INITIAL CONFIGURATION

EDU-210 Version A
PAN-OS® 9.0

GET STARTED RIGHT

- Administrative controls
- Initial system access
- Configuration management
- Licensing and software updates
- Account administration
- Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

Agenda

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

- Connect to the firewall and log in as admin
- Configure the network settings for the management interface port
- Describe the difference between the running config and the candidate config
- Configure dynamic firewall updates to update the applications and threats databases
- Create a local firewall administrative account
- Access the firewall logs

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

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

- Connect to the firewall and log in as admin
- Configure the network settings for the management interface port
- Describe the difference between the running config and the candidate config
- Configure dynamic firewall updates to update the applications and threats databases
- Create a local firewall administrative account
- Access the firewall logs

© 2019 Palo Alto Networks, Inc.

Administrative controls

Initial system access

Configuration management

Licensing and software updates

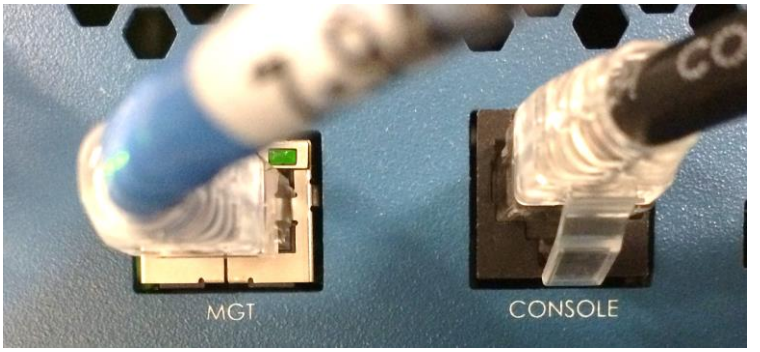
Account administration

Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

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
- Default access:
  - Username: admin
  - Password: admin



Palo Alto Networks firewalls are built with a dedicated out-of-band 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 normal, in-band traffic interfaces.

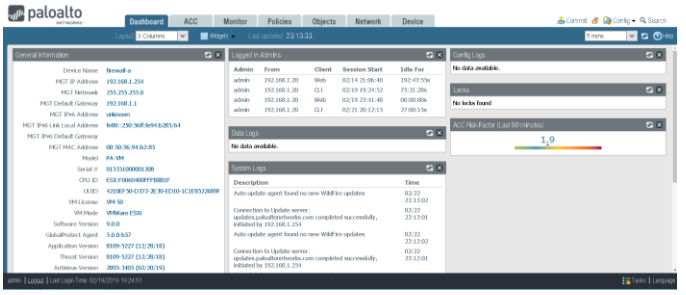
For most models of firewalls, the MGT port has a factory default IP address of 192.168.1.1. For VM-Series firewalls starting with PAN-OS® version 8.0, the MGT port is configured as a DHCP client. You also can configure the MGT port of any firewall model to use DHCP.

You accomplish initial configuration of the firewall by connecting to the MGT port or to 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*. A warning message appears at login in the web interface and the CLI until the default password is changed. The local admin password is stored in the firewall's XML configuration file but is encrypted using the firewall's master key.

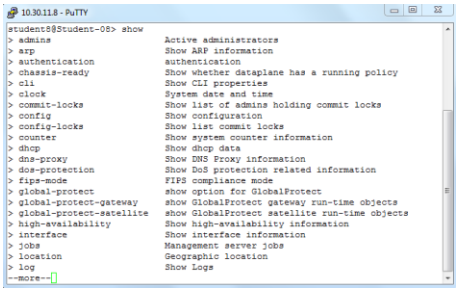
© 2019 Palo Alto Networks, Inc.

Administrative Access

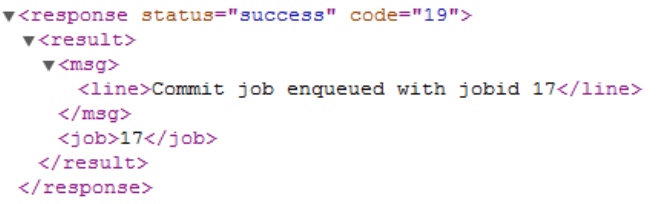


Web Interface

Panorama



SSH/Console CLI



REST XML API

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

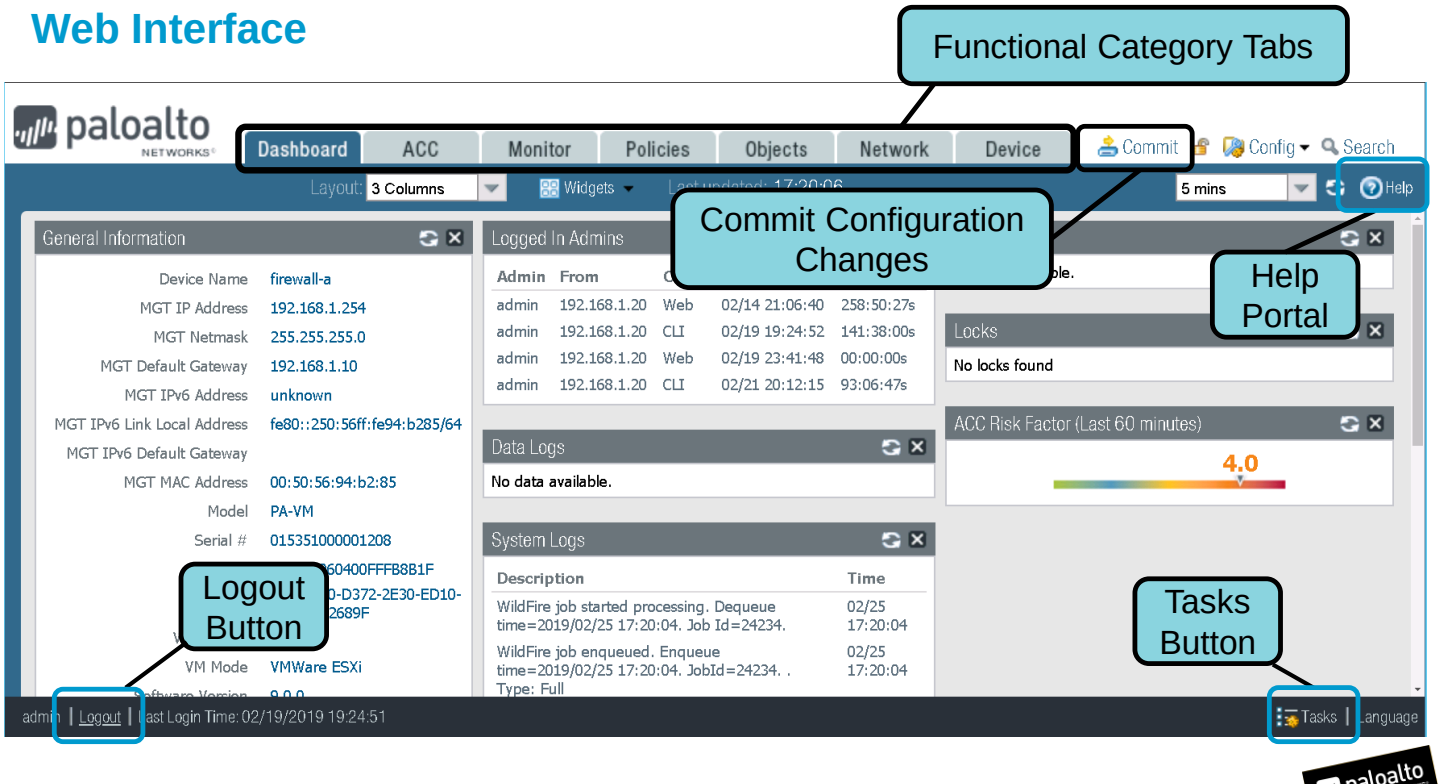
The Palo Alto Networks firewall can be configured and managed centrally using the Panorama management appliance, which is the Palo Alto Networks centralized security management system. If you have multiple firewalls deployed in your network, use Panorama to manage configurations, policies, and software 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, 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 to configure the firewall. The PAN-OS XML API also can be used to 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. PAN-OS 9.0 XML API reference documentation is available at https://docs.paloaltonetworks.com/pan-os. Information about XML API integration is available at https://live.paloaltonetworks.com/.

© 2019 Palo Alto Networks, Inc.

Web Interface



The PAN-OS web interface provides a common management interface across all Palo Alto Networks hardware-based and virtual-based 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 allow ease in switching between administrative tasks.

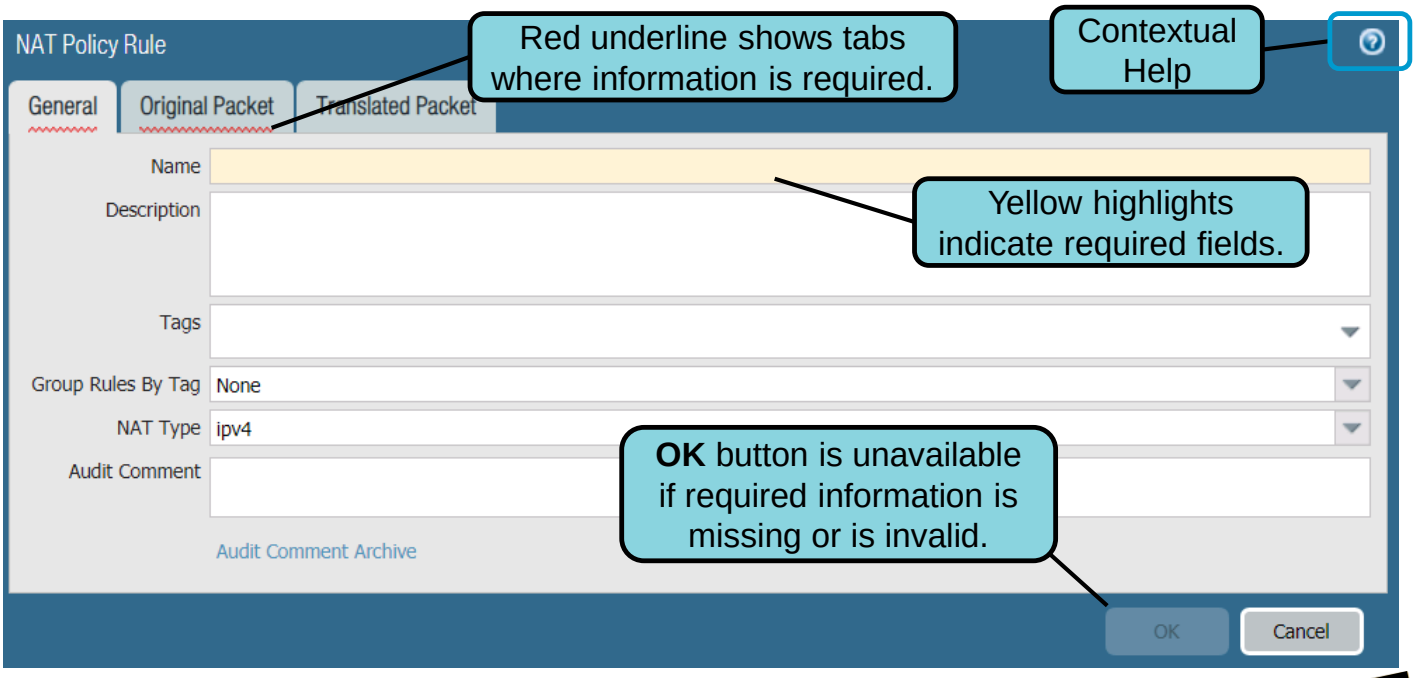
The **Help** button opens an HTML-formatted version of an administrator's guide in a separate browser tab. Click this searchable manual to get information about the options shown in a window or panel.

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

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

© 2019 Palo Alto Networks, Inc.

Web Interface Editing Guidance



The web interface provides guidance throughout the configuration of the firewall:

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

Administrative controls

Initial system access

Configuration management

Licensing and software updates

Account administration

Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

Reset to Factory Configuration

- From CLI with 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

- Without known admin user password:
  - From the console port, type `maint` during bootup
  - Choose **Reset to Factory Default**

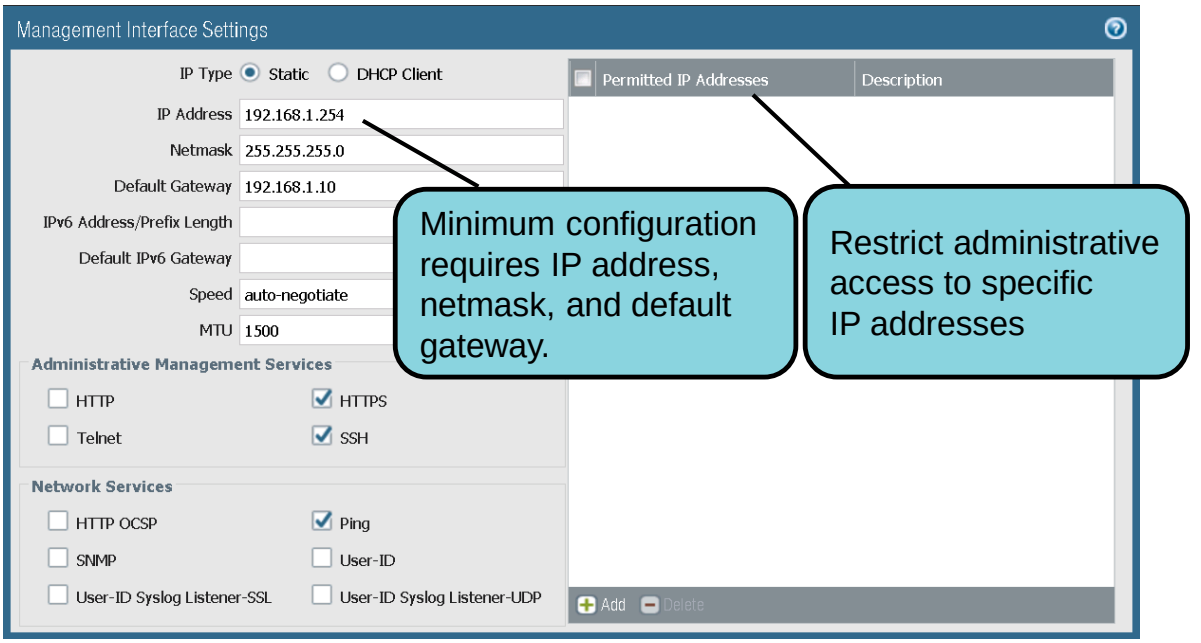
You can reset a firewall to its factory default settings. If you know the admin account password, you can use the CLI command **`request system private-data-reset`**.

If you do not know the admin account password, you must first place the firewall in maintenance mode. To enter maintenance mode, reboot the firewall. As the firewall is booting up, type the command **`maint`** into the CLI through the console port. After some time, you can choose the option to have the firewall reset to default, including the default admin password.

© 2019 Palo Alto Networks, Inc.

MGT Interface Configuration: Web Interface

Device > Setup > Interfaces > Management



You also can configure the MGT interface using 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 network settings for the MGT interface.
8. Reconnect to the web interface using the new network configuration.

HTTPS, SSH, and ping are enabled by default. HTTPS is required to access and manage the firewall through the MGT interface using the web interface. SSH is required to enable CLI connection to the MGT interface. Palo Alto Networks recommends that you enable ping to check connectivity to the MGT interface or to support heartbeats between firewalls deployed as a pair for High Availability. By default, HTTP, SNMP, and Telnet are disabled on the MGT interface. You can configure these settings as appropriate for your environment.

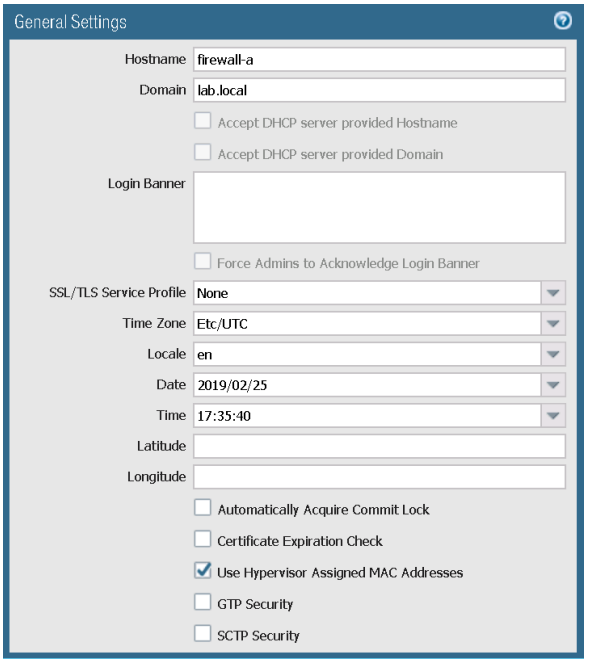
For additional security, enter IP addresses in the **Permitted IP Addresses** field to restrict administrative access to those IP addresses.

© 2019 Palo Alto Networks, Inc.

Configure General 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.
- Configure a security message in the **Login Banner** (optional).
- **Latitude** and **Longitude** are used to place the firewall on maps on the ACC tab.

Device > Setup > Management



A firewall hostname can be a maximum of 31 characters in length and contain a mix of alphanumeric, hyphen, and underscore characters. The factory default hostname is the firewall model name. The domain name can be a maximum of 31 characters in length and contain a mix of alphanumeric, hyphen, and dot characters. The factory default domain is empty. If the MGT interface is configured by DHCP, 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.

The hostname is labeled as Device Name in reports and logs. For example, for custom reports you can request that the report contain the Device Name. You also can filter log entries by Device Name.

A login banner is optional text that you can add to the login page so that administrators will see information they must know before they log in. For example, you could add a message to notify users of restrictions on unauthorized use of the firewall.

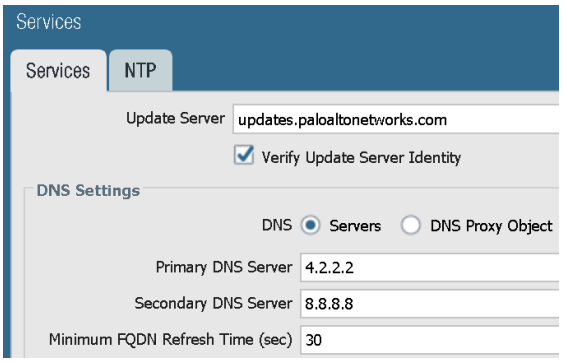
The firewall can provide various services that include a web server for the web interface and a GlobalProtect portal or gateway. Communication between these services running on the firewall, and their clients can be secured by SSL/TLS. When SSL/TLS is used, the firewall requires a digital certificate that is trusted by the clients. The clients and the firewall also must negotiate the protocol SSL/TLS versions to use 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 connecting to the firewall services.

The information that you provide in the **Latitude** and **Longitude** fields enables the geographic placement of the firewall on the ACC tab's **Source Regions** and **Destination Regions** maps.

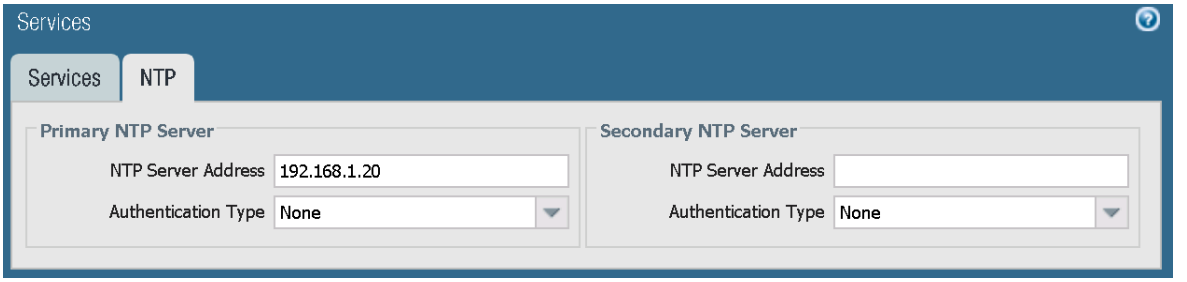
© 2019 Palo Alto Networks, Inc.

Configure DNS and NTP Servers

Device > Setup > Services



- DNS server configuration is required to reach update servers.
- NTP client configuration is optional but is recommended.



If you are configuring the MGT interface using the web interface, assign DNS servers for the MGT interface. You also can configure NTP servers for the firewall.

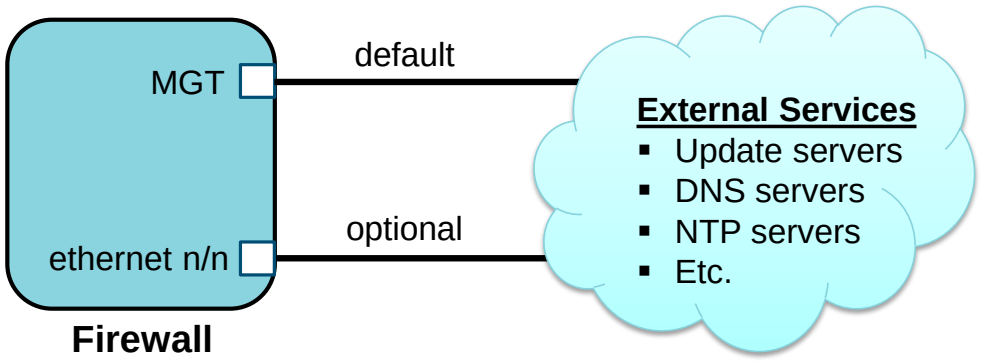
If the MGT interface is configured by DHCP, the DNS and NTP server addresses can be assigned by DHCP.

You also can configure the domain name of the update server used by the firewall to download updated software and updates to the threat database. The default entry is updates.paloaltonetworks.com. If the **Verify Update Server Identity** option is selected, the firewall verifies the SSL certificate of the update server from which the software or threat database update is downloaded. This option adds a level of security for the communication between the firewall and the update server.

© 2019 Palo Alto Networks, Inc.

Service Routes

- By default the MGT port is used to access external services.
- Configure an in-band port to access external services (optional).

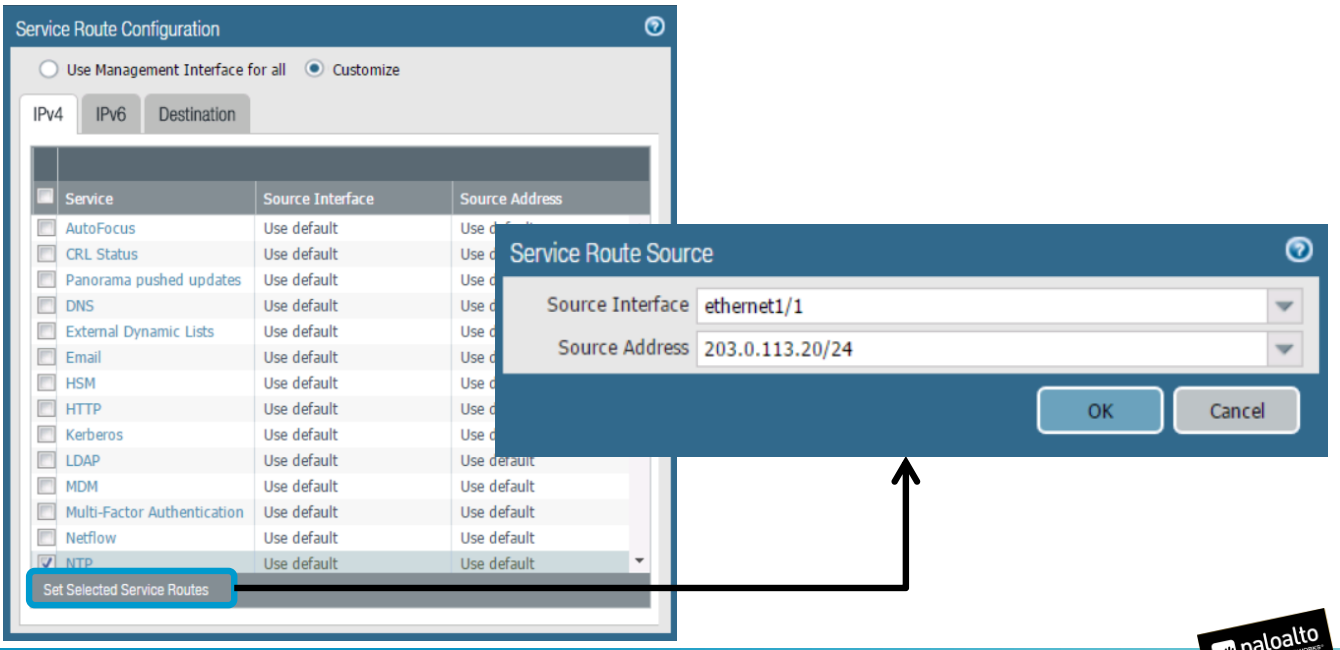


By default, the firewall uses the MGT interface to access remote DNS services, content update services, license retrieval services, NTP services, or other external services. If you do not want to enable external network access to your management network, you must set up an in-band data port to provide access to required external services and set up service routes to instruct the firewall which port to use to access the external services.

© 2019 Palo Alto Networks, Inc.

Configuring Service Routes

Device > Setup > Services > Service Route Configuration



Use **Device** > **Setup** > **Services** > **Service Route Configuration** to configure service routes. Select the check box next to any external services that the firewall will access through an in-band port and then click **Set Selected Service Routes**. In the dialog window that opens, select the **Source Interface** and the **Source Address**. After you commit the configuration, the firewall will use the in-band port to access those external services.

© 2019 Palo Alto Networks, Inc.

Administrative controls

Initial system access

Configuration management

Licensing and software updates

Account administration

Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

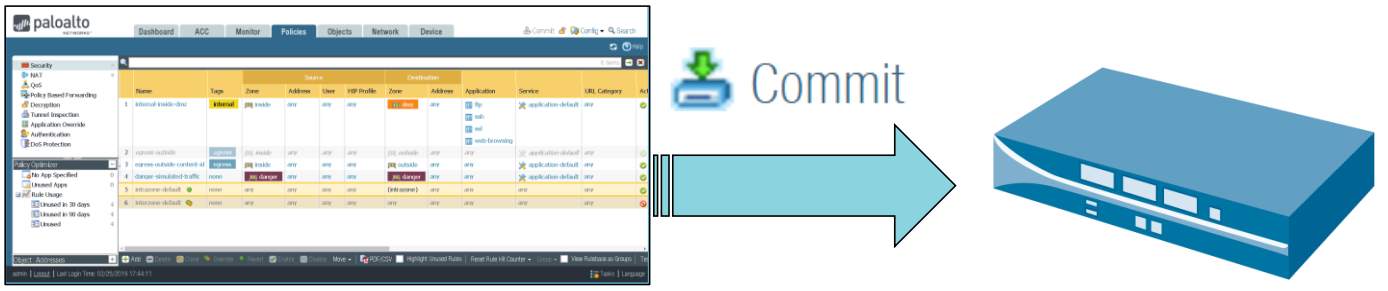
Configuration Types

Candidate Configuration

- Configuration changes made but not committed

Running Configuration

- Configuration settings currently active on the firewall



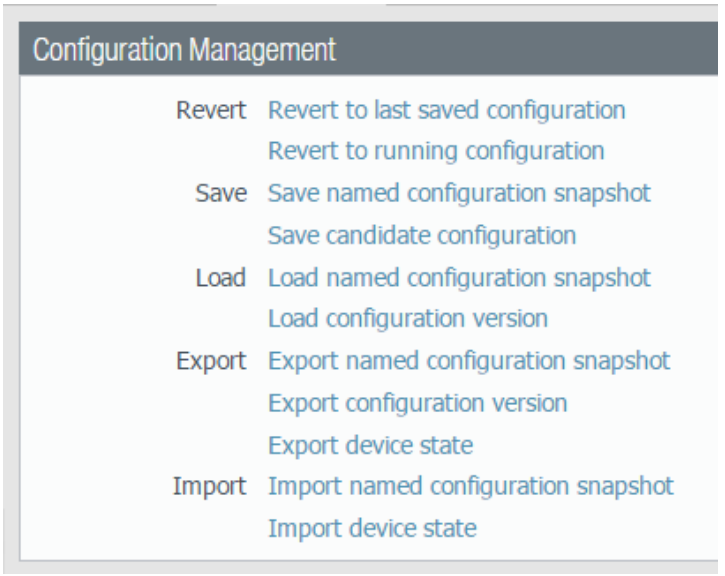
The running configuration is the actual configuration controlling the operation of the firewall. It is maintained in a file on the firewall named running-config.xml. The running configuration is copied to a candidate configuration during firewall startup. In-progress edits are made to the candidate configuration.

After you click **Commit** at the top of the web interface or type **`commit`** in the CLI, the candidate configuration overwrites the current running configuration, which activates all configuration changes. The firewall saves previous running configurations and labels these configurations by date and timestamps. The web interface includes a set of operations that are used to manage the running and candidate configurations. For example, you can use the web interface to switch to a previously running configuration.

© 2019 Palo Alto Networks, Inc.

Global Configuration Management

Device > Setup > Operations



- These operations are global in scope and not per-admin.
- **Revert**, **Save**, and **Load** operations all manage configurations local to the firewall.
- **Export** operations export configurations from the firewall to the host running the web interface.
- **Import** operations import configurations from the firewall to the host running the web interface.

You can manage running, candidate, and saved configurations from **Device > Setup > Operations**. These operations are global in scope. All changes from any administrator will be loaded, saved, reverted, and so on.

The **Revert**, **Save**, and **Load** operations all work with firewall configurations that are local to the firewall.

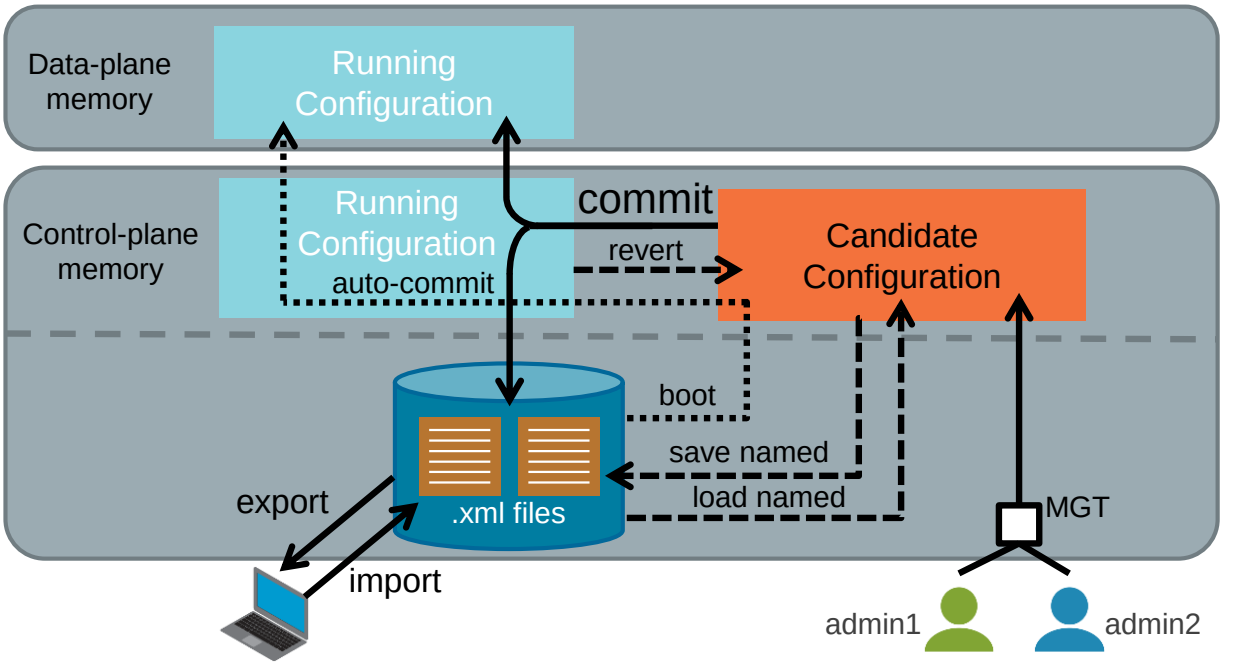
The **Export** operations transfer configurations as XML-formatted files from the firewall to the host running the web interface browser. From your local machine you can save the files as configuration backups. Exported files also can be edited, which means that you could configure a firewall for your environment, export its configuration as an XML file, and then use slightly edited versions of the file as configuration templates for other firewalls. However, note that the Panorama appliance makes building and distribution of template configurations easier than manually exporting, copying, editing, and importing XML files.

The **Import** operations transfer XML configuration files from the host running the web interface browser to the firewall. From there the XML file can be loaded as the candidate configuration or even be committed to become the running configuration.

If you load or revert to a configuration from **Configuration Management** in the web interface and then commit, only a full commit is possible. A full commit writes all changes by all administrators to the running configuration.

© 2019 Palo Alto Networks, Inc.

Configuration Operations

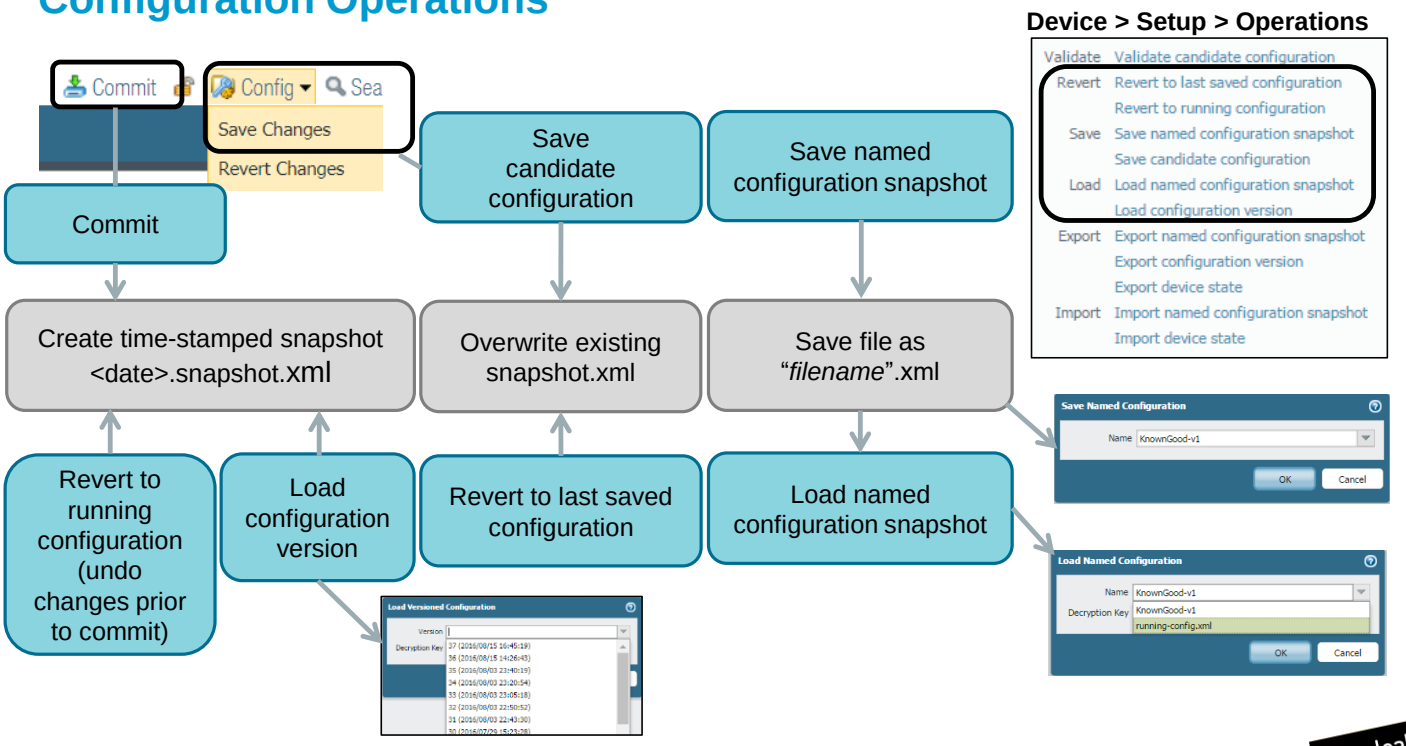


At boot time the latest configuration on disk is loaded to the candidate configuration in control-plane memory. An auto-commit copies the candidate configuration to the running configuration in control-plane memory. The running configuration in control-plane memory is then pushed to data-plane memory, where it is used to inspect and control traffic traversing the firewall.

Administrators make changes to the candidate configuration. A commit operation writes the changes to the running configuration in control-plane and data-plane memory. The firewall creates a date and timestamped version of the running configuration whenever you perform a commit. To restore a previous version of a running configuration, click **Load configuration version**.

© 2019 Palo Alto Networks, Inc.

Configuration Operations



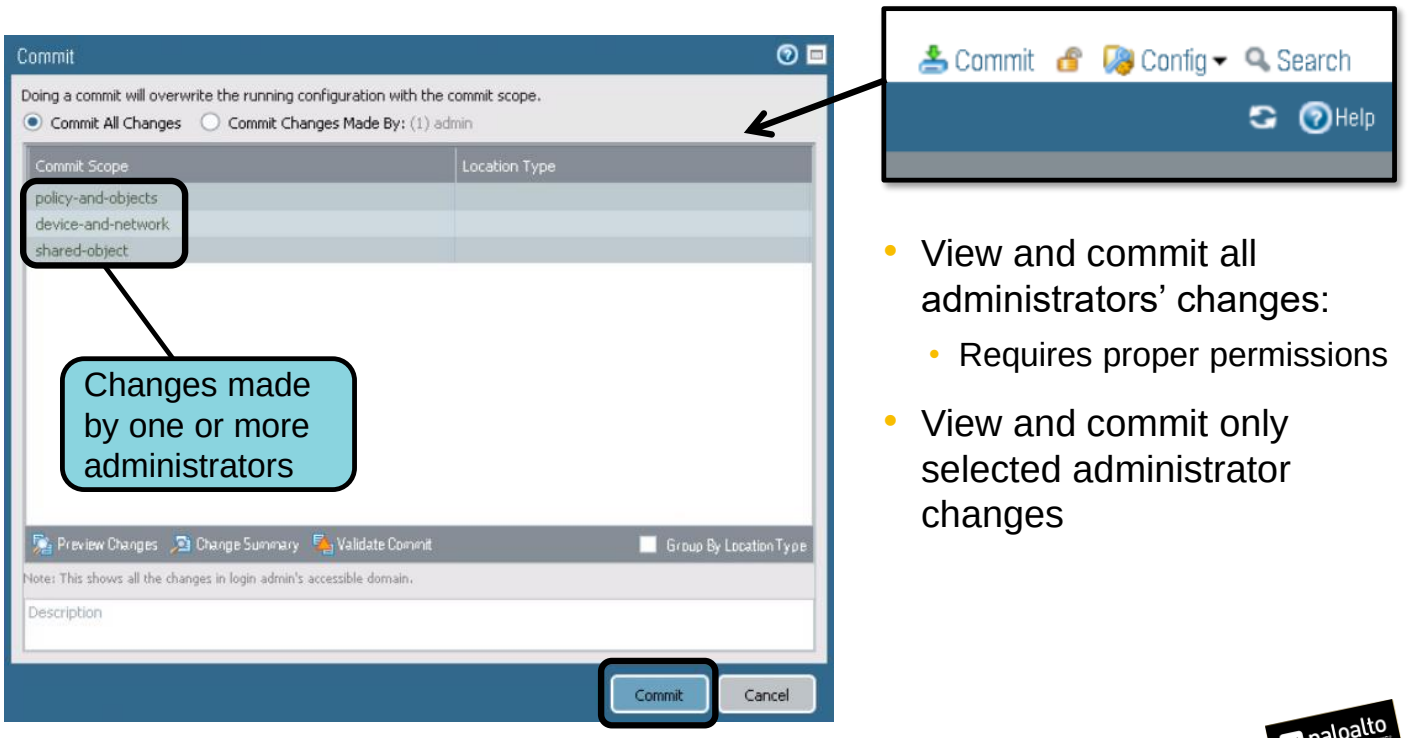
You can save a candidate configuration in several ways. Click **Save candidate configuration** to save the configuration to memory. If you continue editing and click **Save candidate configuration** again, the configuration that is saved in memory is overwritten. This saved configuration is in volatile memory and will not survive if you reboot the firewall. If you were editing and want to abort the changes since the last save, click **Revert to last saved configuration**.

You do not always have to save your changes to memory. You can save your current candidate configuration to an XML filename on disk by clicking **Save named configuration snapshot**. This saved configuration will survive a firewall reboot. You can have multiple named configurations saved on your firewall. You can click **Load named configuration snapshot** to replace the current candidate configuration with the named configuration in an XML file.

If you want to delete your current candidate configuration and start over, you can copy the running configuration to the candidate configuration by clicking **Revert to running configuration**.

© 2019 Palo Alto Networks, Inc.

Admin-Level Commit



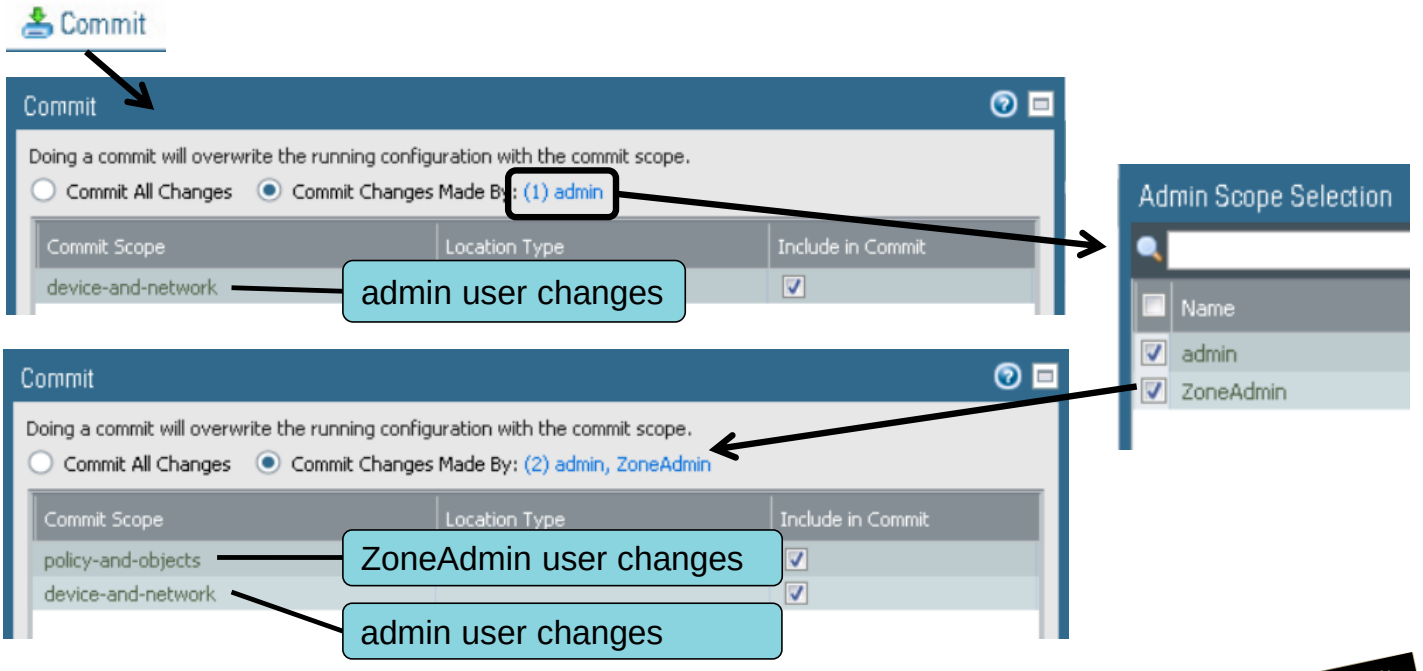
- View and commit all administrators' changes:
  - Requires proper permissions
- View and commit only selected administrator changes

Admin-level commit became available starting with PAN-OS 8.0. It enables each administrator to commit only their changes to the running configuration. Admin-level commit simplifies your configuration workflow because you do not have to coordinate commits with other administrators or be concerned about changes that other administrators have made but are not ready to have committed. In versions prior to PAN-OS 8.0, a commit operation committed all changes made by all administrators.

In the example, **Commit All Changes** is selected, which commits all changes made by all administrators. You must have the necessary privileges to perform this type of commit.

© 2019 Palo Alto Networks, Inc.

Performing a Per-Admin Commit



You can commit just *your* changes or the changes of a *select group* of other administrators. In the top example, only the changes made by the admin user would be committed. However, if you click the admin username, the web interface offers the choice to select additional administrators. In the lower example, the ZoneAdmin user was selected in addition to the admin user. As a result of this selection, changes from both the admin and ZoneAdmin users would be committed to the running configuration.

© 2019 Palo Alto Networks, Inc.

Admin-Level Save and Revert

- Save changes in progress without committing:
  - Per-admin or all changes
- Revert changes to previous saved configuration:
  - Per-admin or all changes

In every version of PAN-OS software, changes made to the current candidate configuration could be saved to a default XML file on the firewall. This capability enables you to save your current progress and continue your work later without your having to commit a partially completed configuration change. Saved changes made by any administrator are written to the same default XML file.

Starting with PAN-OS 8.0, you can save just *your* changes or the changes of a select group of other administrators to the default XML file. Each change is tagged with information about the administrator that made the change.

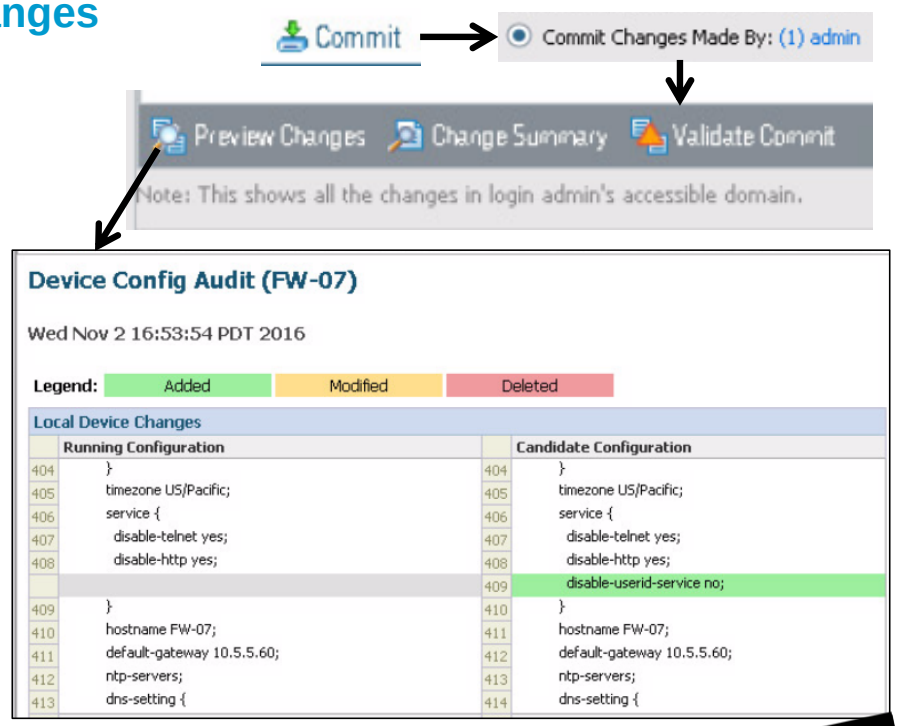
In every version of PAN-OS software, you can revert to the last saved configuration in the default XML file on the firewall's disk. This capability enables you, for example, to remove the most recent changes made since you last saved your candidate configuration.

You can revert to just *your* last saved configuration or revert to the last saved configuration of a select group of other administrators.

© 2019 Palo Alto Networks, Inc.

Preview and Validate Changes

- **Preview Changes** compares the candidate configuration to the running configuration.
- **Change Summary** lists the individual settings for which you are committing changes.
- **Validate Commit** shows any error messages that would appear during a commit.



The **Preview Changes** link opens a window that displays a side-by-side comparison of the running and candidate configurations before you commit. Differences in the configurations are color-coded to indicate which information has been added, deleted, or modified.

The **Change Summary** link lists the individual changes for which you are committing changes. The **Change Summary** lists the object's name; whether it is a shared object or for a specific virtual system; whether it is an edit, create, or delete operation; and the name of the administrator performing the commit.

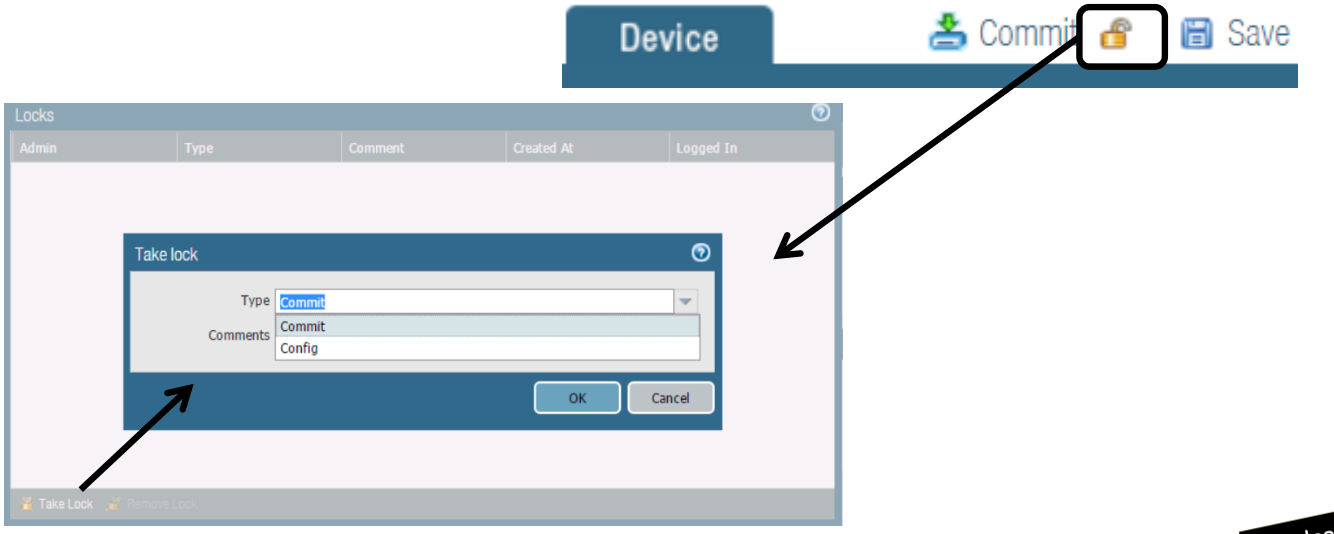
The **Validate Commit** link performs a syntactic validation and semantic validation of a firewall candidate configuration before committing it. A semantic validation determines whether the configuration is accurate and complete. Such validation substantially reduces the number of failures at commit time. The results display all warnings and errors of a full commit. Warnings do not prevent a commit, but errors do. Warnings include rule shadowing and application dependency warnings. Errors include an invalid route destination or a missing account and password that are required to query a server.

The **Preview Changes** and **Validate Commit** links display all changes by all administrators or just those changes associated with selected administrators. In the example, the **Preview Changes** window shows only the changes made to the candidate configuration by the admin user.

© 2019 Palo Alto Networks, Inc.

Transaction Locks for Multiple Admins

- Commit lock: Blocks other admins from committing the candidate configuration
- Config lock: Blocks other admins from changing the candidate configuration



The web interface supports multiple administrators. An administrator can choose to take either a **Commit** lock that prevents commit operations by another administrator, or a **Config** lock that prevents changes to the candidate configuration. You can use admin-level commits rather than take locks.

If you want administrators to automatically acquire a **Commit** lock when they log in, go to **Device** > **Setup** > **Management** > **General Settings** to configure this behavior.

Before you can take a lock, display locks, or remove a lock, first open the **Locks** window, which displays any open locks and provides choices to take or remove locks. Locks can be removed by the administrator who created them or by an administrator with superuser privileges. **Commit** and **Config** locks are released automatically when a **Commit** operation is completed.

© 2019 Palo Alto Networks, Inc.

Administrative controls

Initial system access

Configuration management

Licensing and software updates

Account administration

Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

Activate the Firewall

Step	Hardware Firewall	VM-Based Firewall
Register with Palo Alto Networks Support	Use serial number from **Dashboard**	Use emailed auth codes and purchase/order number
Activate licenses at Device > Licenses	Retrieve license keys from license server	Activate feature using authorization code
Verify update and DNS servers	Use correct update and DNS server in **Device > Setup > Services**	
Manage content updates	Get latest application and threat signatures and URL filtering database	
Install software updates	Verify OS version and install recommended version	

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 then activate the licenses for each of the subscriptions that you 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 VM-Series model that was purchased. To use the authorization code, first register the code to the Support account on the Palo Alto Networks Customer Support Portal. If you have an existing Support account, access 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 that is needed to install the VM-Series firewall.

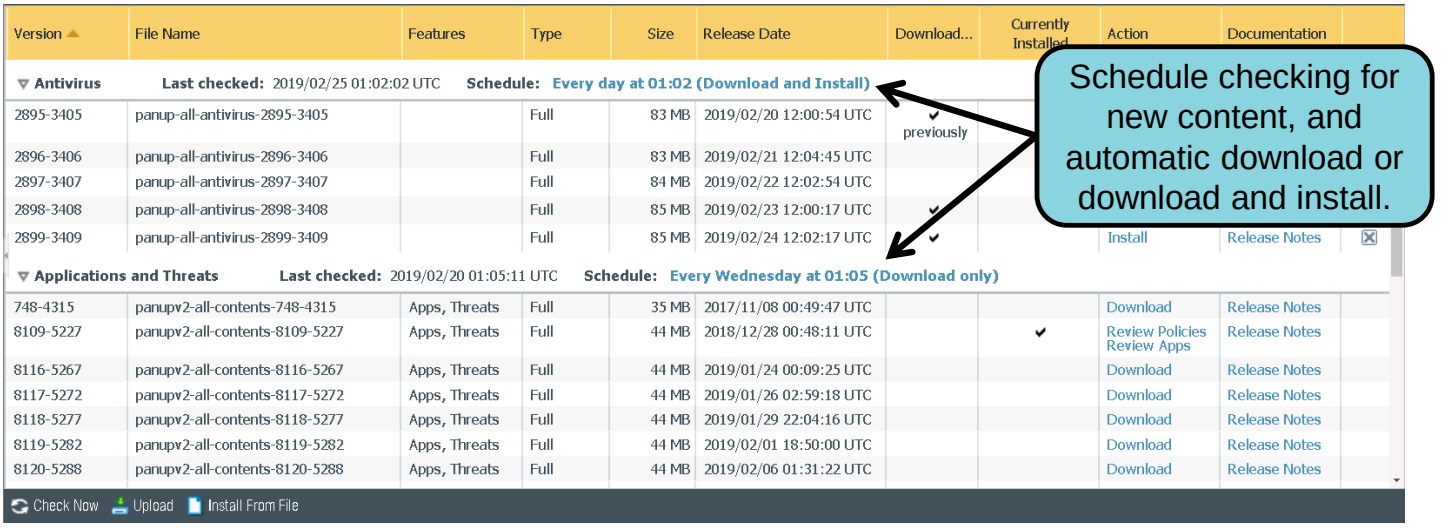
After you purchased your subscriptions you should have received an email from Palo Alto Networks customer service listing the activation code associated with each subscription. Before you can activate these licenses, you must activate your support license. Click **Device** > **Support** and then click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

With support activated, click **Device** > **Licenses** to activate your other subscriptions. There are multiple methods to activate your subscriptions. For guidance, see the *PAN-OS Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html. Activation of a WildFire® license requires a commit.

© 2019 Palo Alto Networks, Inc.

Dynamic Updates

Device > Dynamic Updates



27 | © 2019 Palo Alto Networks, Inc.

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 also can 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:

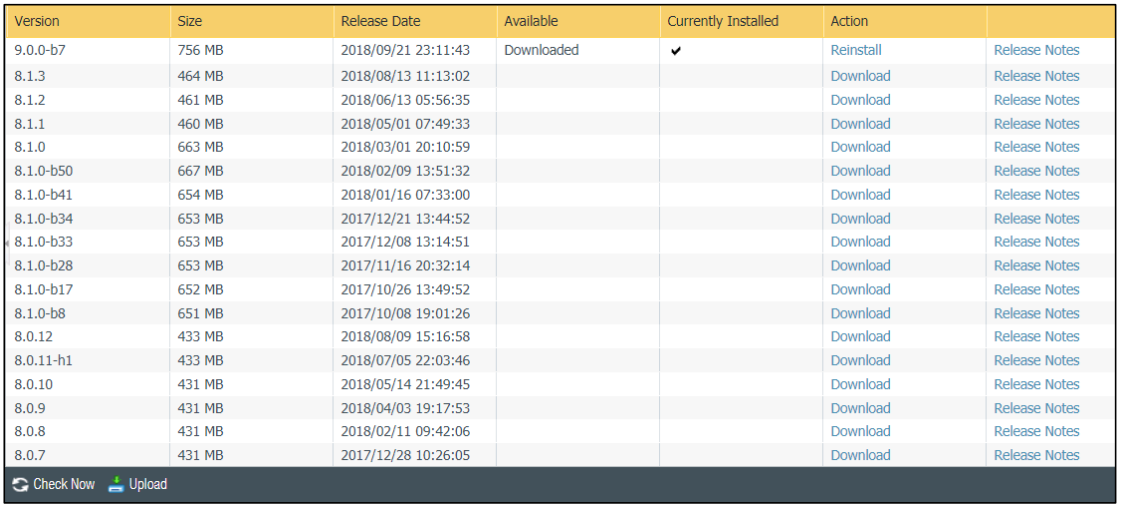
- Antivirus: daily
- Applications and Threats: weekly updates, new applications added monthly
- WildFire: approximately every five minutes

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 as frequently as every minute.

Find additional information in the *Tips for Managing Content Updates* white paper on the Knowledge Base at https://live.paloaltonetworks.com/docs/DOC-1578.

PAN-OS Software Updates

Device > Software



Version	Size	Release Date	Available	Currently Installed	Action	
9.0.0-b7	756 MB	2018/09/21 23:11:43	Downloaded	✔	Reinstall	Release Notes
8.1.3	464 MB	2018/08/13 11:13:02			Download	Release Notes
8.1.2	461 MB	2018/06/13 05:56:35			Download	Release Notes
8.1.1	460 MB	2018/05/01 07:49:33			Download	Release Notes
8.1.0	663 MB	2018/03/01 20:10:59			Download	Release Notes
8.1.0-b50	667 MB	2018/02/09 13:51:32			Download	Release Notes
8.1.0-b41	654 MB	2018/01/16 07:33:00			Download	Release Notes
8.1.0-b34	653 MB	2017/12/21 13:44:52			Download	Release Notes
8.1.0-b33	653 MB	2017/12/08 13:14:51			Download	Release Notes
8.1.0-b28	653 MB	2017/11/16 20:32:14			Download	Release Notes
8.1.0-b17	652 MB	2017/10/26 13:49:52			Download	Release Notes
8.1.0-b8	651 MB	2017/10/08 19:01:26			Download	Release Notes
8.0.12	433 MB	2018/08/09 15:16:58			Download	Release Notes
8.0.11-h1	433 MB	2018/07/05 22:03:46			Download	Release Notes
8.0.10	431 MB	2018/05/14 21:49:45			Download	Release Notes
8.0.9	431 MB	2018/04/03 19:17:53			Download	Release Notes
8.0.8	431 MB	2018/02/11 09:42:06			Download	Release Notes
8.0.7	431 MB	2017/12/28 10:26:05			Download	Release Notes

Check Now Upload

1. **Check Now** to list new software.
2. **Download** from update server or **Upload** from local machine.
3. **Install** software.

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 acquire these updates. The firewall requires 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 latest versions of the PAN-OS software available from Palo Alto Networks. Read the release notes for each version, then select the version to download and install. A support license is required for the download. Software updates require a firewall reboot.

When you upgrade, typically you must download the x.0 base release before you install the maintenance or feature release. For example, to upgrade from 6.1.9 to 7.0.1, download 7.0.0 and 7.0.1. When you install 7.0.1, the 7.0 software is automatically installed.

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. When 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 that is 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.

© 2019 Palo Alto Networks, Inc.

Administrative controls

Initial system access

Configuration management

Licensing and software updates

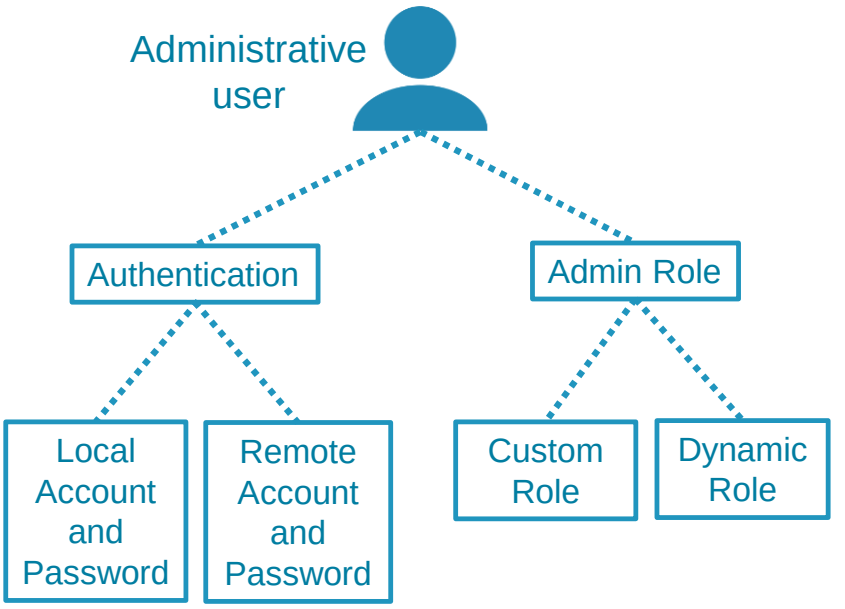
Account administration

Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

Administrator Account and Role Repositories

- Firewall can authenticate locally or remotely defined administrators.
- Each administrative account is assigned a role with specific privileges.
- Administrator actions are logged in the Configuration and System logs:
  - **Monitor > Logs**



By default, only the predefined *admin* account has access to the firewall. However, you can add administrator accounts to the firewall for delegation and auditing purposes. Each additional administrator account you create can have its own set of administrative privileges. Specify administrative privileges by creating one or more Admin Role Profiles with specific sets of privileges, and then assign an Admin Role Profile to each administrator account.

PAN-OS software provides flexibility when administrator accounts and admin roles are created. You can create and manage accounts and admin roles locally on the firewall or incorporate a supported authentication, authorization, and accounting service. PAN-OS software supports remote user accounts in Active Directory, Kerberos, LDAP, RADIUS, and TACACS+. PAN-OS software supports remote role assignment in RADIUS or TACACS+ using Vendor-Specific Attributes (VSAs).

No matter which user makes changes to the running configuration, all changes are logged in the firewall's Configuration and System logs. The System log records the time when an administrator logs in, and the Configuration log records any changes that they make.

To create a local administrator account:

1. Create an Admin Role Profile.
2. Create a local administrator account.

To create a non-local administrator account:

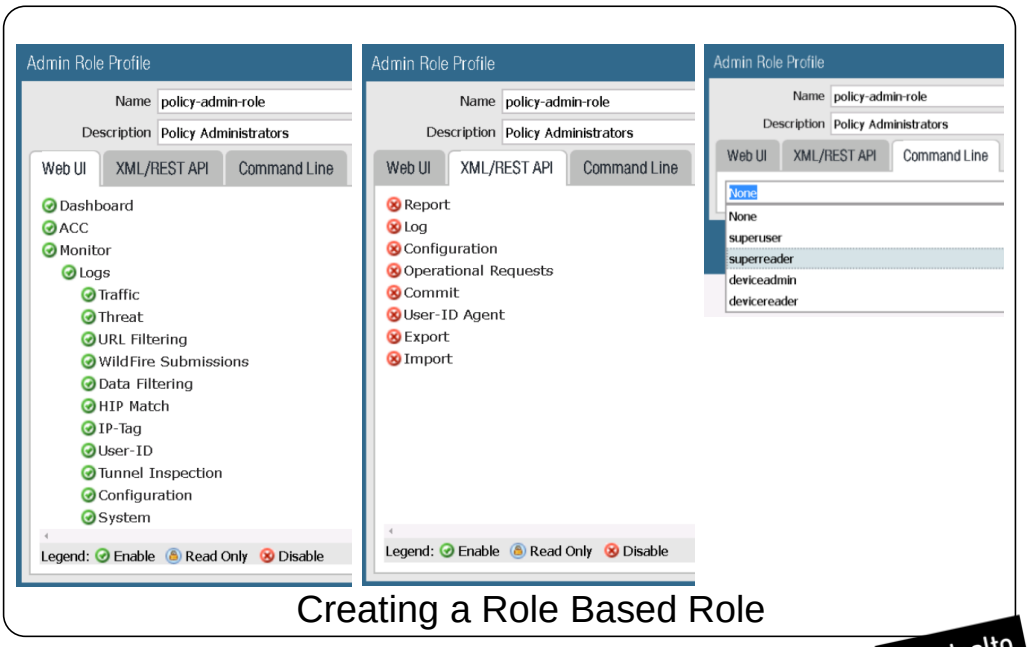
1. Create an Admin Role Profile.
2. Create a Server Profile.
3. Create an Authentication Profile.
4. Create an authentication sequence (optional).
5. Create a non-local administrator account.

© 2019 Palo Alto Networks, Inc.

Creating an Administrator Role

- Roles define administrative privileges on the firewall.
- Two types:
  - Dynamic: Predefined permission sets:
    - superuser
    - superuser (read only)
    - device administrator
    - device administrator (read only)
  - Role Based: Custom permission sets

Device > Admin Roles > Add



Creating a Role Based Role

The two types of Admin role profiles are predefined Dynamic Profiles and administrator-defined Role Based Profiles.

There are six Dynamic Profiles with predefined privileges labeled superuser, superuser (read only), device administrator, device administrator (read only), and, if your firewall is capable of virtual systems, virtual system administrator and virtual system administrator (read only). These are Dynamic Profiles because they are updated automatically when new capabilities are added to the PAN-OS software. The primary differences, aside from some roles being read-only, are that a device administrator cannot manage administrator accounts or create new virtual systems, and a virtual system administrator can manage only virtual systems assigned to them.

Use the **Admin Roles** page to define Role Based Profiles that specify sets of custom privileges that you assign to administrative user accounts on the firewall.

You define three types of privileges in a Role Based Profile: Web UI, XML/REST API, and CLI. These permissions are represented by three tabs in the web interface, which you use to assign very granular privileges to a Role Based Profile.

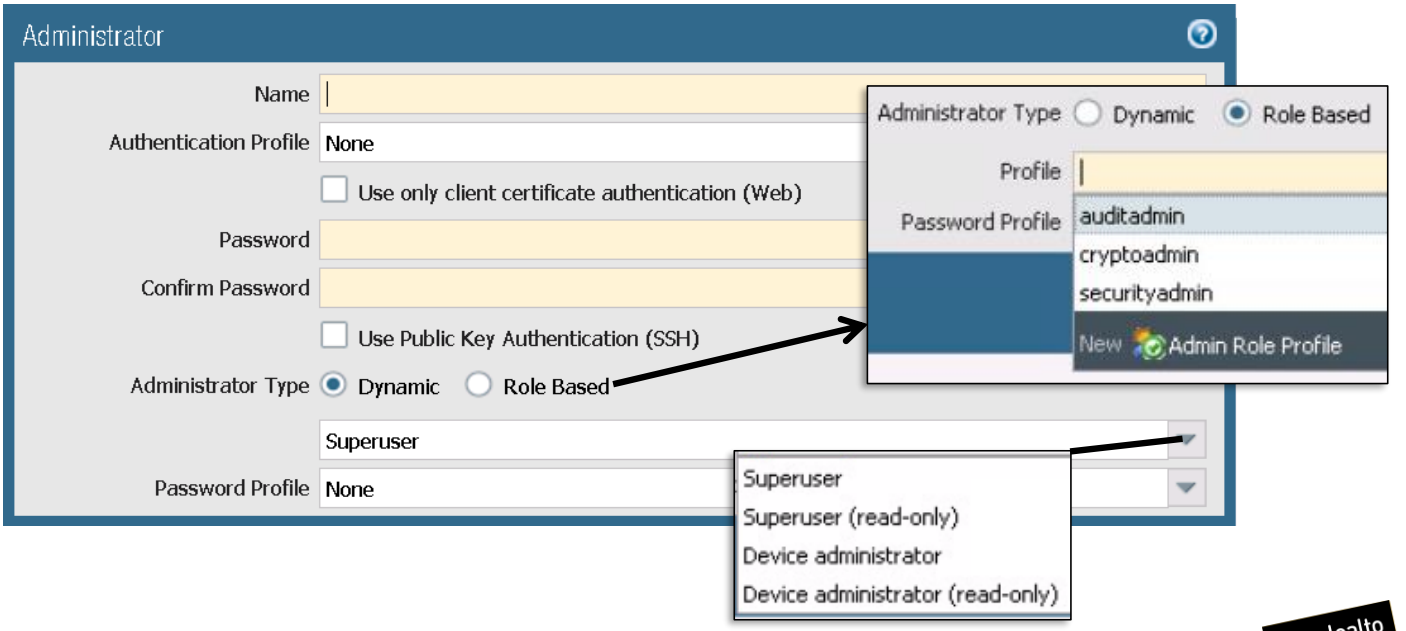
Role-based privileges on the **Command Line** tab are predefined. No customization is possible. The privileges are:

- None: No access granted to the CLI
- superuser: All access to all options of the firewall
- superreader: Read-only access to all options of the firewall
- deviceadmin: Same as superuser, except for no creation of administrative accounts
- devicereader: Same as deviceadmin, except for read-only

© 2019 Palo Alto Networks, Inc.

Creating a Local Administrator Account

Device > Administrators > Add



Use the web interface to create an administrator account that is local to the firewall. The privileges of the administrator account are determined by the role profile assigned to the account. The web interface assumes a local account and prompts for a password when you do not select an Authentication Profile.

In this example a Dynamic Profile is selected, which means that user rights are defined using one of the predefined roles. These roles affect the web interface and the CLI. The following is a brief description of the predefined roles:

- superuser: All access to all options of the firewall
- superuser (read only): Read-only access to all options of the firewall
- device administrator: Full access to the firewall except for creation of virtual systems and administrative accounts
- device administrator (read only): Read-only access to the firewall except for viewing other administrative accounts
- virtual system administrator: Full access to a specific virtual system
- virtual system administrator (read only): Read-only access to a specific virtual system

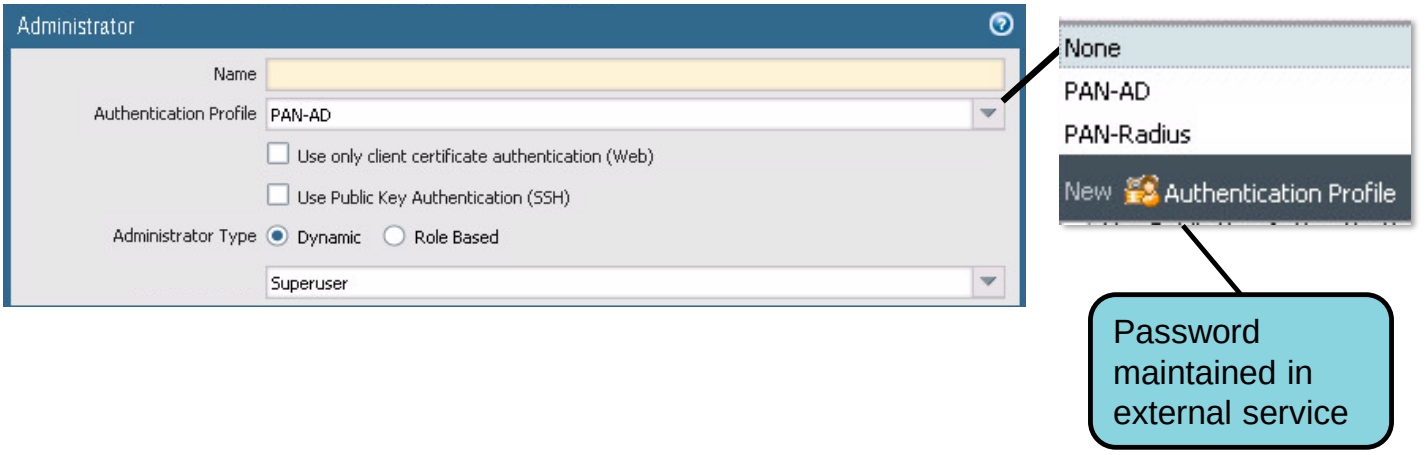
To ensure that locally stored passwords are strong passwords and are reset periodically, PAN-OS software enables you to set global minimum password complexity requirements and password aging values at **Device > Setup > Management > Minimum Password Complexity**. By default there are no minimum requirements and password aging is not enabled.

Those administrator accounts whose passwords might require more frequent resets to meet organizational or legal requirements can be assigned a Password Profile. A Password Profile specifies password aging values that override the global password aging values. Configure Password Profiles at **Device > Password Profiles**.

© 2019 Palo Alto Networks, Inc.

Creating a Non-Local Administrator Account

Device > Administrators > Add



You may use the web interface to create administrator accounts whose passwords are maintained in a supported external service. For example, the account password might be maintained in Active Directory. To indicate that the account password is maintained in a supported external service, create an Authentication Profile that connects to an external service and then specify that Authentication Profile when you create an administrator account.

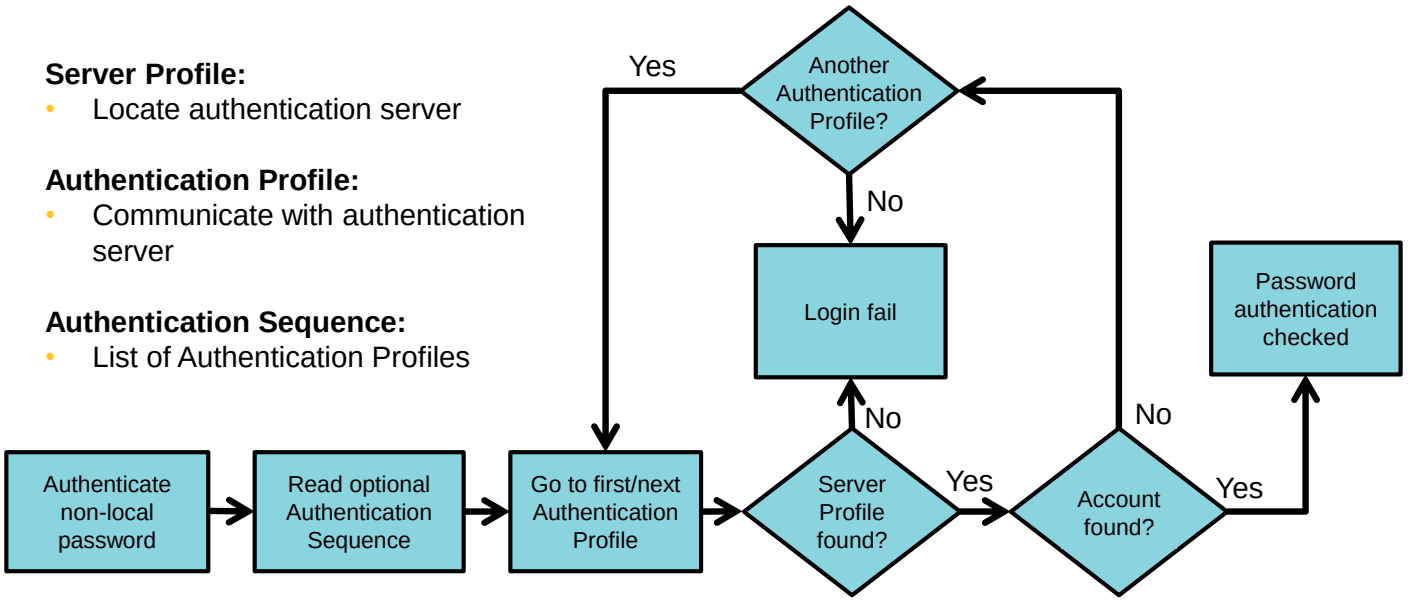
© 2019 Palo Alto Networks, Inc.

Firewall Authentication of Non-Local Passwords

Server Profile:
- Locate authentication server

Authentication Profile:
- Communicate with authentication server

Authentication Sequence:
- List of Authentication Profiles



Non-local account passwords must be authenticated through their external authentication service. Before you can access an external authentication service, you must create the appropriate profiles on the firewall. An Authentication Profile contains the information necessary to authenticate an administrator account with an external authentication service after one of the service's servers has been located. An Authentication Profile uses a Server Profile, which you have created, to locate an external authentication service's servers. You configure a Server Profile with a list of an external authentication service's servers.

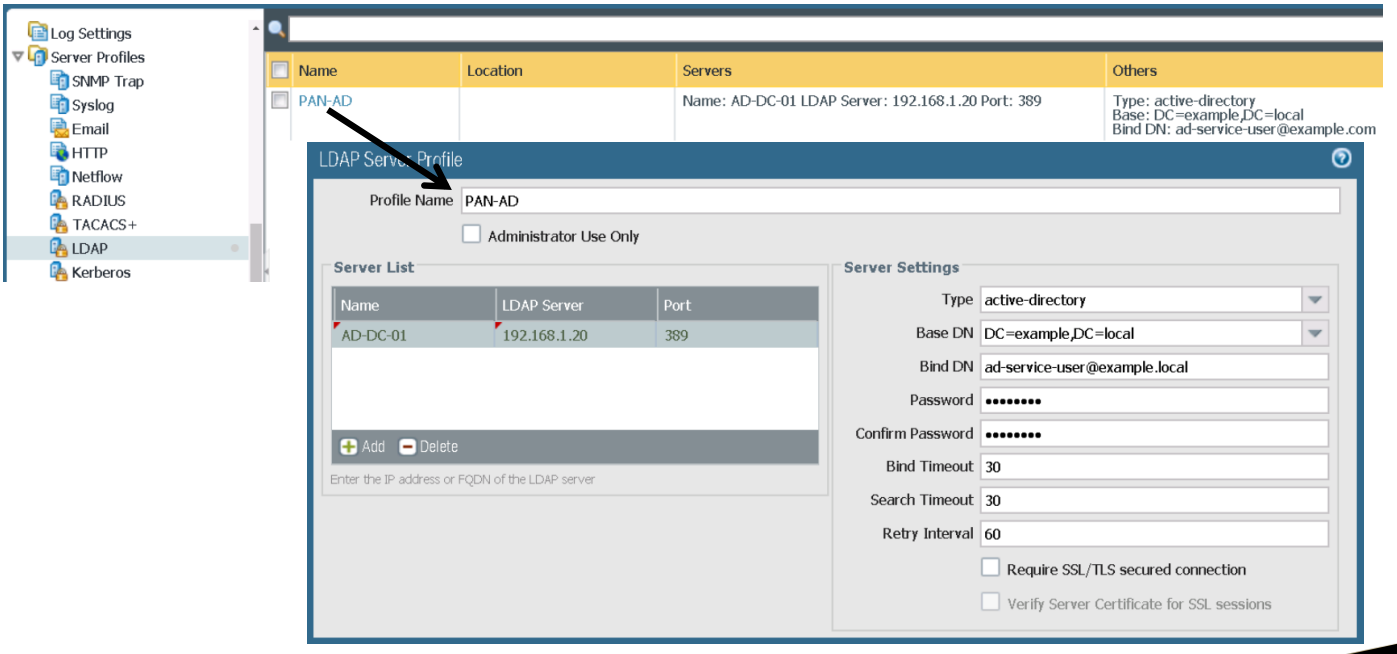
A firewall can consult multiple external services to authenticate an account. You specify an ordered list of Authentication Profiles by adding them to an optional Authentication Sequence on the firewall. If you have created an Authentication Sequence, then specify the Authentication Sequence in place of an Authentication Profile when you add a user account on the firewall.

The flowchart shows how a firewall authenticates a non-local account. If the administrator account specifies an Authentication Sequence, then the firewall attempts to authenticate the account using the ordered list of specified Authentication Profiles. Each Authentication Profile specifies a Server Profile with a list of servers for the external authentication service. The firewall connects to each external service until either the user is located or no Authentication Profiles are left. If no Authentication Profiles are left, then the login attempt fails.

© 2019 Palo Alto Networks, Inc.

Configuring Server Profiles

Device > Server Profiles



Server Profiles define connections that the firewall can make to external servers of specific types. For authentication purposes, specify Kerberos, LDAP, RADIUS, SAML, or TACACS+ servers.

Authentication Profiles require Server Profiles to validate login information for administrator accounts that are not created on the firewall.

© 2019 Palo Alto Networks, Inc.

Configuring Authentication Profiles

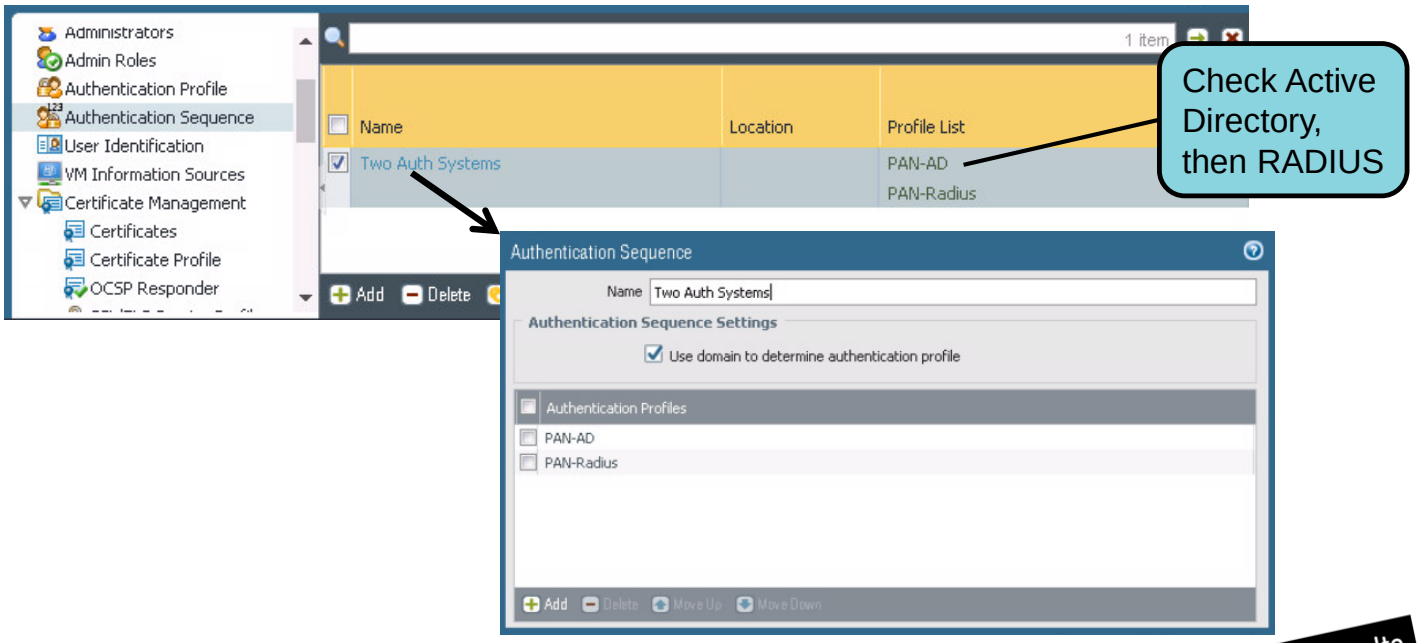
Device > Authentication Profiles

An Authentication Profile specifies which authentication server and settings are used to authenticate an administrator account. You specify an Authentication Profile when you create an administrator account where the account name and password are maintained on an external service.

© 2019 Palo Alto Networks, Inc.

Configuring an Authentication Sequence

Device > Authentication Sequence > Add



An Authentication Sequence is optional if you have defined multiple external services. First create the Authentication Sequence that lists, in order, the Authentication Profiles that should be checked to authenticate an administrator account. The Authentication Profiles should be in order from the most preferred method listed first to the least preferred method listed last. You can use the **Move Up** or **Move Down** button to change the order of the listed profiles.

If you have configured an Authentication Sequence, the firewall checks against each profile in sequence until one profile successfully authenticates the user. A user is denied access only if authentication fails for all the profiles in the sequence.

© 2019 Palo Alto Networks, Inc.

Administrative controls

Initial system access

Configuration management

Licensing and software updates

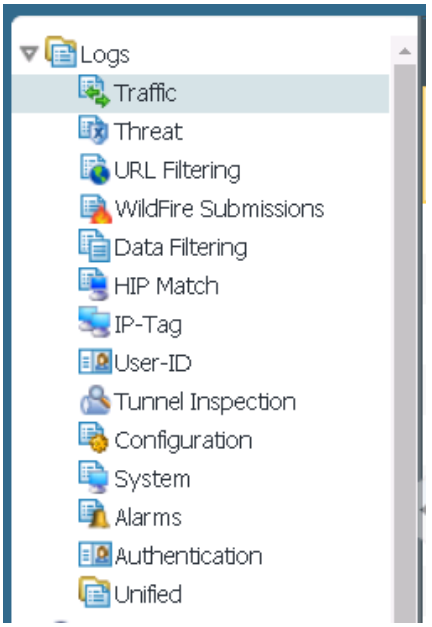
Account administration

Viewing and filtering logs

© 2019 Palo Alto Networks, Inc.

Accessing Firewall Logs

Monitor > Logs



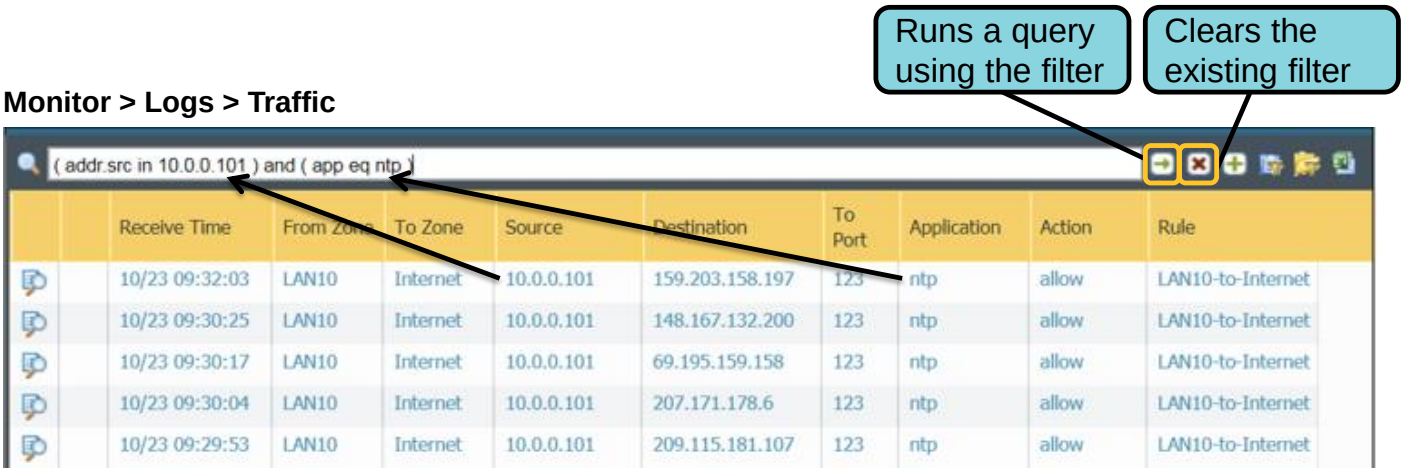
- Each firewall maintains multiple log types.

To display firewall logs, select **Monitor > Logs**. The available log types are listed in the web interface.

© 2019 Palo Alto Networks, Inc.

Constructing a Log Filter

- Click any link in the log listing to add that item as a log filter option.

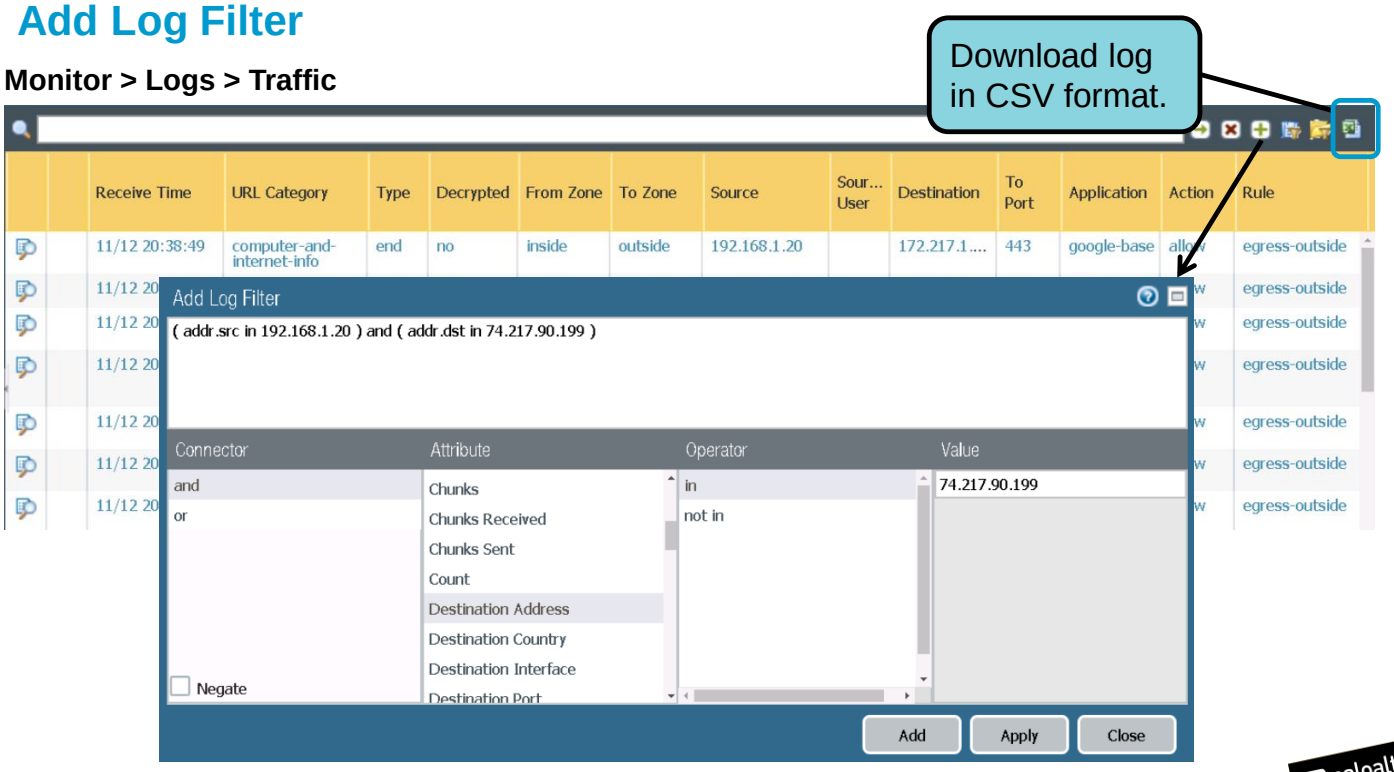


Click any link in the log listing to add that item as a log filter option.

© 2019 Palo Alto Networks, Inc.

Add Log Filter

Monitor > Logs > Traffic



The filter bar allows administrators to display only the lines in the log that match specified criteria.

To enter a value, click a column entry or build a filter using the **Add Log Filter** interface.

Frequently used filters can be saved and reused.

© 2019 Palo Alto Networks, Inc.

Module Summary

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

- Connect to the firewall and log in as admin
- Configure the network settings for the management interface port
- Describe the difference between the running config and the candidate config
- Configure dynamic firewall updates to update the applications and threats databases
- Create a local firewall administrative account
- Access the firewall logs

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

© 2019 Palo Alto Networks, Inc.

Questions?

Review Questions

1. Palo Alto Networks firewalls are built with a dedicated out-of-band management port that has which three attributes? (Choose three.)
   a. Labeled MGT by default.
   b. Passes only management traffic for the device and cannot be configured as a standard traffic port.
   c. Administrators use the out-of-band management port for direct connectivity to the management plane of the firewall.
   d. Cannot be configured to use DHCP.
2. Which three statements are true regarding the candidate configuration? (Choose three.)
   a. You can roll back the candidate configuration by pressing the **Undo** button.
   b. You can revert the candidate configuration to the running configuration.
   c. Clicking **Save** creates a copy of the current candidate configuration.
   d. Choosing **Commit** updates the running configuration with the contents of the candidate configuration.
3. True or false? Firewall administrator accounts can be individualized for user needs, granting or restricting permissions as appropriate?
   a. true
   b. false
4. Firewall administration can be done using which four interfaces? (Choose four.)
   a. web interface
   b. Panorama
   c. command line interface
   d. Java API
   e. XML API
5. True or false? Service routes can be used to configure an in-band port to access external services.
   a. true
   b. false

Initial Configuration Lab (Pages 11-23 in the Lab Guide)

- Load a firewall lab configuration file
- Create an admin role
- Create an administrator account
- Manage commit locks
- Manage external firewall services
- Schedule dynamic updates

© 2019 Palo Alto Networks, Inc.

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, b, c
2. b, c, d
3. a (true)
4. a, b, c, e
5. a (true)

© 2019 Palo Alto Networks, Inc.

This page intentionally left blank

© 2019 Palo Alto Networks, Inc.