.0/24 subnet.
2. Connect to the MGT port with an Ethernet cable.
3. Launch a web browser connection to https://192.168.1.1.
4. Log in using the default firewall username and password.
5. Select **Device > Setup > Interfaces**.
6. Click **Management**.
7. In the window that opens configure the MGT interface's network settings.
8. Reconnect to the web interface using the new network configuration.

By default, HTTPS, SSH, and ping are enabled on the MGT port. HTTPS is required to access and manage the firewall through the web interface, and SSH manages the firewall through the CLI. Palo Alto Networks also recommends selecting **Ping** to enable you to check connectivity to the MGT interface. The selection of **Ping** also allows two firewalls deployed in a high availability pair to send periodic heartbeats to verify connectivity. By default, HTTP, SNMP, and Telnet are disabled on the MGT interface. You can configure these settings as appropriate for your environment.

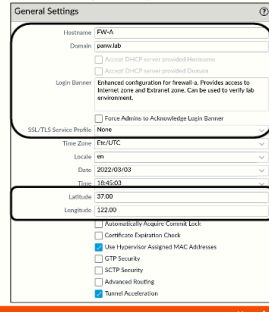
For additional security, in the **PERMITTED IP ADDRESSES** pane, enter only those IP addresses from which the firewall will accept administrative access to its MGT port.

Other Initial Configuration Settings

- Configure hostname and domain name:
  - Each defaults to the firewall model name.
- The **Accept DHCP...** options are available only if MGT is configured by DHCP.
- (Optional) Configure a security message in **Login Banner**.
- **Latitude** and **Longitude** are used to place the firewall on maps on the **ACC** and **Monitor** tabs.

For a Tech Doc about this topic, log into Live and search for "Configure Banners and Messages"

Device > Setup > Management



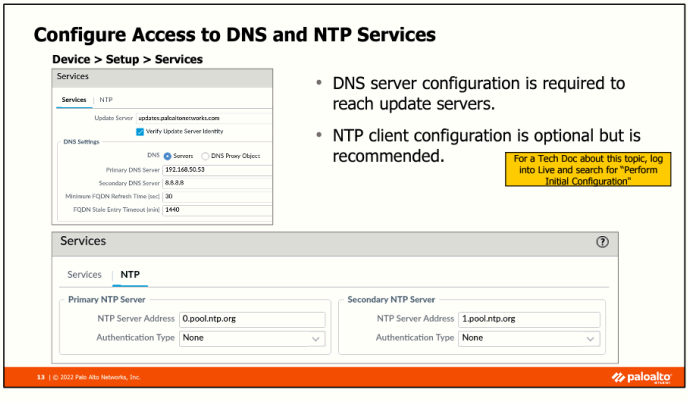
You can configure the firewall with a hostname to quickly identify the device that you are managing. A firewall hostname must be unique and can be a maximum of 31 characters in length. The hostname is case sensitive and can contain a mix of an alphanumeric, hyphen, and underscore characters. The factory default hostname is the firewall model name. The domain name can also be a maximum of 31 characters in length and contain a mix of an alphanumeric, hyphen, and dot characters. The factory default domain is empty.

If DHCP configures the MGT interface, then the **Accept DHCP server provided Hostname,** and the **Accept DHCP server provided Domain** options become available. Select these options to configure the firewall to allow hostname and domain name configuration by DHCP.

A login banner is an optional text that you can add to the login page so that administrators will see this information before they log in. For example, you could add a message to notify users of restrictions related to unauthorized firewall access. The login banner is displayed below the Name and Password fields on the web interface login page.

The firewall can provide various services, including a web server for the web interface or a GlobalProtect Portal or Gateway. SSL/TLS can secure communication between these firewall services and their clients. When SSL/TLS is used, the firewall requires a digital certificate that the clients trust. The clients and the firewall must also negotiate the protocol SSL/TLS versions for communication. An SSL/TLS Service Profile is configured to specify the firewall's certificate and the acceptable protocol versions that can be used by the clients when they connect to the firewall services.

The information you provide in the **Latitude** and **Longitude** fields enables the geographic placement of the firewall on the **ACC** tab's maps. The ACC maps include the **Source Regions** and **Destination Regions** maps. In addition to the ACC maps, the geographical information can be seen in **Monitor > App Score > Threat** and **Traffic** maps.

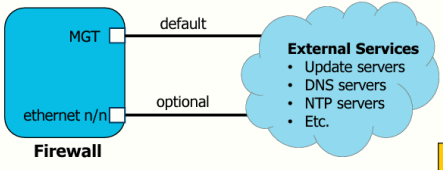


If you are configuring the MGT interface through the web interface, you should assign DNS servers for the MGT interface. You can configure a primary and secondary DNS server that will be used for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management. You can also configure primary and secondary NTP servers for the firewall. The firewall synchronizes the clock of the firewall with the time of the NTP server. If DHCP configures the MGT interface, the DNS and NTP server addresses can be assigned by DHCP.

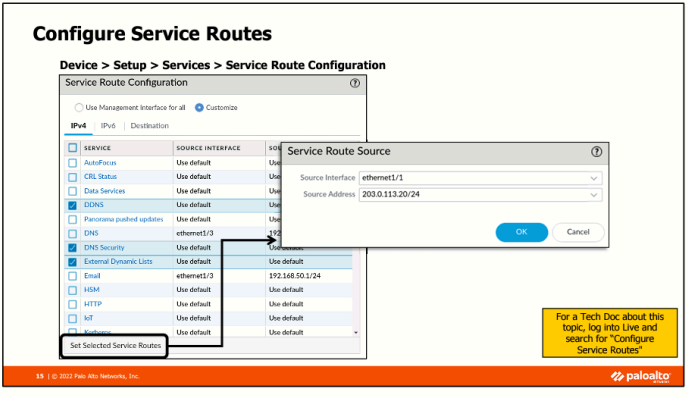
You can also configure the domain name of the update server used by the firewall to download updated software or malware signatures to the threat database. The default entry is updates.paloaltonetworks.com. It is recommended that you not change the default setting unless instructed by technical support. If the **Verify Update Server Identity** option is selected, the firewall verifies the digital certificate of the update server from which the software or threat database update is downloaded. This option adds security for the communication between the firewall and the update server.

Service Routes

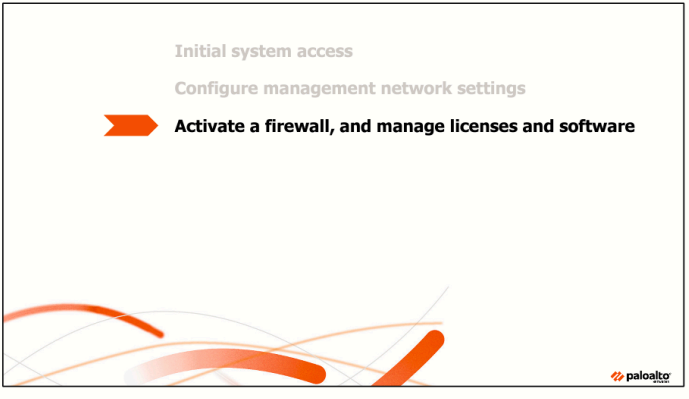
- By default, the MGT port is used to access external services.
- Configure an in-band port to access external services (optional):
  - Such a configuration is called a "service route."



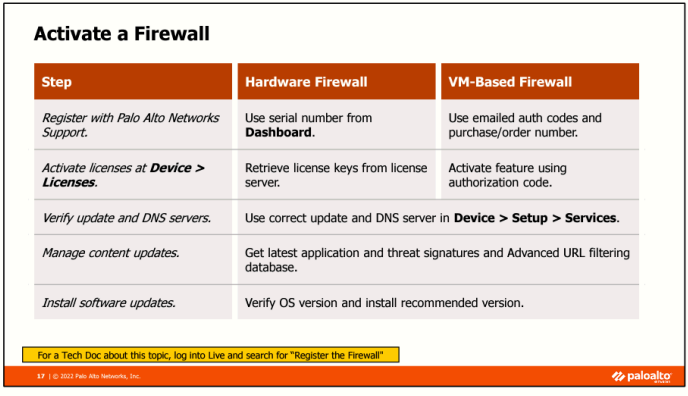
By default, the firewall uses the management (MGT) interface to access external services, such as DNS servers, external authentication servers, Palo Alto Networks services such as software, URL updates, licenses, and AutoFocus. An alternative to using the MGT interface is configuring a data port (a standard interface) to access these services. The path from the interface to the service on a server is a service route. The service packets exit the firewall on the port assigned for the external service, and the server responds to the configured source interface and source IP address.



Use **Device > Setup > Services > Service Route Configuration** to configure service routes. Select the check box next to any external services you want the firewall to access through an in-band port, and then click **Set Selected Service Routes**. Select the Source Interface and the Source Address in the dialog box that opens. If the selected interface has multiple IP addresses assigned to the interface, you can choose which source address the service route will use from the drop-down menu. After committing the configuration, the firewall will use the in-band port to access those external services.



This section provides an overview of subscription licenses and licensing, and PAN-OS software and content database updates.



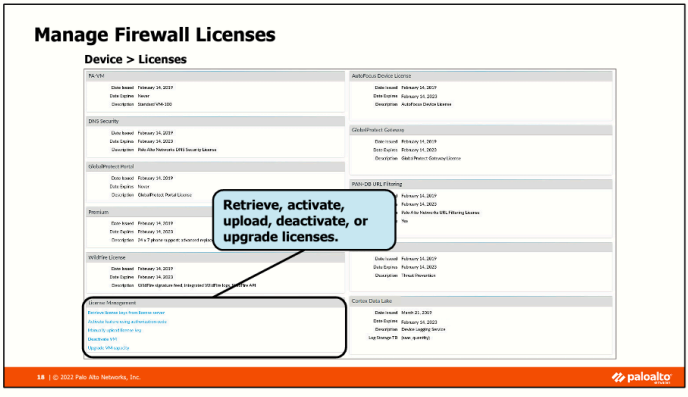
Before you can start using your firewall to secure the traffic on your network, you must register your firewall with Palo Alto Networks, activate your support license, and activate the licenses for each subscription you have purchased. Before you can retrieve a license, the firewall must be configured with an IP address, netmask, default gateway, and DNS server IP address.

To register a hardware firewall, click **Assets** on the Palo Alto Networks Customer Support Portal, enter your serial number, and click **Register Device**. The Customer Support Portal is at https://support.paloaltonetworks.com.

When you purchase a VM-Series firewall, you receive a set of authorization codes by email. The email typically includes authorization codes to license the purchased VM-Series model. First, register the code to the Support account on the Customer Support Portal to use the authorization code. If you have an existing Support account, click the **VM-Series Authentication Code** link on the Customer Support Portal to manage the VM-Series firewall licenses and download the software. If you do not have an existing Support account, use the **capacity auth-code** to register and create an account on the Customer Support Portal. After the new account is verified and the registration is complete, you can log in and download the software package needed to install the VM-Series firewall.

After you purchased your subscriptions, you should have received an email from Palo Alto Networks customer service that lists the activation code associated with each subscription. Before you can activate these licenses, you must activate your support license. Click **Device > Support** and then click **Activate support using authorization code**.

After support is activated, click **Device > Licenses** to activate your other subscriptions. There are multiple methods to activate your subscriptions. For additional guidance, log into Live and search for PAN-OS admin guide or see the PAN-OS Administrator's Guide at https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin.html. Activation of a WildFire® license requires a commit.

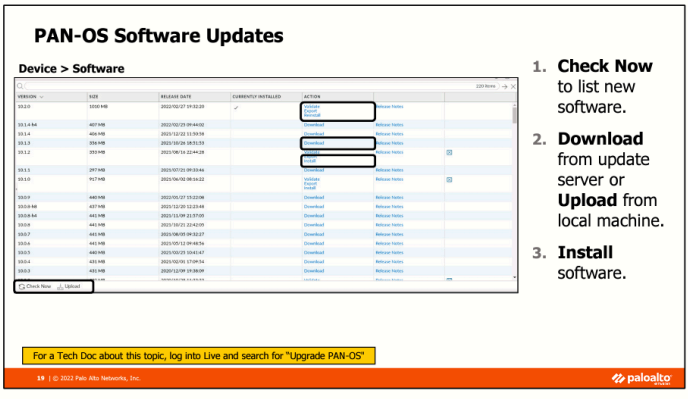


Before you can start using your firewall to secure the traffic on your network, you must activate the licenses for each service you purchased. Subscriptions unlock certain firewall features or enable the firewall to leverage a Palo Alto Networks cloud-delivered service, or both. To enable a subscription, you must first activate each subscription license. When active, most subscription services can use dynamic content updates to provide new and updated functionality to the firewall.

Available licenses and subscriptions include the following:

- **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.
- **GlobalProtect**: Provides mobility solutions and large-scale VPN capabilities. By default, you can deploy GlobalProtect portals and gateways (without HIP checks) without a license. If you want to use HIP checks, you will also need gateway licenses (subscription) for each gateway.
- **WildFire**: Basic WildFire support is included in the Advanced 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), and the ability to upload files using the WildFire API. A WildFire subscription is also required if your firewalls forward files to a WF-500 appliance.
- **AutoFocus**: Provides a graphical analysis of firewall traffic logs and identifies potential risks to your network by using threat intelligence from the AutoFocus portal. With an active license, you can also open an AutoFocus search based on logs recorded on the firewall.
- **URL Filtering**: Enables you to create security policies to enforce web access based on dynamic URL categories. To set up Advanced 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 the PAN-DB private cloud.
- **Threat Prevention**: Provides antivirus, anti-spyware, and vulnerability protection.

- **Virtual Systems**: This license is required to support multiple virtual systems on PA-2000 and PA-3000 Series firewalls. In addition, you must purchase a Virtual Systems license if you want to increase the number of virtual systems beyond the base number provided by default on PA-4000 Series, PA-5000 Series, and PA-7000 Series firewalls (the base number varies by platform). The PA-800, PA-500, PA-200, and VM-Series firewalls do not support virtual systems.
- **Cortex Data Lake**: Provides cloud-based, centralized log storage and aggregation. In earlier versions of PAN-OS, Cortex Data Lake was called the Logging Service.
- **SD-WAN**: Enables you to use multiple internet and private services to create an intelligent and dynamic WAN, which helps lower costs and maximize application quality and usability. The SD-WAN overlay supports dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use.



The firewall requires updates to the PAN-OS software and threat databases to maintain the most current protection levels. The MGT interface can be used to acquire these updates, or an in-band traffic interface can be configured to receive these updates. The firewall requires a DNS server configuration to connect to the update servers.

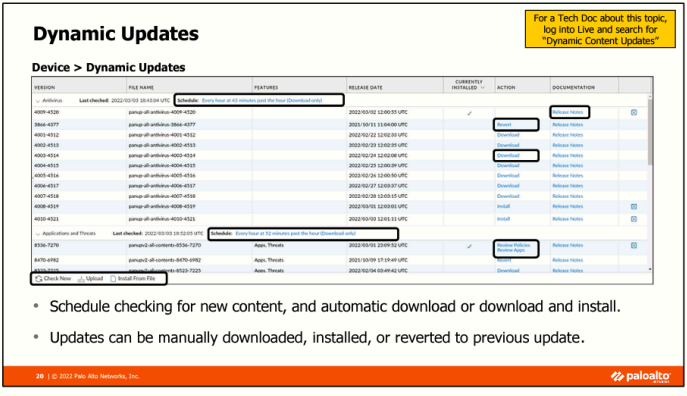
To upgrade to a new release of the PAN-OS software, click **Check Now** to display the list of available versions of the PAN-OS software. Read the release notes for each version and select a version to download and install. A support license is required for the download. Software updates require a firewall reboot.

When you upgrade, you must typically download the x.0 base release before installing the maintenance or feature release. For example, to upgrade from 8.1.1 to 9.1.0, download and install 8.1.10 first, then download and install 9.0.0 and 9.1.0.

The software can be downloaded directly from the Palo Alto Networks update server. Or the software can be downloaded to another system, such as a user desktop or a Panorama management appliance, and then uploaded to the firewall. After you manually upload a software image to the Palo Alto Networks firewall, the image appears in the list of available software at **Device > Software.** Click **Install** just as you would with software downloaded from the update server.

Before you upgrade the firewall software, the firewall must be running the most recent version of the Applications and Threats updates. The software installation process fails if it does not have a current update, and a prompt indicates that an update to the Applications and Threats file is required.

For information about upgrading PAN-OS, log into Live and search for "PAN-OS upgrade guide" or see the documentation at https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade.html.



Palo Alto Networks regularly updates its threats and application databases. Updates include new antivirus and spyware definitions, new malicious domains and URLs, and new application signatures. This new information must be downloaded to the firewall to maintain the most current protections. Before you can download Applications and Threats updates, you must have a Threat Prevention license. To fully protect your environment, you also should purchase and activate the separate Antivirus and WildFire licenses.

You can download updates directly from the Palo Alto Networks update server. You can also download the updates to another system, such as a user desktop or a Panorama management appliance, and then upload them to the firewall. Whether you download an update through the web or upload an update from Panorama, the update will appear in the list of available updates at **Device > Dynamic Updates**. Click **Install** to install the update.

Updated content is made available by Palo Alto Networks on the following schedule:

- Antivirus: daily
- Applications and Threats: weekly updates, new applications added monthly
- WildFire: about every five minutes

You configure how frequently the firewall checks for available updates. The firewall can check for Antivirus updates as frequently as every hour, for Applications and Threats updates as frequently as every 30 minutes, and for WildFire updates, they can be downloaded in Real-time allowing you to access the signatures as soon as they are generated.

Module Summary

Now that you have completed this module, you should be able to:

- Identify available firewall management interfaces and the methods to access them
- Configure firewall management interface network settings and services
- Identify the purpose and location of the firewall licenses and how to manage licenses
- Identify how to update the PAN-OS® software

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"Zone Security, Security and NAT Policies"

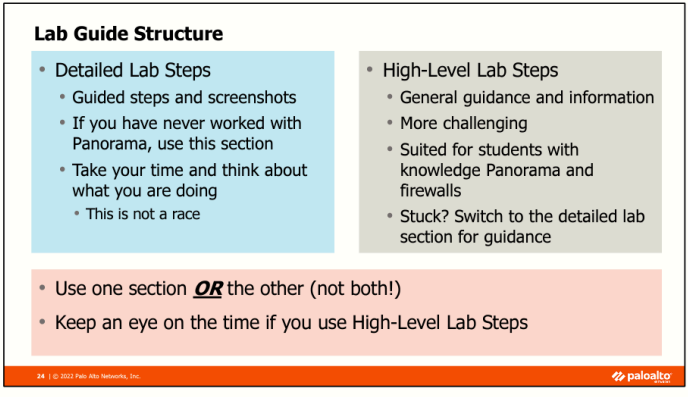
Review Questions

1. What are the two attributes of the dedicated out-of-band network management port in Palo Alto Networks firewalls? (Choose two.)
   a. labeled MGT by default
   b. cannot be configured as a standard traffic port
   c. supports only SSH connections
   d. requires a static, non-DHCP network configuration

2. True or false? You will need the firewall's serial number to register a hardware firewall.
   a. true
   b. false

3. In the web interface, what is signified when a text box is highlighted in red?
   a. The value in the text box is optional.
   b. The value in the text box is required.
   c. The value in the text box is an error.
   d. The value in the text box is controlled by Panorama.

4. True or false? Service routes can be used to configure an in-band port to access external services.
   a. true
   b. false



There are two sections for each lab in this guide:

- High-Level Lab Steps
- Detailed Lab Steps

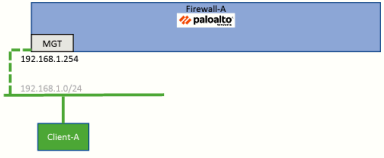
The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with the firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

You do not need to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Use either one or the other.

Lab 2 Overview



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 2: Configuring Initial Firewall Settings

- Connect to the firewall web interface
- Load a starting lab configuration
- Set DNS servers for the firewall
- Set NTP servers for the firewall
- Configure a login banner for the firewall
- Set Latitude and Longitude for the firewall
- Configure permitted IP addresses for firewall management
- Schedule dynamic updates

Answers to Review Questions

1. a, b
2. a (true)
3. b
4. a (true)