

CONNECT TO THE MANAGEMENT NETWORK



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

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
- Activate firewall licenses and update PAN-OS® software
- Identify the purpose and location of firewall configuration skillets





Initial system access

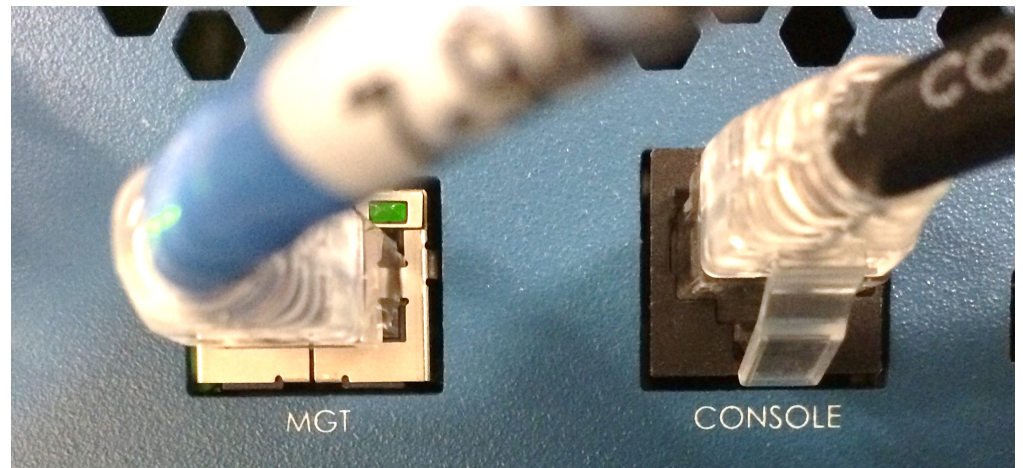
Configure management network settings

Activate a firewall, and manage licenses and software

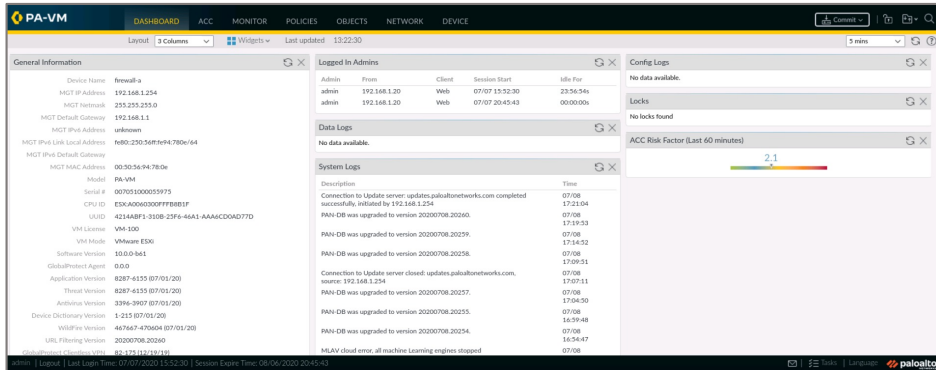


Initial Access to the Firewall

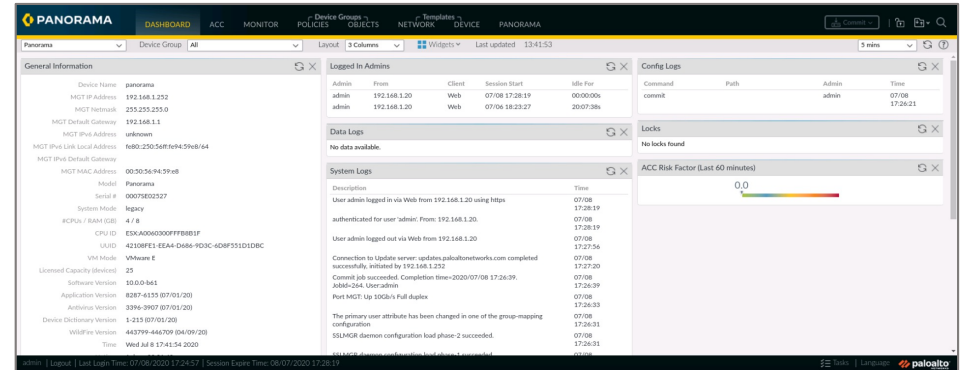
- Initial configuration must be performed using either:
 - Dedicated out-of-band management Ethernet interface (MGT)
 - Serial console connection
- Default MGT IP addressing:
 - Most firewall models: 192.168.1.1/24
 - VM-Series firewalls: DHCP client
- Predefined administrator:
 - Username: admin
 -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



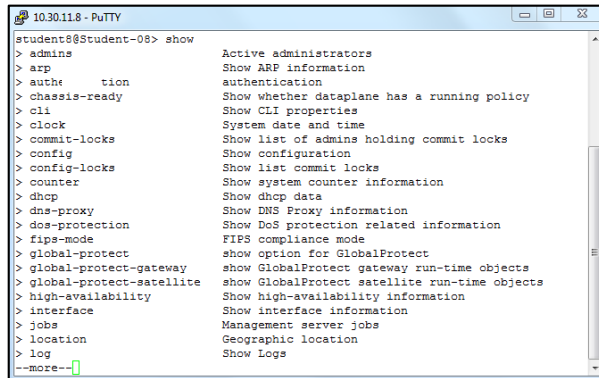
Administrative Access Tools



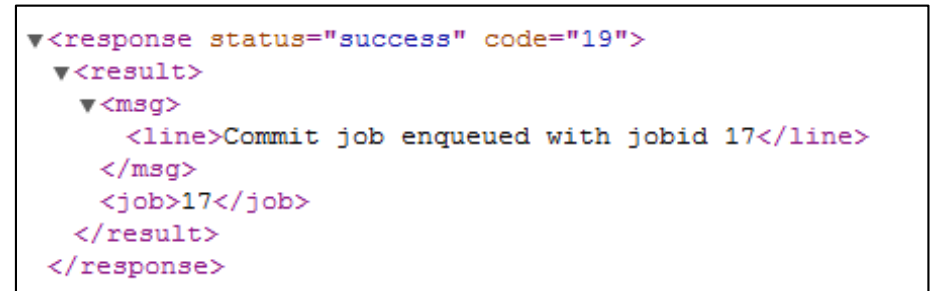
Web Interface



Panorama

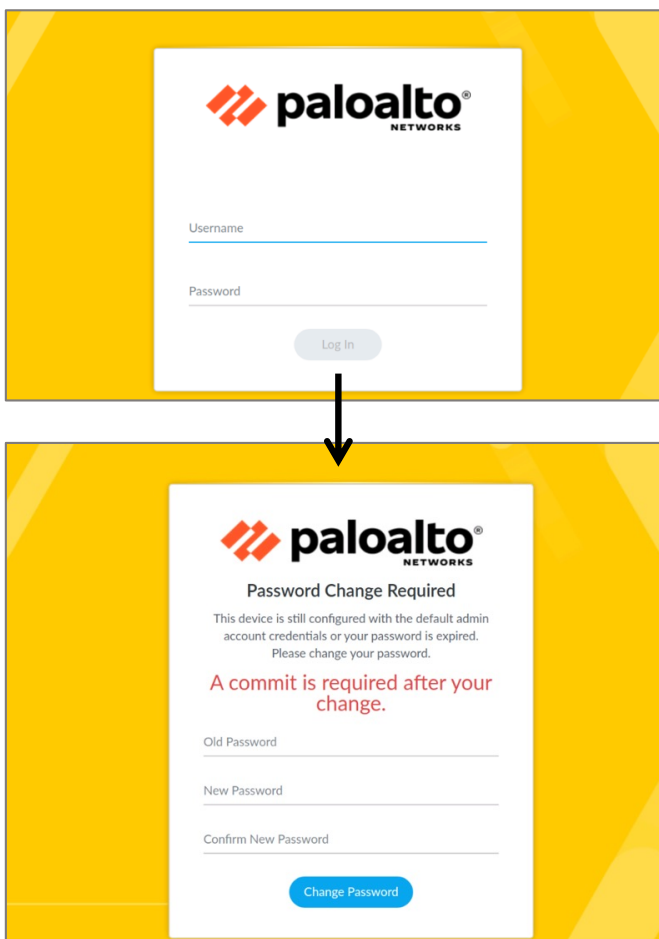


SSH/Console CLI



REST/XML API

Initial Login to the Web Interface



The image displays two screenshots of the Palo Alto Networks web interface. The top screenshot shows the initial login page with the Palo Alto Networks logo, fields for Username and Password, and a Log In button. An arrow points down to the bottom screenshot, which shows the 'Password Change Required' page. This page includes a message about default credentials, a red warning 'A commit is required after your change.', and fields for Old Password, New Password, and Confirm New Password, with a Change Password button.

- 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

Web Interface

The screenshot displays the Palo Alto Networks PA-VM web interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. A 'Commit' button with a dropdown arrow is located in the top right corner. Below the navigation bar, the interface is divided into several sections. On the left, the 'General Information' section lists device details for 'firewall-a'. In the center, the 'Data Logs' and 'System Logs' sections are visible. On the right, the 'Config Logs' and 'ACC Risk Factor' sections are shown. A 'Logout' button is located in the bottom left corner. A 'Tasks' button and a 'Language' setting are located in the bottom right corner. A help portal icon is also present in the top right corner.

Functional category tabs

Commit configuration changes.

Help portal

Logout button

Tasks button and Language setting

| Description | Time |
|--|----------------|
| User admin logged in via Web from 192.168.1.20 using https | 07/08 17:53:05 |
| authenticated for user 'admin'. From: 192.168.1.20. | 07/08 17:53:05 |
| Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254 | 07/08 17:51:35 |
| PAN-DB was upgraded to version 20200708.20268. | 07/08 17:50:00 |
| User admin logged out via Web from 192.168.1.20 | 07/08 |

Web Interface Editing Guidance

The screenshot displays the 'NAT Policy Rule' configuration page. At the top, there are three tabs: 'General' (selected and underlined in red), 'Original Packet', and 'Translated Packet'. A 'Contextual help' button with a question mark icon is located in the top right corner. The 'General' tab contains several fields: 'Name' (a red-outlined text box), 'Description' (a large text area), 'Group Rules By Tag' (a dropdown menu set to 'None'), 'NAT Type' (a dropdown menu set to 'ipv4'), and 'Audit Comment' (a text area). Below the 'Audit Comment' field is a link labeled 'Audit Comment Archive'. At the bottom right, there are 'OK' and 'Cancel' buttons. The 'OK' button is disabled (grayed out). Four callout boxes provide guidance: 1. A box pointing to the red underline on the 'General' tab says 'Red underline shows tabs where information is required.' 2. A box pointing to the red outline on the 'Name' field says 'Red highlights indicate required fields.' 3. A box pointing to the disabled 'OK' button says 'OK button is unavailable if required information is missing or is invalid.'

NAT Policy Rule

Contextual help

General | Original Packet | Translated Packet

Name

Description

Group Rules By Tag None

NAT Type ipv4

Audit Comment

[Audit Comment Archive](#)

OK Cancel

Red underline shows tabs where information is required.

Red highlights indicate required fields.

OK button is unavailable if required information is missing or is invalid.

Initial system access



Configure management network settings

Activate a firewall, and manage licenses and software



MGT Interface Configuration: Web Interface

Device > Setup > Interfaces > Management

Management Interface Settings

IP Type ☒ Static ☐ DHCP Client

IP Address

Netmask

Default Gateway

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed

MTU

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 |
|---|-----------------------------------|
| <input type="checkbox"/> 192.168.0.0/16 | Mgt access from these hosts only. |

+ Add - Delete

OK Cancel

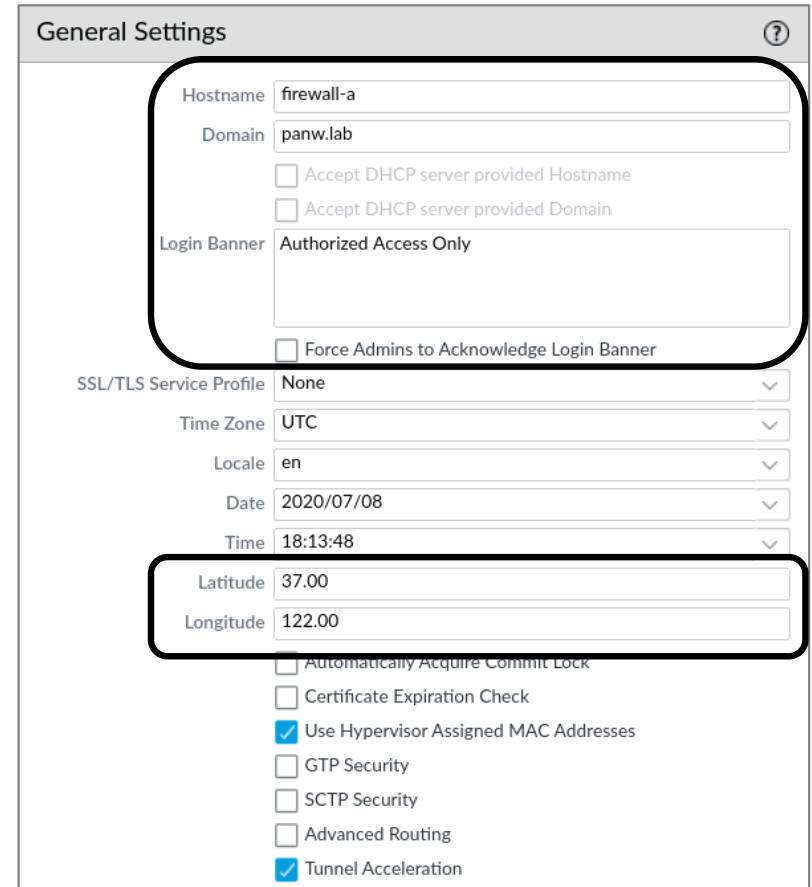
Minimum configuration requires IP address, netmask, and default gateway.

Restrict administrative access to specific IP addresses.

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.

Device > Setup > Management

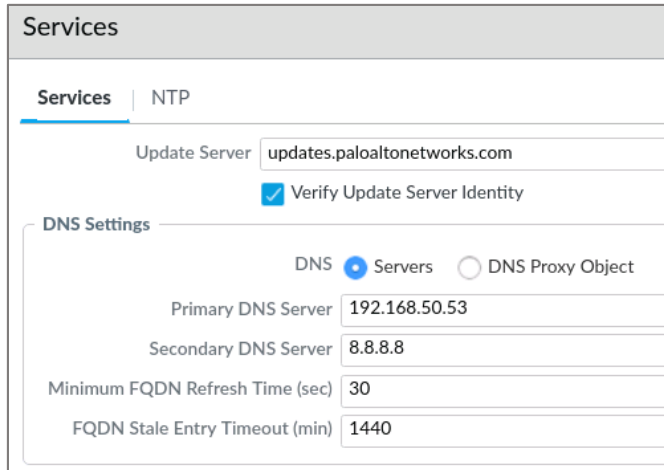


The screenshot displays the 'General Settings' configuration page for a Palo Alto Networks firewall. The page is titled 'General Settings' with a help icon. It contains several configuration fields and checkboxes. Two areas are highlighted with red rectangles: the top section containing Hostname, Domain, and Login Banner settings, and the bottom section containing Latitude and Longitude coordinates. The Hostname is 'firewall-a' and the Domain is 'panw.lab'. The Login Banner is set to 'Authorized Access Only'. The SSL/TLS Service Profile is 'None', Time Zone is 'UTC', Locale is 'en', Date is '2020/07/08', and Time is '18:13:48'. The Latitude is '37.00' and the Longitude is '122.00'. Below these, there are several checkboxes: 'Automatically Acquire Commit Lock' (unchecked), 'Certificate Expiration Check' (unchecked), 'Use Hypervisor Assigned MAC Addresses' (checked), 'GTP Security' (unchecked), 'SCTP Security' (unchecked), 'Advanced Routing' (unchecked), and 'Tunnel Acceleration' (checked).

| Field | Value |
|--|-------------------------------------|
| Hostname | firewall-a |
| Domain | panw.lab |
| Accept DHCP server provided Hostname | <input type="checkbox"/> |
| Accept DHCP server provided Domain | <input type="checkbox"/> |
| Login Banner | Authorized Access Only |
| Force Admins to Acknowledge Login Banner | <input type="checkbox"/> |
| SSL/TLS Service Profile | None |
| Time Zone | UTC |
| Locale | en |
| Date | 2020/07/08 |
| Time | 18:13:48 |
| Latitude | 37.00 |
| Longitude | 122.00 |
| Automatically Acquire Commit Lock | <input type="checkbox"/> |
| Certificate Expiration Check | <input type="checkbox"/> |
| Use Hypervisor Assigned MAC Addresses | <input checked="" type="checkbox"/> |
| GTP Security | <input type="checkbox"/> |
| SCTP Security | <input type="checkbox"/> |
| Advanced Routing | <input type="checkbox"/> |
| Tunnel Acceleration | <input checked="" type="checkbox"/> |

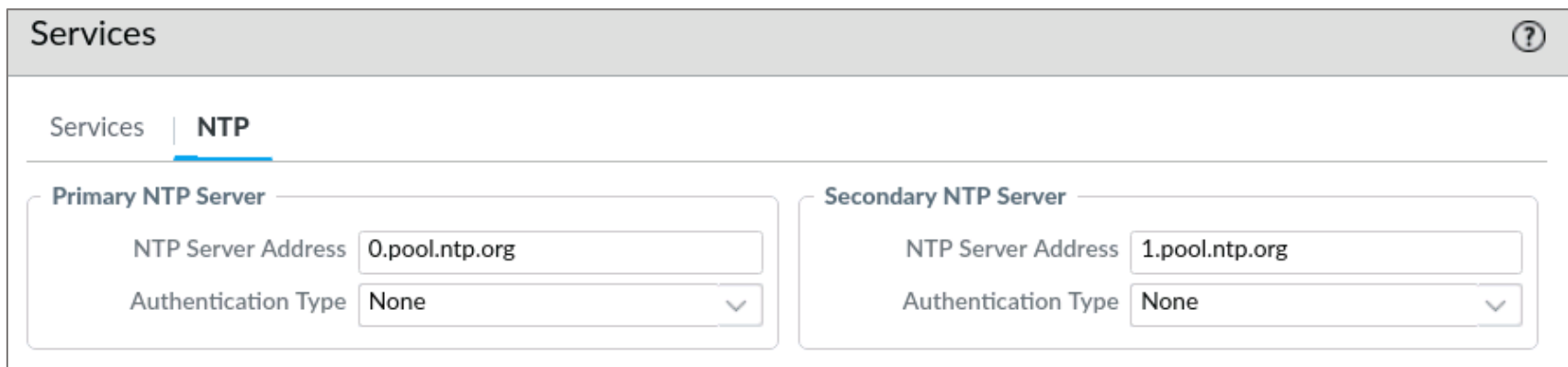
Configure Access to DNS and NTP Services

Device > Setup > Services



The screenshot shows the 'Services' configuration page with the 'DNS' tab selected. The 'Update Server' is set to 'updates.paloaltonetworks.com' and 'Verify Update Server Identity' is checked. Under 'DNS Settings', 'Servers' is selected. The 'Primary DNS Server' is '192.168.50.53', the 'Secondary DNS Server' is '8.8.8.8', the 'Minimum FQDN Refresh Time (sec)' is '30', and the 'FQDN Stale Entry Timeout (min)' is '1440'.

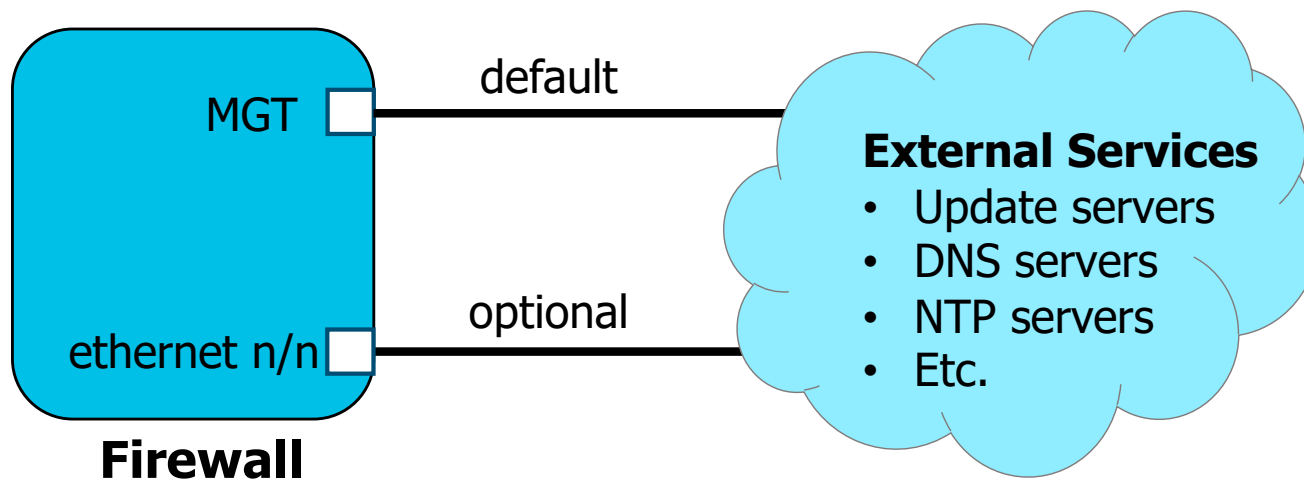
- DNS server configuration is required to reach update servers.
- NTP client configuration is optional but is recommended.



The screenshot shows the 'Services' configuration page with the 'NTP' tab selected. Under 'Primary NTP Server', the 'NTP Server Address' is '0.pool.ntp.org' and the 'Authentication Type' is 'None'. Under 'Secondary NTP Server', the 'NTP Server Address' is '1.pool.ntp.org' and the 'Authentication Type' is 'None'.

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.”



Configure Service Routes

Device > Setup > Services > Service Route Configuration

The screenshot shows the 'Service Route Configuration' window. At the top, there are radio buttons for 'Use Management Interface for all' and 'Customize' (which is selected). Below this are tabs for 'IPv4', 'IPv6', and 'Destination'. A table lists various services with checkboxes and default source settings. The 'DNS' service is highlighted, and a modal titled 'Service Route Source' is open, showing 'ethernet1/1' as the source interface and '203.0.113.20/24' as the source address. An arrow points from the 'DNS' row in the table to the modal. At the bottom of the table, a button labeled 'Set Selected Service Routes' is highlighted with a red box.

Service Route Configuration

☐ Use Management Interface for all ☒ Customize

IPv4 | IPv6 | Destination

| SERVICE | SOURCE INTERFACE | SOURCE ADDRESS |
|--|------------------|----------------|
| <input type="checkbox"/> AutoFocus | Use default | Use default |
| <input type="checkbox"/> CRL Status | Use default | Use default |
| <input type="checkbox"/> Dataplane | Use default | Use default |
| <input type="checkbox"/> DDNS | Use default | Use default |
| <input type="checkbox"/> Panorama pushed updates | Use default | Use default |
| <input type="checkbox"/> DNS | Use default | Use default |
| <input type="checkbox"/> External Dynamic Lists | Use default | Use default |
| <input type="checkbox"/> Email | Use default | Use default |
| <input type="checkbox"/> HSM | Use default | Use default |
| <input type="checkbox"/> HTTP | Use default | Use default |
| <input type="checkbox"/> IoT | Use default | Use default |
| <input type="checkbox"/> Kerberos | Use default | Use default |
| <input type="checkbox"/> LDAP | Use default | Use default |

Set Selected Service Routes

Service Route Source

Source Interface: ethernet1/1

Source Address: 203.0.113.20/24

OK Cancel

Initial system access

Configure management network settings



Activate a firewall, and manage licenses and software



Activate a Firewall

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

Manage Firewall Licenses

Device > Licenses

PA-VM

Date Issued

February 14, 2019

Date Expires

Never

Description

Standard VM-100

DNS Security

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

Palo Alto Networks DNS Security License

GlobalProtect Portal

Date Issued

February 14, 2019

Date Expires

Never

Description

GlobalProtect Portal License

Premium

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

24 x 7 phone support; advanced replac

WildFire License

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

WildFire signature feed, integrated WildFire logs, WildFire API

License Management

Retrieve license keys from license server

Activate feature using authorization code

Manually upload license key

Deactivate VM

Upgrade VM capacity

AutoFocus Device License

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

AutoFocus Device License

GlobalProtect Gateway

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

GlobalProtect Gateway License

PAN-DB URL Filtering

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

Palo Alto Networks URL Filtering License

Yes

Threat Prevention

Date Issued

February 14, 2019

Date Expires

February 14, 2023

Description

Threat Prevention

Logging Service

Date Issued

March 21, 2019

Date Expires

February 14, 2023

Description

Device Logging Service



Log Storage TB

{saas_quantity}

Retrieve, activate, upload, deactivate, or upgrade licenses.

PAN-OS Software Updates

Device > Software

| VERSION ▾ | SIZE | RELEASE DATE | DOWNLOADED | CURRENTLY INSTALLED | ACTION | | |
|---|--------|---------------------|------------|---------------------|-----------|-------------------------------|---|
| 10.0.0 | 806 MB | 2020/07/01 13:11:26 | ✓ | ✓ | Reinstall | Release Notes | |
| 9.2.0-b46 | 793 MB | 2020/06/01 11:55:47 | ✓ | | Install | Release Notes | ☒ |
| 9.2.0-b36 | 796 MB | 2020/05/06 04:18:05 | | | Download | Release Notes | |
| 9.2.0-b30 | 788 MB | 2020/04/06 15:29:53 | | | Download | Release Notes | |
| 9.2.0-b22 | 782 MB | 2020/03/03 16:04:41 | | | Download | Release Notes | |
| 9.2.0-b17 | 782 MB | 2020/02/07 13:59:59 | | | Install | | ☒ |
| 9.1.3-h1 | 381 MB | 2020/06/30 15:08:51 | | | Download | Release Notes | |
| 9.1.3 | 381 MB | 2020/06/23 12:22:15 | | | Download | Release Notes | |
| 9.1.2-h1 | 320 MB | 2020/04/23 13:08:14 | | | Download | Release Notes | |
| 9.1.2 | 320 MB | 2020/04/08 10:49:27 | | | Download | Release Notes | |
| 9.1.1 | 327 MB | 2020/02/10 14:11:38 | | | Download | Release Notes | |
| 9.1.0-h3 | 242 MB | 2019/12/21 10:49:09 | | | Download | Release Notes | |
| 9.1.0-b62 | 716 MB | 2019/11/25 09:36:57 | | | Download | Release Notes | |
| 9.1.0-b56 | 715 MB | 2019/11/06 04:44:19 | | | Download | Release Notes | |
| 9.1.0-b55 | 715 MB | 2019/10/24 22:40:21 | | | Download | Release Notes | |
| 9.1.0-b49 | 714 MB | 2019/10/02 21:43:46 | | | Download | Release Notes | |
| 9.1.0 | 714 MB | 2019/12/13 09:35:35 | | | Install | | ☒ |
| <div>  Check Now  Upload </div> | | | | | | | |

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

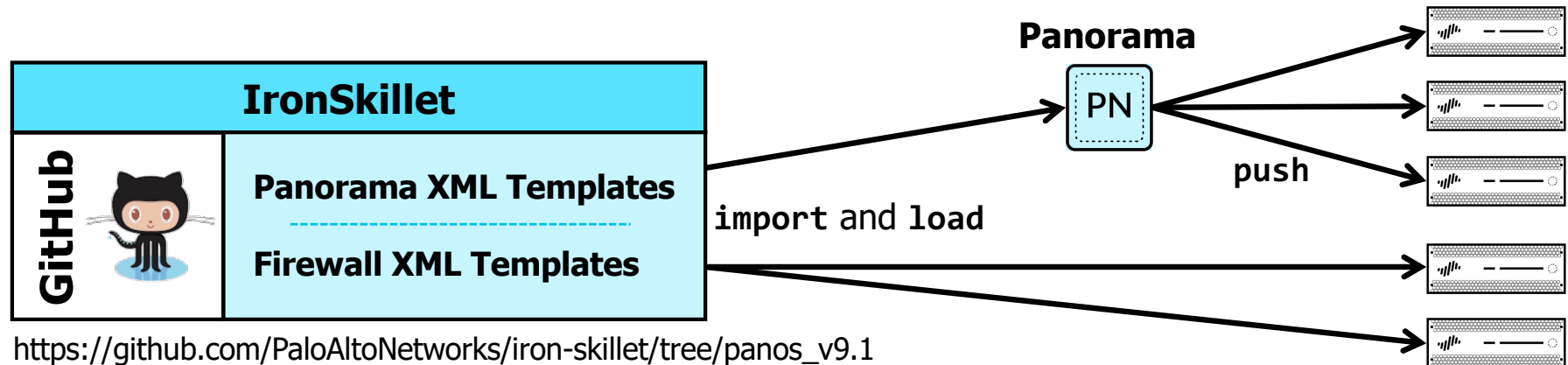
Dynamic Updates

Device > Dynamic Updates

| VERSION ^ | FILE NAME | FEATURES | TYPE | SIZE | SHA256 | RELEASE DATE | DOWNLOAD... | CURRENTLY INSTALLED | ACTION | DOCUMENTATION | |
|---|--------------------------------|---------------|------|-------|--------|-------------------------|--------------|---------------------|--------------------------------|---------------|---|
| Antivirus Last checked: 2020/07/01 17:43:03 UTC Schedule: Every hour at 5 minutes past the hour (Download and Install) | | | | | | | | | | | |
| 3392-3903 | panup-all-antivirus-3392-3903 | | Full | 99 MB | | 2020/06/27 11:03:19 UTC | | | Download | Release Notes | |
| 3393-3904 | panup-all-antivirus-3393-3904 | | Full | 98 MB | | 2020/06/28 11:01:33 UTC | ✓ previously | | Revert | Release Notes | |
| 3394-3905 | panup-all-antivirus-3394-3905 | | Full | 98 MB | | 2020/06/29 11:04:04 UTC | | | Download | Release Notes | |
| 3395-3906 | panup-all-antivirus-3395-3906 | | Full | 98 MB | | 2020/06/30 12:33:04 UTC | ✓ | | Install | Release Notes | ☒ |
| 3396-3907 | panup-all-antivirus-3396-3907 | | Full | 97 MB | | 2020/07/01 11:04:41 UTC | ✓ | ✓ | | Release Notes | ☒ |
| Applications and Threats Last checked: 2020/07/08 01:02:07 UTC Schedule: Every 30 minutes at 10 minutes past half-hour (Download and Install) | | | | | | | | | | | |
| 8278-6109 | panupv2-all-contents-8278-6109 | Apps, Threats | Full | 50 MB | | 2020/05/28 00:51:13 UTC | ✓ previously | | Revert | Release Notes | |
| 8281-6129 | panupv2-all-contents-8281-6129 | Apps, Threats | Full | 50 MB | | 2020/06/09 17:08:18 UTC | | | Download | Release Notes | |
| 8282-6133 | panupv2-all-contents-8282-6133 | Apps, Threats | Full | 50 MB | | 2020/06/11 22:53:26 UTC | | | Download | Release Notes | |
| 8283-6138 | panupv2-all-contents-8283-6138 | Apps, Threats | Full | 50 MB | | 2020/06/16 05:03:50 UTC | | | Download | Release Notes | |
| 8284-6141 | panupv2-all-contents-8284-6141 | Apps, Threats | Full | 56 MB | | 2020/06/17 04:10:45 UTC | | | Download | Release Notes | |
| 8285-6146 | panupv2-all-contents-8285-6146 | Apps, Threats | Full | 56 MB | | 2020/06/23 22:53:57 UTC | | | Download | Release Notes | |
| 8286-6150 | panupv2-all-contents-8286-6150 | Apps, Threats | Full | 56 MB | | 2020/06/26 02:03:18 UTC | | | Download | Release Notes | |
| 8287-6155 | panupv2-all-contents-8287-6155 | Apps, Threats | Full | 56 MB | | 2020/07/01 05:46:42 UTC | ✓ | ✓ | Review Policies Review Apps | Release Notes | ☒ |
| 8288-6160 | panupv2-all-contents-8288-6160 | Apps, Threats | Full | 56 MB | | 2020/07/03 01:48:09 UTC | | | Download | Release Notes | |
| Check Now Upload Install From File | | | | | | | | | | | |

- Schedule checking for new content, and automatic download or download and install.
- Updates can be manually downloaded, installed, or reverted to previous update.

Best Practice Configuration Templates



- The GitHub IronSkillet repository holds Day 1 configuration templates:
 - Implements *inbound*, *outbound*, and *internal* traffic protection methodology
 - Loads configuration settings and custom reports for Panorama or firewalls
 - Minimizes deployment time and errors
- Day 1 configuration also is available through the Support Portal when you register a new firewall.

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
- Activate firewall licenses and update PAN-OS® software
- Identify the purpose and location of firewall configuration skillets



Questions



Lab 2: Connect to the Management Network

- Connect to Your Student Firewall
- Configure the Update Server and DNS Server
- Configure General Settings
- Modify Management Interface
- Check for New PAN-OS Software



**Protecting our
digital way
of life.**

This page intentionally left blank.