paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

Palo Alto Networks Panorama: NGFW Management

Lab Guide

ILT-13

PAN-OS® 11.1

Courseware Version A

December 2024

Palo Alto Networks Technical Education

Palo Alto Networks, Inc.
https://www.paloaltonetworks.com

Table of Contents

Typographical Conventions

This guide uses the following typographical conventions for special terms and instructions.

Convention	Meaning	Example
Bolding	Names of selectable items in the web interface	Click **Security** to open the **Security Rule** Page
Consolas font	Text that you enter and coding examples	Enter the following command: **a:\setup** The **show arp all** command yields this output: **username@hostname> show arp** **<output>**
Calibri 11 pt. gray font	Lab step results and explanations	A new zone should appear in the web interface.
Click	Click the left mouse button	Click **Administrators** under the **Device** tab
Right-click	Click the right mouse button	Right-click the number of a rule you want to copy, and select **Clone Rule**
< > (text enclosed in angle brackets)	Denotes a variable parameter. Actual value to use is defined in the Lab Guide document.	Click **Add** again and select **<Internal Interface>**

Lab Guidance

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 Panorama and firewalls. If you have never worked with Panorama, 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.

Browsers

You will use two different browsers for these lab exercises:

- Configuration Browser - use this application to configure the firewall.
- Testing Browser - use this application to test features once you have configured the firewall.

There are two browsers available in the lab environment:

- Chromium
- Firefox

Note: For all lab exercises, we recommend always using the Chromium browser as the configuration browser when accessing the FireWall and Panorama WebUI and Firefox as the testing browser. Chromium has been shown to produce fewer errors than other browsers like Firefox when navigating the FireWall and Panorama WebUI. Please note that the FireWall and Panorama WebUI require a lot of memory, and having more than three browser windows or tabs open at the same time can consume the client's entire memory and consequently slow down the lab. We also recommend you restart your browser at least once a day.

The detailed lab guide sections tell which browser to use for each task.

Lab Guide Objectives

After you have finished these labs, you should be able to complete these tasks:

- Perform an initial configuration of your Panorama instance
- Connect your firewalls to the Panorama platform as managed Devices
- Create Templates and configure network and Device settings
- Configure Device Groups, policies, and objects
- Create Panorama and Device administrators
- Configure log forwarding to a Panorama instance
- Use Panorama for aggregated reporting and monitoring
- Perform troubleshooting to resolve various issues with Panorama

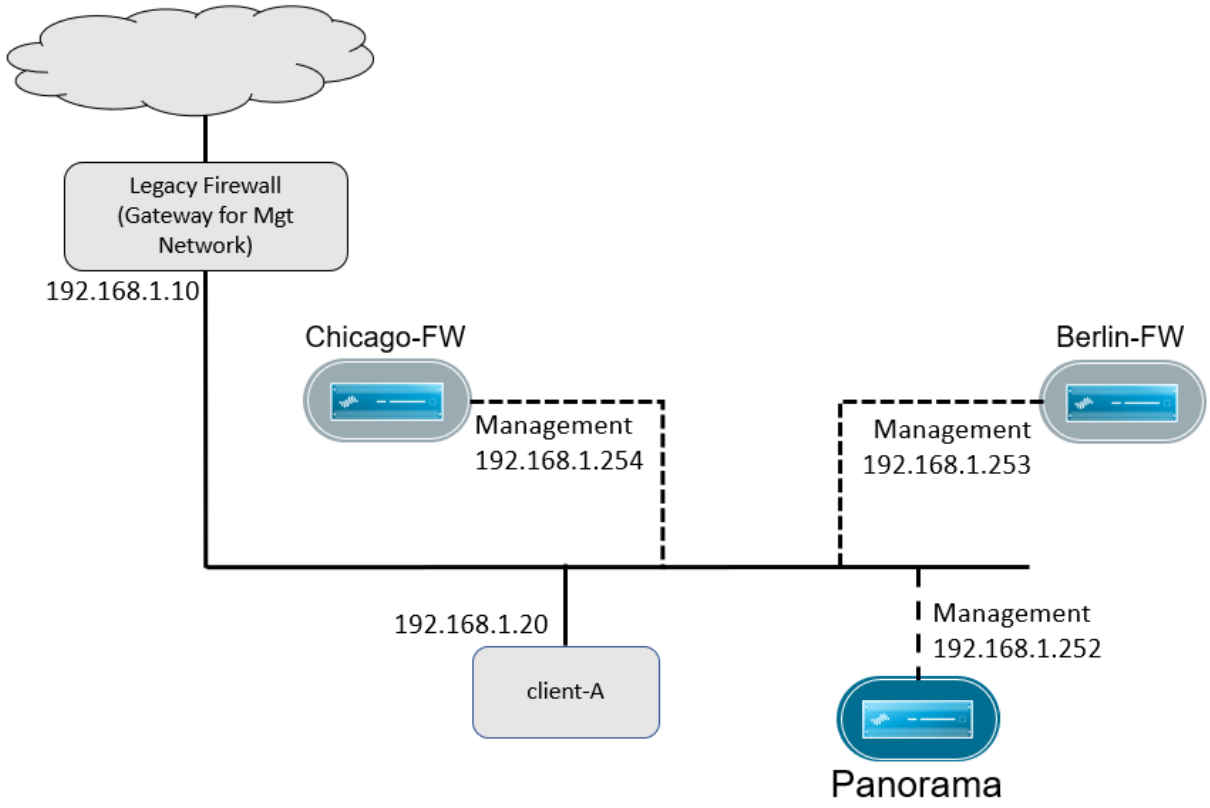
Lab 1 Scenario: Initial Configuration

A third-party vendor has installed a new Panorama appliance and two firewalls in your network. The Panorama appliance and one firewall are installed in Chicago. The second firewall has been installed in Berlin.

All three Devices have been configured with a management IP address on your company's management network (192.168.1.0/24).

A legacy firewall (192.168.1.10) acts as the default gateway for all Devices on the management network. After the Palo Alto Networks firewalls are in place, you will change the management network default gateway for Panorama, the Chicago firewall, and the Berlin firewall to an interface on the Chicago firewall.

Your task is to take ownership of these three Devices and to perform the initial configuration of the newly installed Panorama appliance. The network topology you will use follows:



Your instructor will provide login instructions about how to connect to the lab environment. You will use client-A to initially connect to the Panorama appliance and to the two firewalls.

Lab Objectives

In this lab, you will perform the following tasks:

- Connect to the class desktop
- Connect to Panorama and each firewall
- Use the Panorama web interface to verify licenses
- Configure a Panorama management interface
- Verify Panorama DNS, NTP, and update servers
- Configure General Settings
- Schedule Panorama Config Export
- Configure Dynamic Updates for Panorama
- Save the named Panorama configuration snapshot
- Export the named Panorama configuration snapshot

High-Level Lab Steps

Connect to the Class Desktop

Connect to the client-A desktop using the login credentials and hostname provided by your instructor.

Connect to Panorama and Each Firewall

From client-A, use the Configuration web browser to connect to the web interface of the Panorama appliance and each of your firewalls:

- Panorama: **`https://192.168.1.252`**. Username: **`admin`** Password: **`Pal0Alt0!`**
- firewall-a: **`https://192.168.1.254`**. Username: **`admin`** Password: **`Pal0Alt0!`**
- firewall-b: **`https://192.168.1.253`**. Username: **`admin`** Password: **`Pal0Alt0!`**

Use the Panorama Web Interface to Verify License and System Information

- When prompted for **Telemetry Data Collection**, select **OK**.
- Use the Panorama web interface to answer the following questions:
  - Which version of the operating system is Panorama running? _____
  - Is this a physical or virtual Panorama appliance? _____
  - How many Devices can this installation of Panorama manage? _____
  - When does support expire for this instance of Panorama? _____

Configure Panorama Management Interface

- Verify the Management Interface Settings:
  - IP Address = 192.168.1.252
  - Netmask = 255.255.255.0
  - Default Gateway = 192.168.1.10
- Enable the **SNMP** Network Service.
- Restrict access to Panorama from the 192.168.0.0/16 management network only.

Verify Panorama DNS and Update Servers

- Confirm that Panorama has been configured with the correct **Update Server** settings:
  - **Update Server** = **`updates.paloaltonetworks.com`**
  - **Verify Update Server Identity** = **`enabled`**
- Set the **Primary DNS Server** to **`192.168.50.53`**
- Verify that the **Secondary DNS Server** is set to **`8.8.8.8`**

Verify Panorama NTP Servers

- Set the network time protocol (NTP) servers are set to the following:
  - **`192.168.1.10`** for the **Primary NTP Server**
  - **`time-a-g.nist.gov`** for the **Secondary NTP Server**

Configure General Settings

- Set the **Domain** for Panorama to **`panw.lab`**.
- For the **Login Banner** field, enter **`*** This is Panorama ***`**
- Verify that the **Time Zone** is set to **`Europe/Dublin`**.
- Set the **Latitude** to **`41.00`** and the **Longitude** to **`87.00`** (Chicago, IL, USA)

Schedule Panorama Config Export

Configure and enable a daily configuration export to a storage server using SCP.

- Use the information below to create the entry:

Name	**Daily-Export-SCP**
Description	**Panorama and firewall configurations**
Scheduled Export Start Time (Daily)	**01:30**
Protocol	**SCP**
Hostname	**192.168.50.150**
Port	**22**
Path	**/home/paloalto42/**
Username	**paloalto42**
Password	**Pal0Alt0!**

This connection is not available until you finish configuring elements for the firewalls in your lab. If you try the Test SCP server connection at this point, the connection will time out.

Configure Dynamic Updates for Panorama

- Use the following information to create an **Antivirus Update Schedule**:

Recurrence	**Weekly**
Day	**sunday**
Time	**01:00**
Action	**download-and-install**

- Use the following information to create an **Applications and Threats Update Schedule**:

Recurrence	`Weekly`
Day	`sunday`
Time	`02:00`
Action	`download-and-install`

The **Recurrence** for these updates is set to **Weekly** because of lab environment restrictions. In a production environment, you should follow the recommended best practices for Dynamic Content updates.

For more information on this topic, log in to live.paloaltonetworks.com and search for "Best Practices for Applications and Threats Content Updates" to locate the most recent article.

Commit Changes to Panorama

- Enter a Description when you commit the changes to Panorama:
  `Initial configuration completed for Lab 1 by <your initials>`
- Examine the **Task Manager – All Tasks (Panorama)** and note the **Commit Description** that matches your entry.

If you do not enter information in the **Description** field for a **Commit**, the **Commit Description** link is not available. Using the Description field for Panorama commits is optional but recommended if you need to track changes made by administrators.

Save the Named Panorama Configuration Snapshot

Save a copy of this Panorama configuration with the following name:

- **`Panorama-Lab1-End.xml`**

Export the Named Panorama Configuration Snapshot

- Export the named Panorama configuration snapshot **Panorama-Lab1-End.xml** to the client-A workstation.
- Verify that the file has been saved to the **Downloads** folder on the client-A workstation.

Detailed Lab Steps

Connect to the Class Desktop

1. Connect to the client-A desktop using the login credentials and hostname provided by your instructor.

Connect to Panorama and Each Firewall

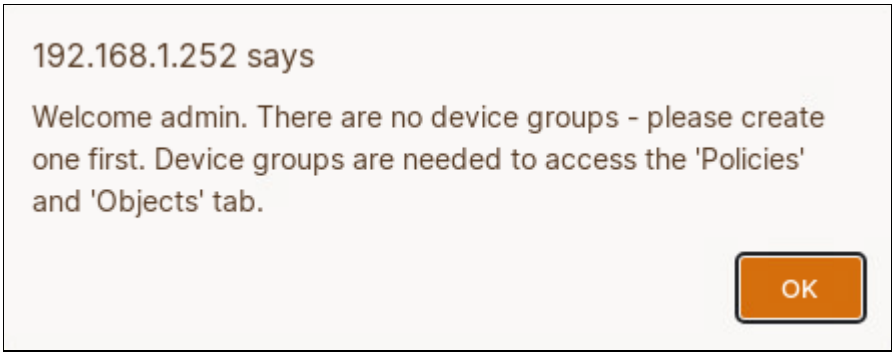
2. From client-A, use the configuration web browser to connect to the web interface of the Panorama appliance and each of your firewalls. Use a separate tab for each Device.

   Note the use of HTTPS. (Click through any certificate warning messages.)

   - Panorama: **`https://192.168.1.252`**. Username: **`admin`** Password: **`Pal0Alt0!`**
   - firewall-a: **`https://192.168.1.254`**. Username: **`admin`** Password: **`Pal0Alt0!`**
   - firewall-b: **`https://192.168.1.253`**. Username: **`admin`** Password: **`Pal0Alt0!`**

Use the Panorama Web Interface to Verify License and System Information

3. The Panorama web interface may present a message indicating that there are no Device groups:



4. Click **OK** to clear the message.

   You will create Device Groups later in this course.

5. If a Welcome window appears, place a check in the box for Do not show again.
6. Click **OK**.
7. Panorama may present a **Telemetry Data Collection** message.
8. Click **OK**.
9. Panorama initially will display only four tabs: **Dashboard**, **ACC**, **Monitor**, and **Panorama**.
10. Click the **Dashboard** tab, and then review the **General Information** section. Write the answers to the following questions in the space provided:

    a. Which version of the operating system is Panorama running? _____

    b. Is this a physical or virtual Panorama appliance? _____

11. Select the **Panorama** tab.
12. Locate the navigation tree on the left side of the screen.

    Notice the small gray circle  to the right of several options.

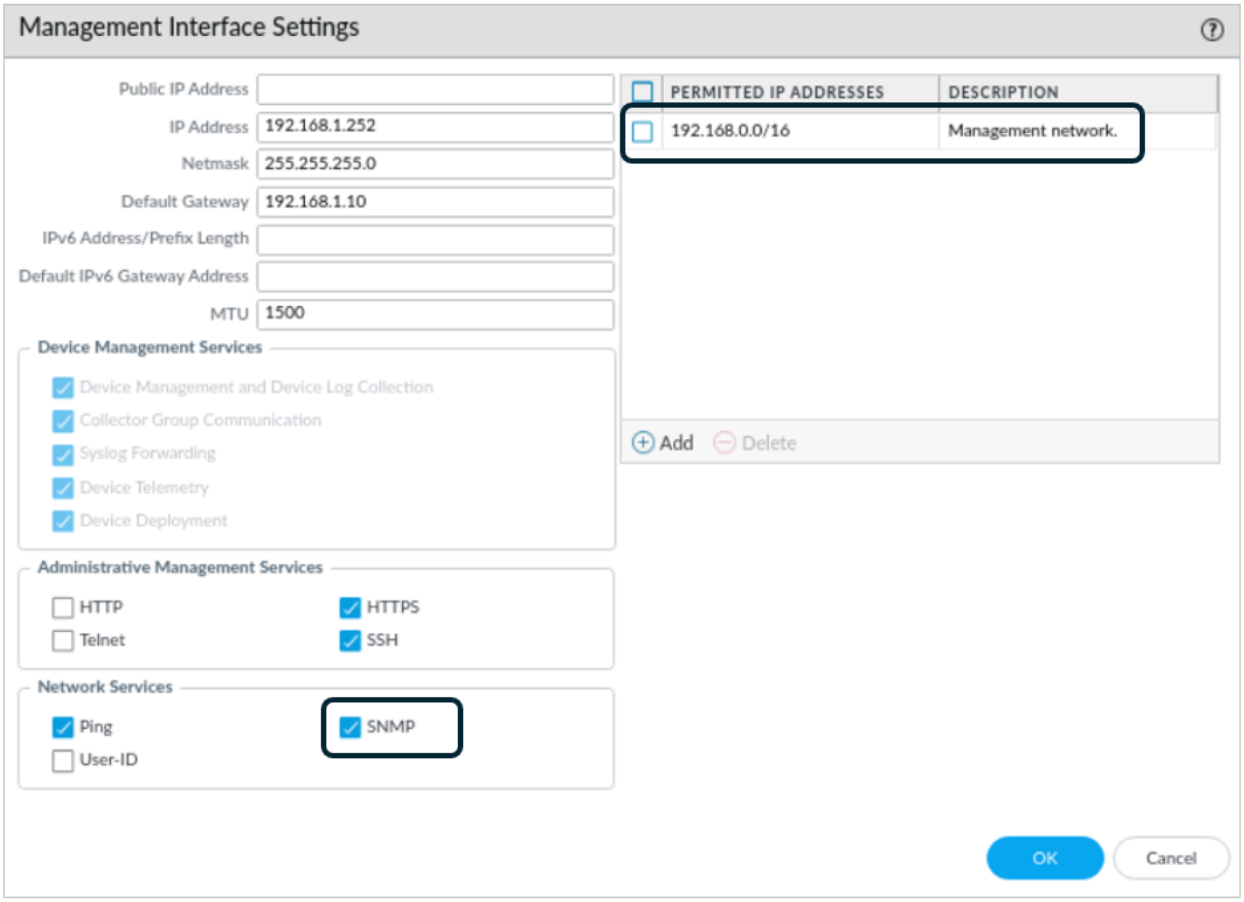
    Hover the pointer over a circle to display specific information about the configuration.
13. Navigate to **Panorama** > **Licenses**.
    a. How many Devices can this installation of Panorama manage? _____
14. Navigate to **Panorama** > **Support**.
    a. When does support expire for this instance of Panorama? _____

Configure Panorama Management Interface

Examine the Panorama management interface settings and restrict management access to Panorama from hosts on the 192.168.0.0/16 network.

15. Select **Panorama** > **Setup** > **Interfaces**.
16. Click the **Management** entry under the column titled **Interface Name**.
17. Verify the entries for the **Management Interface Settings**:
    - IP Address = 192.168.1.252
    - Netmask = 255.255.255.0
    - Default Gateway = 192.168.1.10
18. Check the box for **SNMP** under the **Network Services** section.
19. Restrict access to Panorama from the management network only by adding an entry to the **Permitted IP Addresses** section:
    a. Click **Add**.
    b. Under **Permitted IP Addresses**, enter **`192.168.0.0/16`**.

c. Under **Description**, enter **`Management network.`**:



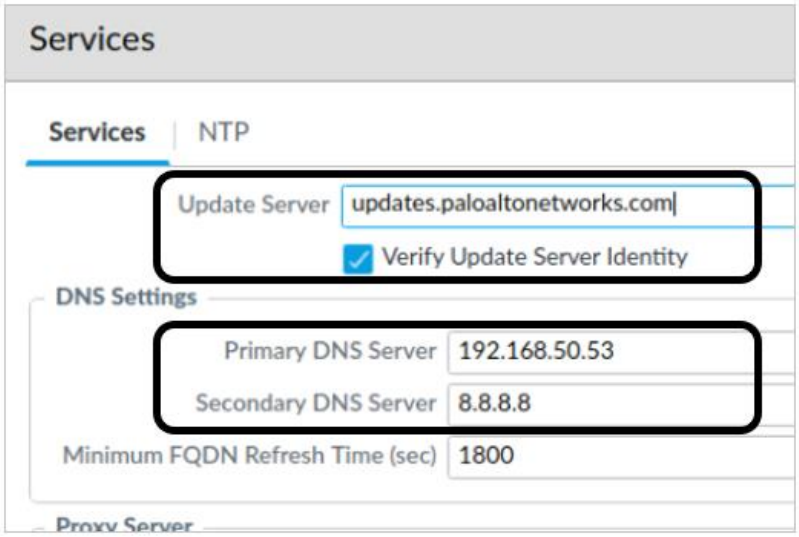
20. Click **OK**.

Verify Panorama DNS and Update Servers

Verify the Palo Alto Networks update server and set DNS servers for Panorama.

21. Navigate to **Panorama** > **Setup** > **Services**.
22. Click the **gear**  icon, which allows you to edit the **Services** settings.
23. Confirm that Panorama has been configured with the correct **Update Server** settings:
    - **Update Server** = **`updates.paloaltonetworks.com`**
    - **Verify Update Server Identity** = enabled
24. Set the DNS servers:
    - **Primary DNS Server** = **`192.168.50.53`**

Verify that the Secondary DNS Server is set to `8.8.8.8`



25. Leave the **Services** window open.

Verify Panorama NTP Servers

Verify that the network time protocol (NTP) servers are set.

26. In the **Services** window, click the **NTP** tab.
27. Verify **192.168.1.10** in the **NTP Server Address** field for the **Primary NTP Server**.
28. Set **time-a-g.nist.gov** in the **NTP Server Address** for the **Secondary NTP Server**:

29. Leave the **Authentication Type** set to **None** for both values.
30. Click **OK**.

Configure General Settings

Set the **Login Banner**, **Time Zone**, **Longitude**, and **Latitude** for Panorama.

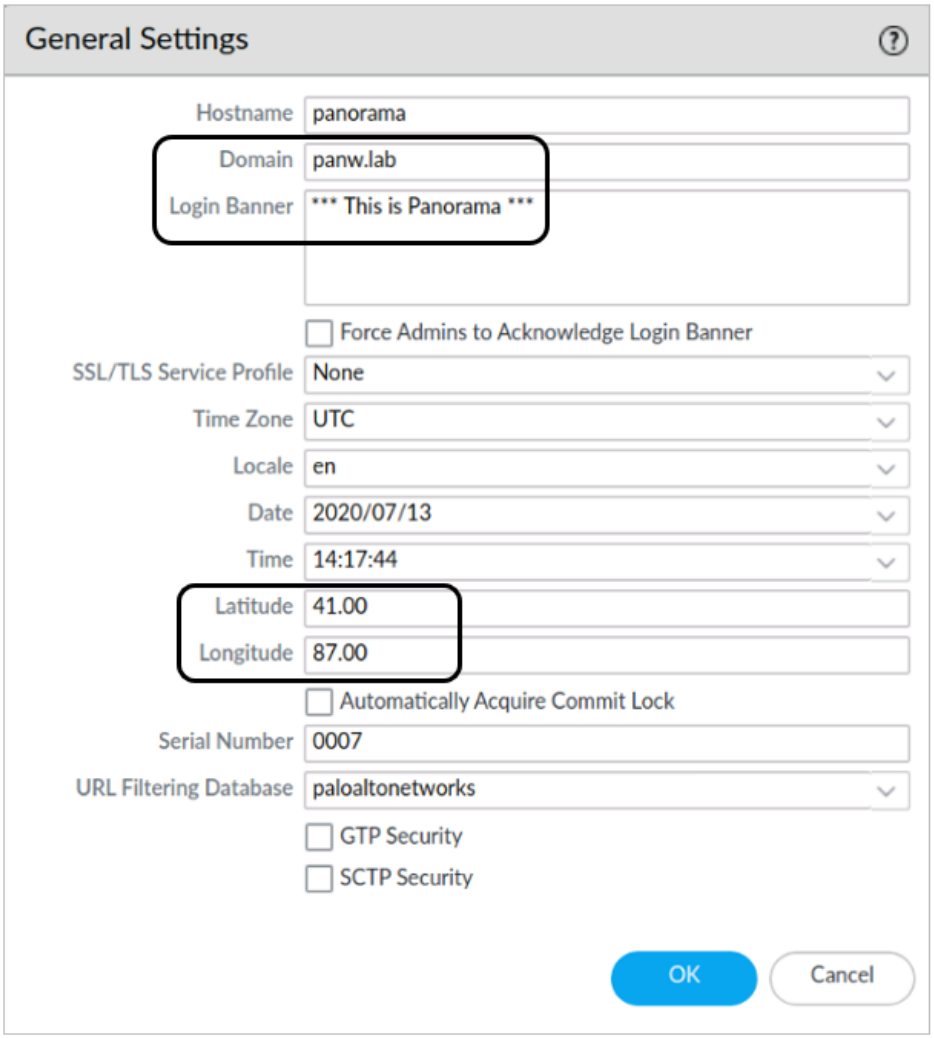
31. Navigate to **Panorama > Setup > Management**.
32. Click the **gear** icon in the upper-right corner of the **General Settings** section, which allows you to edit the **General Settings**.
33. In the **Domain** field, enter **`panw.lab`**.
34. In the **Login Banner** field, enter: **`*** This is Panorama ***`**

This notice will enable you to easily distinguish between Panorama and managed firewalls when you are working in the web interface.

35. Verify that the **Time Zone** is set to **Dublin/Europe**.
36. Set the **Latitude** to **`41.00`**.

37. Set the **Longitude** to **`87.00`**.

These latitude and longitude settings are for Chicago, where your Panorama Device resides. Setting the latitude and longitude allows the Application Command Center (ACC) and other tools to place Panorama in the correct geographic location on monitoring maps.



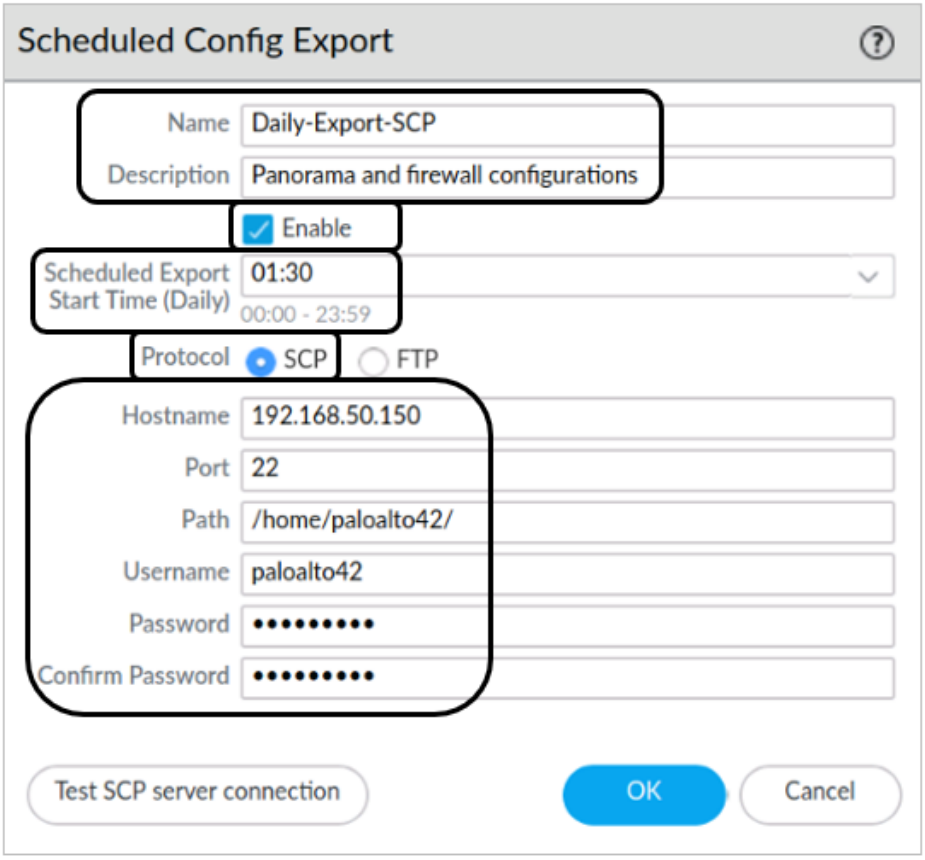
38. Leave the remaining settings unchanged, and then click **OK**.

Schedule Panorama Config Export

Configure Panorama with a daily configuration export to a storage server using SCP.

39. Navigate to **Panorama** > **Scheduled Config Export**.
40. Click **Add** at the bottom of the window.
41. For **Name**, enter **`Daily-Export-SCP`**.

42. For **Description**, enter **`Panorama and firewall configurations`**.
43. Place a **check mark** in the box for **Enable**.
44. Set the **Scheduled Export Start Time (Daily)** to **01:30**.
45. Set the **Protocol** to **SCP**.
46. For **Hostname**, enter **`192.168.50.150`**.
47. For **Port**, enter **`22`**.
48. For **Path**, enter **`/home/paloalto42/`**
49. For **Username**, enter **`paloalto42`**
50. For **Password** and **Confirm Password**, enter **`Pal0Alt0!`** as the value:



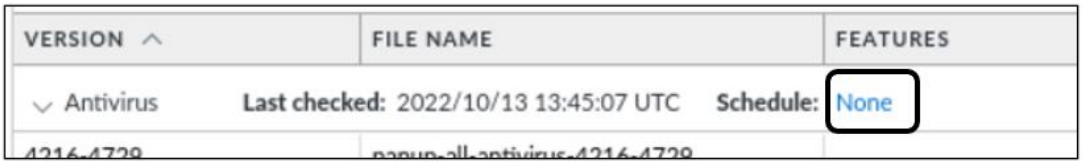
This connection is not available until you finish configuring elements for the firewalls in your lab. If you try the **Test SCP server connection** at this point, the connection will time out.

51. Leave the remaining settings unchanged and click **`OK`**.

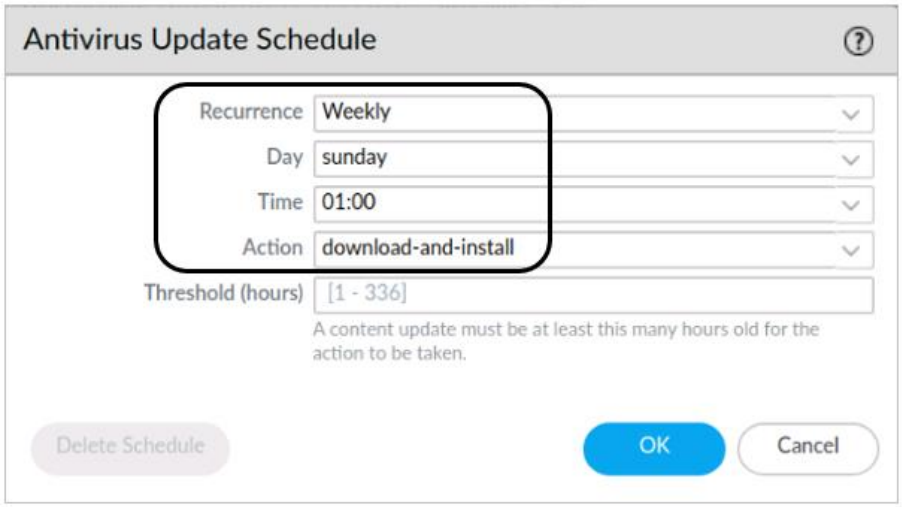
Configure Dynamic Updates for Panorama

Panorama needs to have the most recent application and threat definitions from Palo Alto Networks. In this section, you will configure Panorama to download these definitions on a scheduled basis.

52. Navigate to **Panorama > Dynamic Updates**.
53. In the section for **Antivirus**, click the link for **None**:



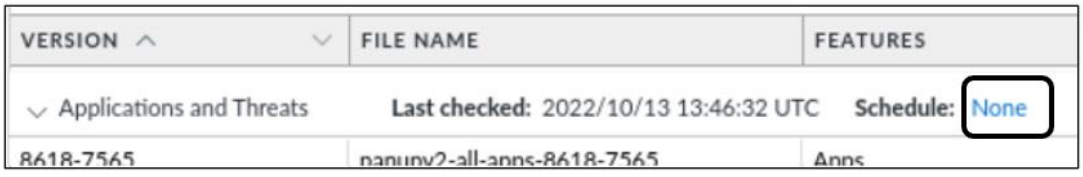
54. In the **Antivirus Update Schedule** window, change the **Recurrence** to **Weekly**.
55. Set the **Day** to **sunday**.
56. Set the **Time** to **01:00**.
57. Set the **Action** to **download-and-install**.
58. Leave the **Threshold (hours)** unchanged:



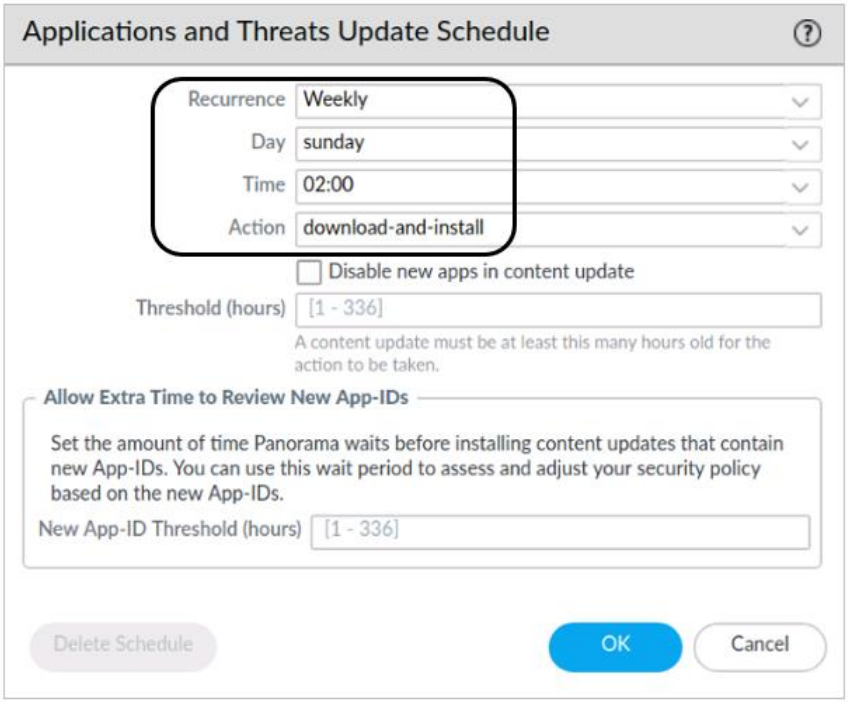
This schedule instructs Panorama to check with the Palo Alto Networks update servers each week on Sunday at 1 a.m. and to download and install any new Antivirus updates.

In a production environment, you should set the schedule to check hourly.

59. Click **OK**.
60. Scroll down in the **Dynamic Updates** screen to locate the **Applications and Threats** section.
61. Click the link for **None**:



62. Set the **Recurrence** to **Weekly**.
63. Set the **Day** to **sunday**.
64. Set the **Time** to **02:00**.
65. Set the **Action** to **download-and-install**.
66. Leave the remaining settings unchanged.



You have set this schedule to download and install new updates for Applications and Threats each Sunday at 2:00 a.m. In a production environment, you should set this schedule to check hourly.

67. Leave the remaining settings unchanged.
68. Click **OK**.

Note that the **Recurrence** for these updates is set to **Weekly** because of lab environment restrictions.

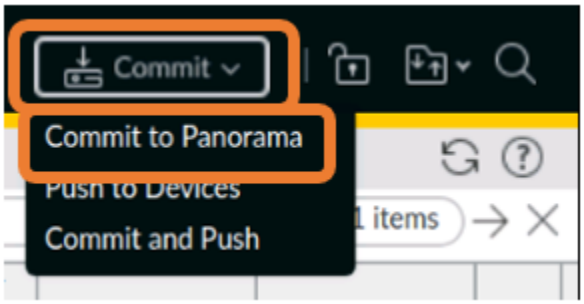
In a production environment, you should follow the recommended best practices for Dynamic Content updates.

For more information on this topic, log in to live.paloaltonetworks.com and search for "Best Practices for Applications and Threats Content Updates" to locate the most recent article.

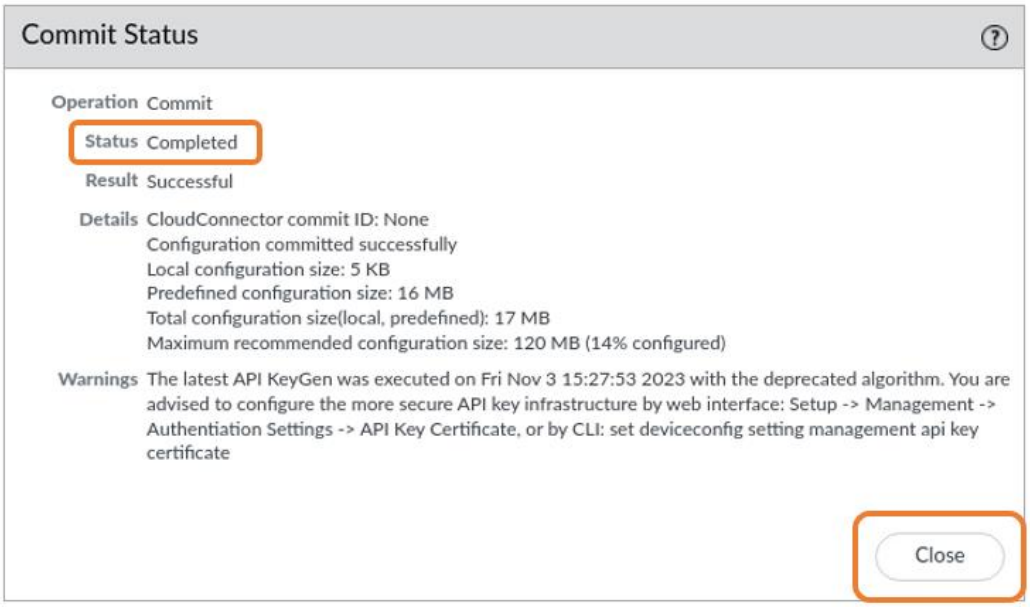
Commit Changes to Panorama

You now will commit these changes to Panorama.

69. Click the **Commit** option in the upper-right corner.
70. Then select **Commit to Panorama**:



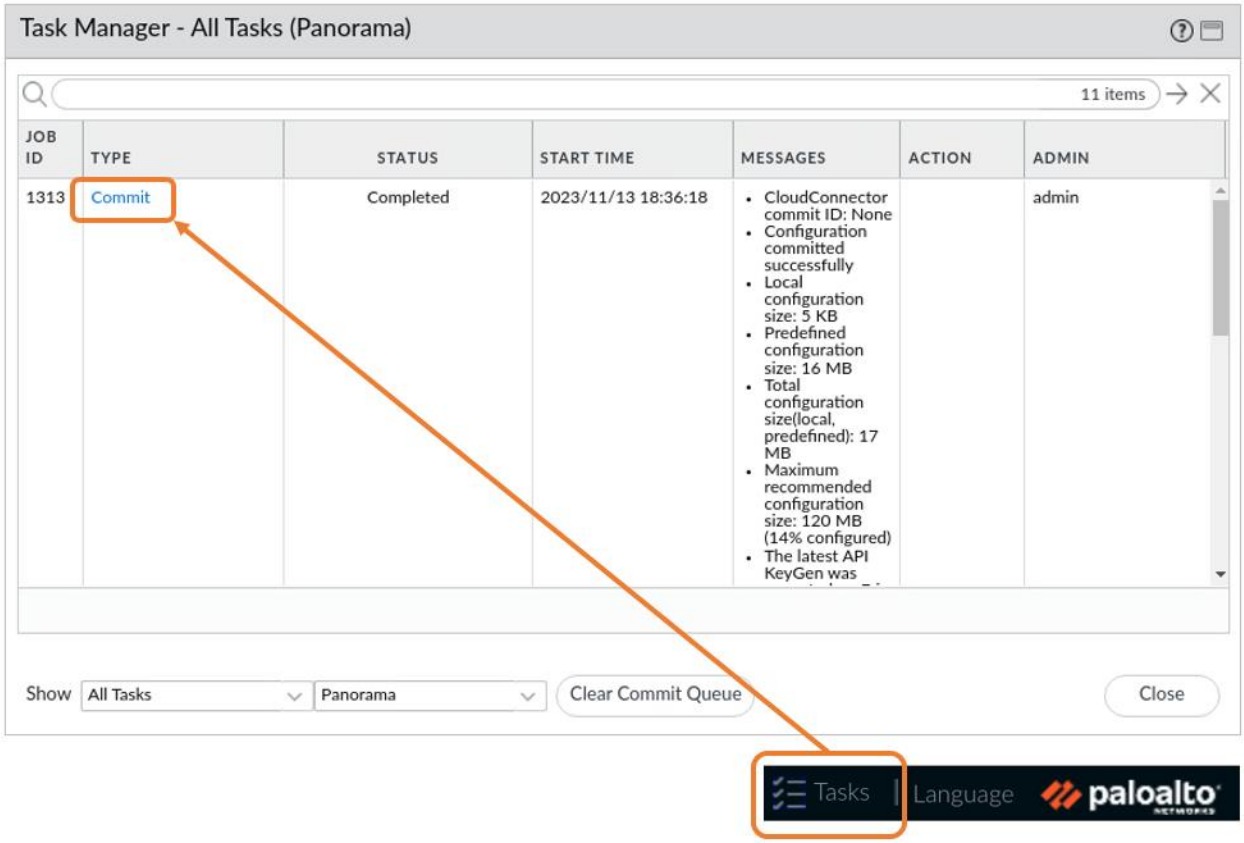
71. When the **Commit to Panorama** window appears, enter the following information in the Description field: **`Initial configuration completed for Lab 1 by <your initials>`**
72. Leave the remaining settings unchanged and click **Commit**.
73. When the **Status** is **Completed**, click **Close**:



If you receive a message regarding the deprecated algorithm used to generate the API KeyGen, ignore it. This message will have no effect on the labs.

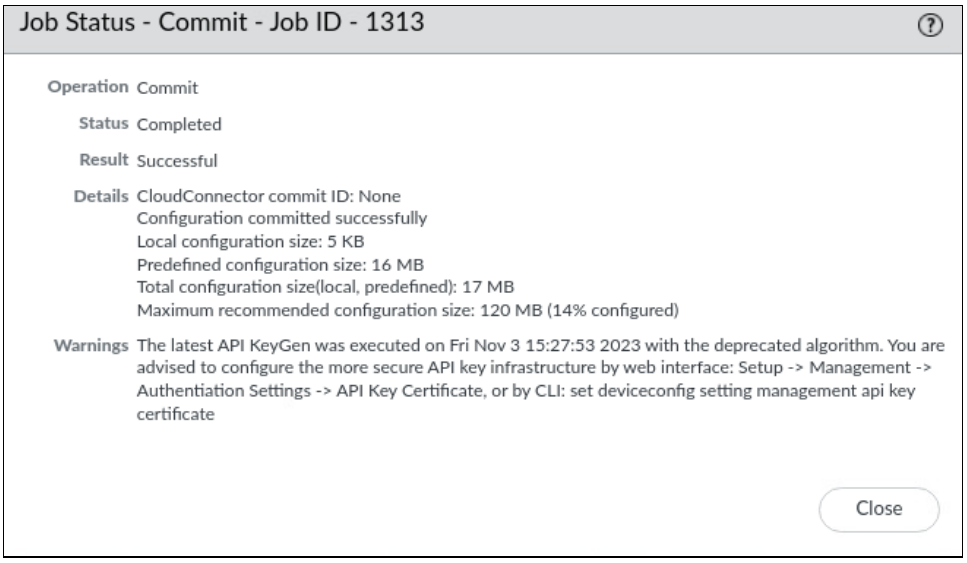
There is a Bonus Lab at the end of this guide that will show you how to address this issue.

74. In the bottom-right corner of the web interface, click the **Tasks** button to display the **Task Manager – All Tasks (Panorama)** window.
75. In the **Task Manager** window that appears, click the first **`Commit`** hyperlink:

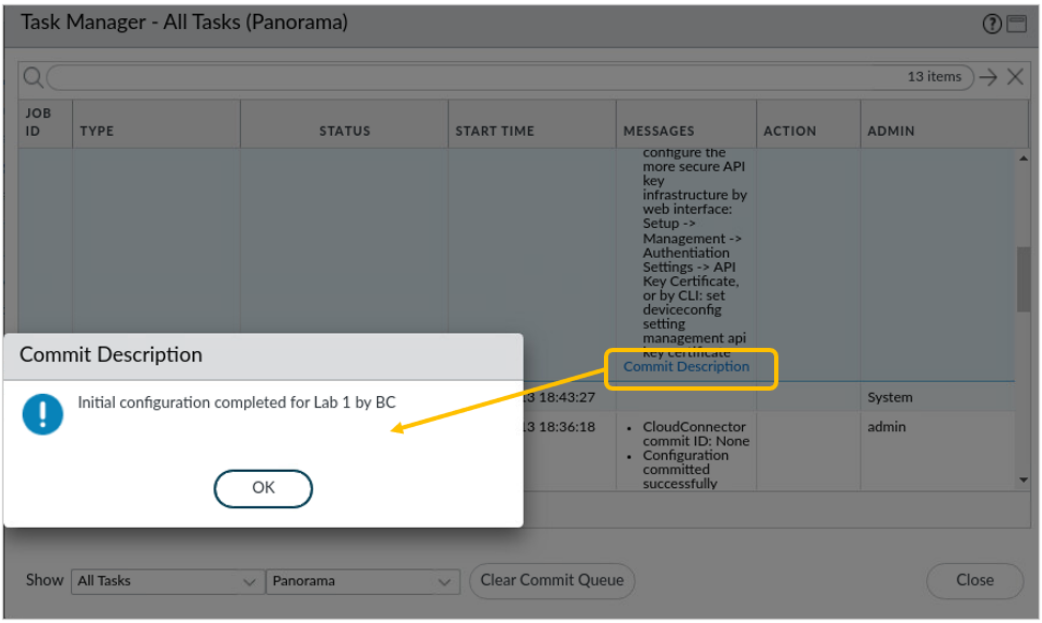


Note that the list of tasks displayed in this window may vary.

76. Panorama displays a **Job Status - Commit** window with details about the commit process you selected.



77. Click **Close**.
78. In the **Task Manager – All Tasks (Panorama)** window, click the link for **Commit Description** in the first row to display the description for this commit (you may need to scroll down in the window to see the link):



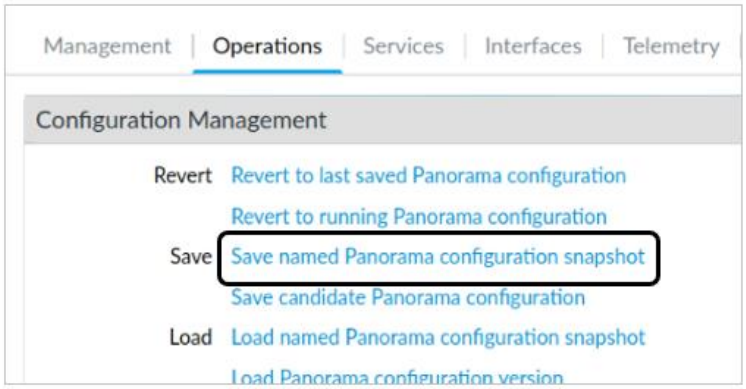
If you do not enter information in the **Description** field for a **Commit**, the **Commit Description** link is not available. Using the Description field for Panorama commits is optional but recommended if you need to track changes made by administrators.

79. Click **OK** in the **Commit Description** window.
80. Click **Close** in the **Task Manager** window.

Save the Named Panorama Configuration Snapshot

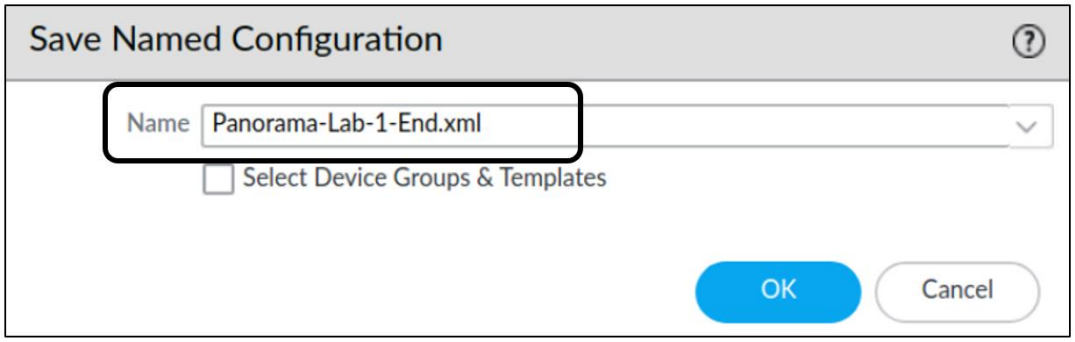
You now will save a copy of this Panorama configuration.

81. Select **Panorama > Setup > Operations > Save named Panorama configuration snapshot**:

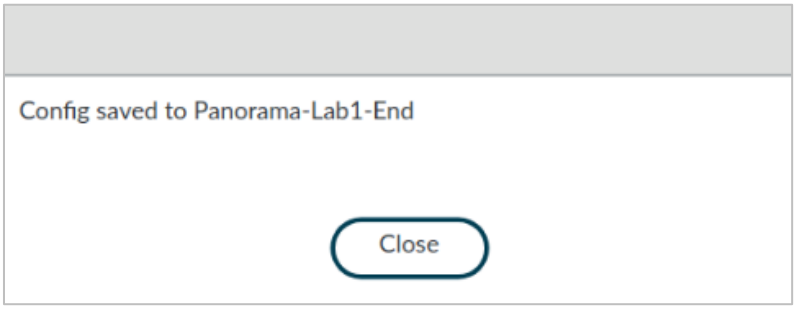


82.

83. For the **Name**, enter **`Panorama-Lab1-End.xml`**:



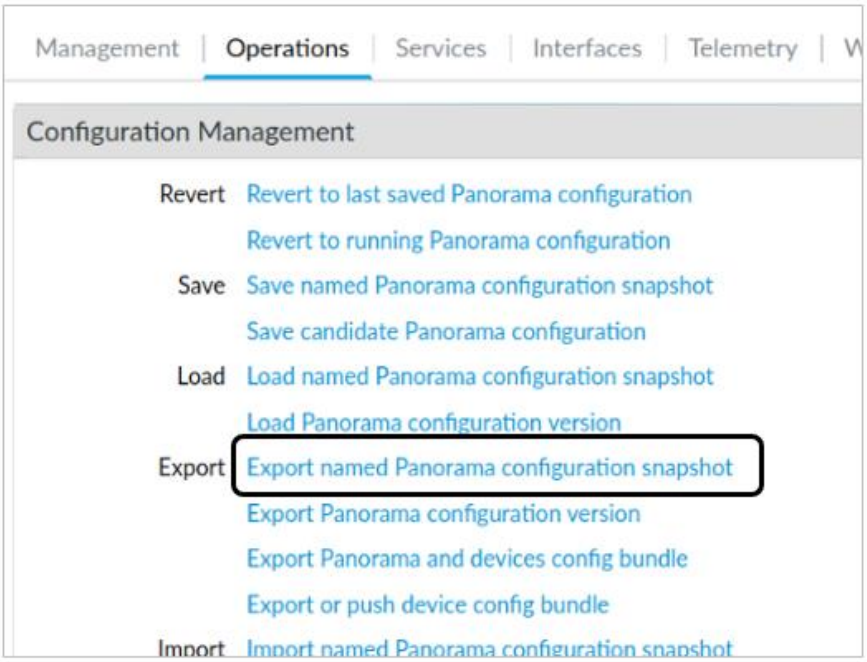
84. Click **OK**.
85. Click **Close** to dismiss the confirmation window:



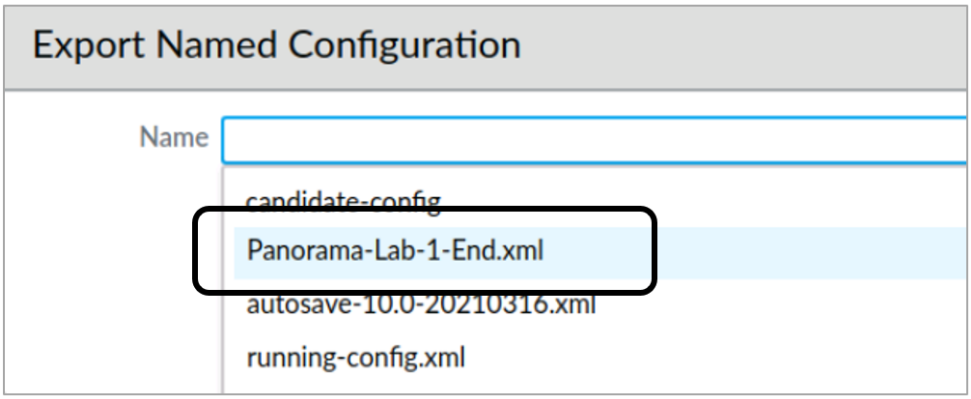
Export the Named Panorama Configuration Snapshot

When you save a configuration using the **Save named Panorama configuration snapshot**, the file is saved to Panorama itself. In this section, you will export the saved configuration file from Panorama to your workstation.

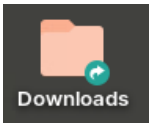
86. Select **Panorama > Setup > Operations > Export named Panorama configuration snapshot**:



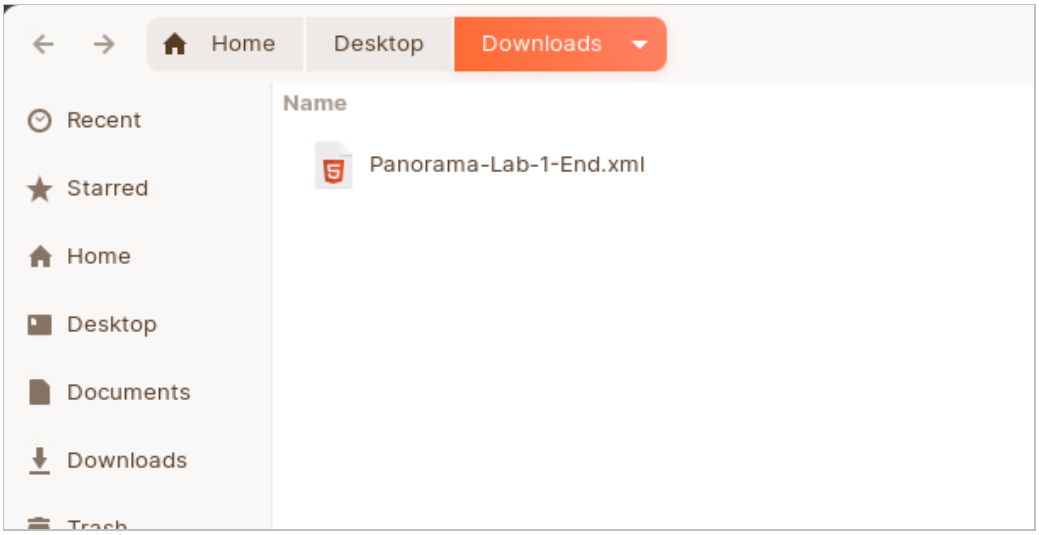
87. Use the drop-down list to select the **Panorama-Lab1-End.xml** entry:



88. Click **OK**.
89. When prompted, save the file to the Downloads folder on the workstation.
90. On your workstation desktop, open the **Downloads** folder:



91. You should see the **Panorama-Lab1-End** configuration file that you exported from Panorama:



92. Close the **File Manager** window.

Stop. This is the end of the lab.

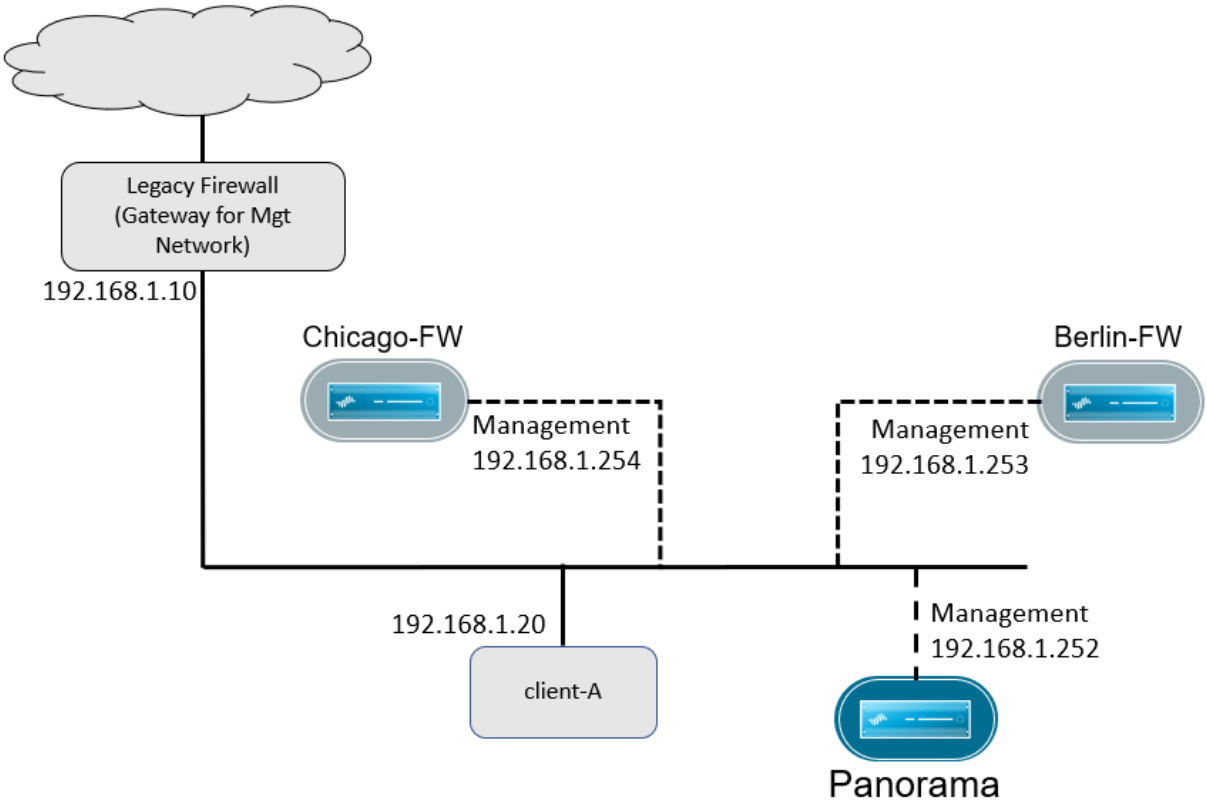
Lab 2 Scenario: Adding Managed Firewalls to Panorama

You have established connectivity to Panorama and to both firewalls. Your next task is to add both firewalls as managed Devices to Panorama. You also need to ensure that external backups of firewall and Panorama configurations are available.

Lab Objectives

In this lab, you will perform the following tasks:

- Copy serial numbers from firewalls
- Set the location for firewalls
- Configure firewalls to communicate with Panorama
- Add firewalls to Panorama
- Modify columns in the Summary window
- Verify that both firewalls are connected to Panorama
- Verify firewall licenses in Panorama
- Schedule Dynamic Updates for firewalls



High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-2-Start.xml** configuration file on Panorama

Copy the Serial Number from firewall-a

- Copy the serial number for firewall-a to a text file on the client-A desktop

Copy the Serial Number from firewall-b

- Copy the serial number for firewall-b to a text file on the client-A desktop

Add the Firewalls to Panorama

- Copy and paste the firewall serial numbers into the **Managed Devices** section of Panorama
- Generate an Auth Key in Panorama and paste the value into a text file

Configure firewall-a to Communicate with Panorama

- Configure firewall-a to communicate with Panorama

Set the Location of firewall-a

- For firewall-a, set the **Latitude** to **`41.00`** and the **Longitude** to **`87.00`**.
- Set the **Hostname** to **`chicago-fw`**.
- Set the **Domain** to **`panw.lab`**.
- Verify that the **Time Zone** is set to **Europe/Dublin**.

Configure firewall-b to Communicate with Panorama

- Configure firewall-b to communicate with Panorama

Set the Location of firewall-b

- For firewall-b, set the **Latitude** to **`52.00`** and the **Longitude** to **`13.00`**.
- Set the **Hostname** to **`berlin-fw`**.
- Set the **Domain** to **`panw.lab`**.
- Verify that the **Time Zone** is set to **Europe/Dublin**.

Commit the Changes to Panorama

- Commit these changes to Panorama

Verify that Both Firewalls are Connected to Panorama

- Periodically refresh the **Managed Devices > Summary** window and verify that both firewalls are **Connected**

Modify Columns in the Summary Window

- **Unselect** all but the following items in the Panorama Summary Device window:
  - Device Group
  - Model
  - Tags
  - Serial Number
  - IP Address IPV4
  - Variables
  - Template
  - Status Device State
  - Status Template
  - Status Template Last Commit State
  - Software Version
  - Apps and Threat
  - Antivirus
  - URL Filtering
  - WildFire
  - Backups
- Drag and drop the **IP Address** column between the **Device Name** and **Model** columns

Verify Firewall Licenses in Panorama

- Use Panorama to refresh the licenses for both firewalls.
- **Refresh** the list to display the applied licenses.

Schedule Dynamic Updates to Firewalls

- Use the information below to create a **Schedule** for **Applications and Threat** updates for both firewalls:

Name	**Weekly-App-and-Threat-Updates**
Type	**App and Threat**
Recurrence	**Weekly**
Day	**Sunday**
Time	**02:30**
Action	**Download and Install**

- Use the information below to create a **Schedule** for Antivirus updates:

Name	**Weekly-AV-Updates**
Type	**Anti Virus**
Recurrence	**Weekly**
Day	**Sunday**
Time	**02:45**
Action	**Download and Install**

Commit the Changes to Panorama

- Commit these changes to Panorama.

Detailed Lab Steps

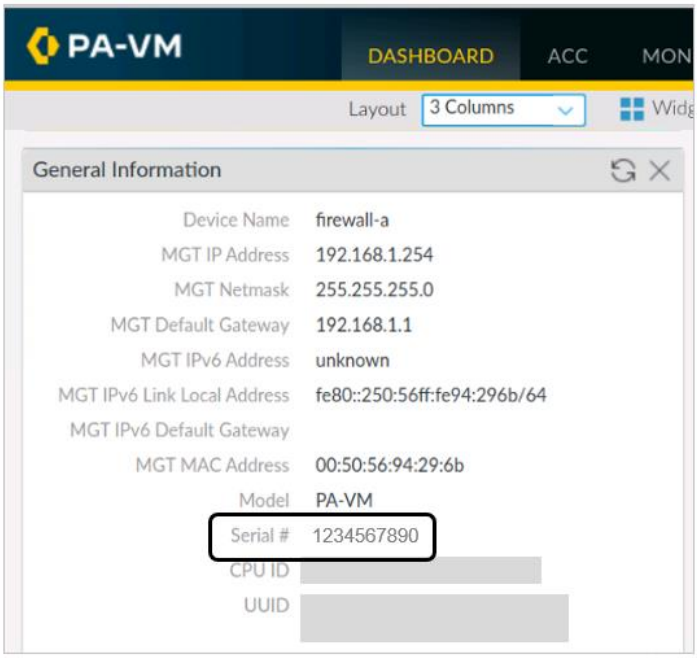
Load the Lab Start Configuration File

1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-2-Start.xml**.
4. Leave the remaining settings unchanged.
5. Click **OK** to close the **Load Named Configuration** window.
6. Click **Close** on the **Loading Configuration** window.
7. Commit the changes to Panorama by selecting **Commit** > **Commit to Panorama** in the upper-right corner of the window.
8. In the **Commit to Panorama** window, click **Commit**.
9. Allow the process to complete.
10. Click **Close** in the **Commit Status** window.

Copy the Serial Number from firewall-a

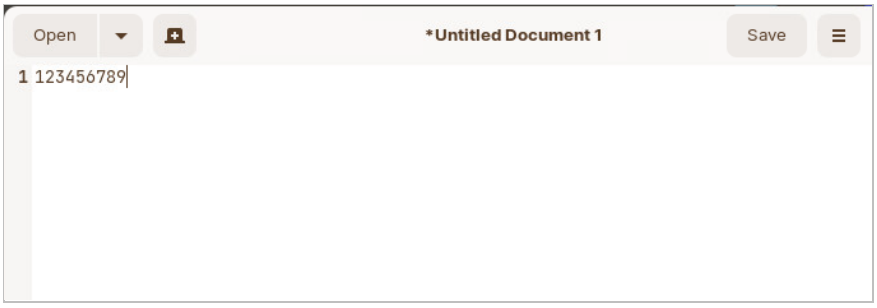
Copy the serial number from the **Dashboard** of firewall-a and paste it into a text file.

11. Copy the serial number from the **Dashboard** of firewall-a and paste it into a text file.
12. In the configuration browser, select the tab for **firewall-a**.
13. If you see a Welcome window, place a check in the box for Do not show again.
14. Click **OK** if the Telemetry Data Collection window appears, and click **Close**.
15. Under the **Dashboard** tab, locate the **Serial #** field in the **General Information** section:



16. Copy the serial number for firewall-a to the clipboard.
17. From the client-A desktop, open **Text Editor**:

18. Paste the serial number from firewall-a into **Text Editor**:



The serial number for your Chicago firewall will be different than the example shown here.

19. Leave **Text Editor** open.

Copy the Serial Number from firewall-b

Copy the serial number from the **Dashboard** of the firewall and paste it into a text file.

20. In the configuration browser, select the tab for **firewall-b**.
21. In the Welcome window, place a check in the box for Do not show again.
22. Click **OK** if the Telemetry Data Collection window appears.
23. Click **Close**.
24. Under the **Dashboard** tab, locate the **Serial #** field in the **General Information** section.
25. Copy the serial number for firewall-b.
26. Paste the serial number from firewall-b into **Text Editor** just below the serial number for firewall-a.
27. Leave **Text Editor** open.

Add the Firewalls to Panorama

In this section, you will add the serial numbers from both firewalls to Panorama.

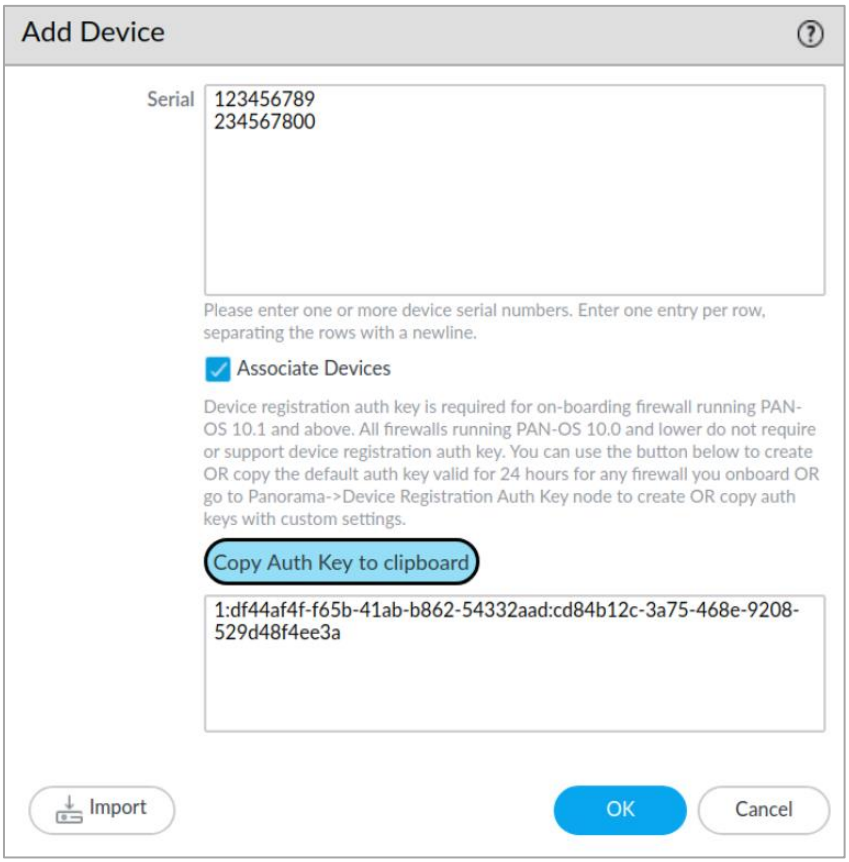
28. In the Panorama web interface, select **Panorama > Managed Devices > Summary**.
29. Click the **Add** button in the bottom-left corner of the window.
30. Leave the box checked for **Associate Devices**.
31. Click the button for **Generate Auth Key**:

This action will create a value that you must use when you configure a firewall to communicate with Panorama. You will carry out that process in the next section.

32. Copy the Auth Key value to the clipboard.
33. Leave the **Add Device** window open in the Panorama web interface.
34. Paste the Auth Key value into the Text Editor file below the two firewall serial numbers:

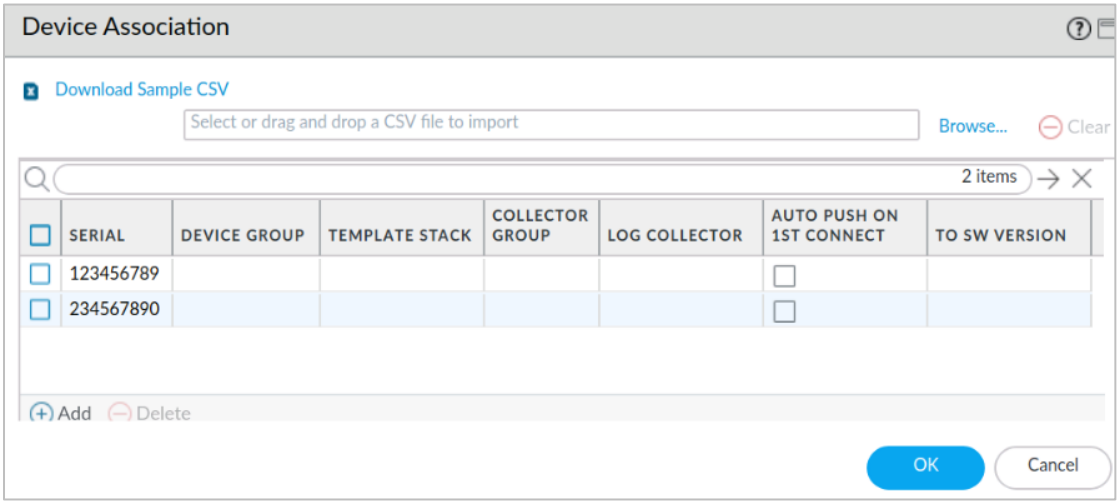
The serial numbers for your Chicago and Berlin firewall devices will be different from the example shown here. The Auth Key will also be different.

35. Copy the serial numbers from **Text Editor** and paste them into the **Serial** section of the Add Device window in Panorama.



Each Serial number entry must be on a separate line.

36. Click **OK**.
37. Panorama displays the **Device Association** window, which lists both firewalls by serial number:



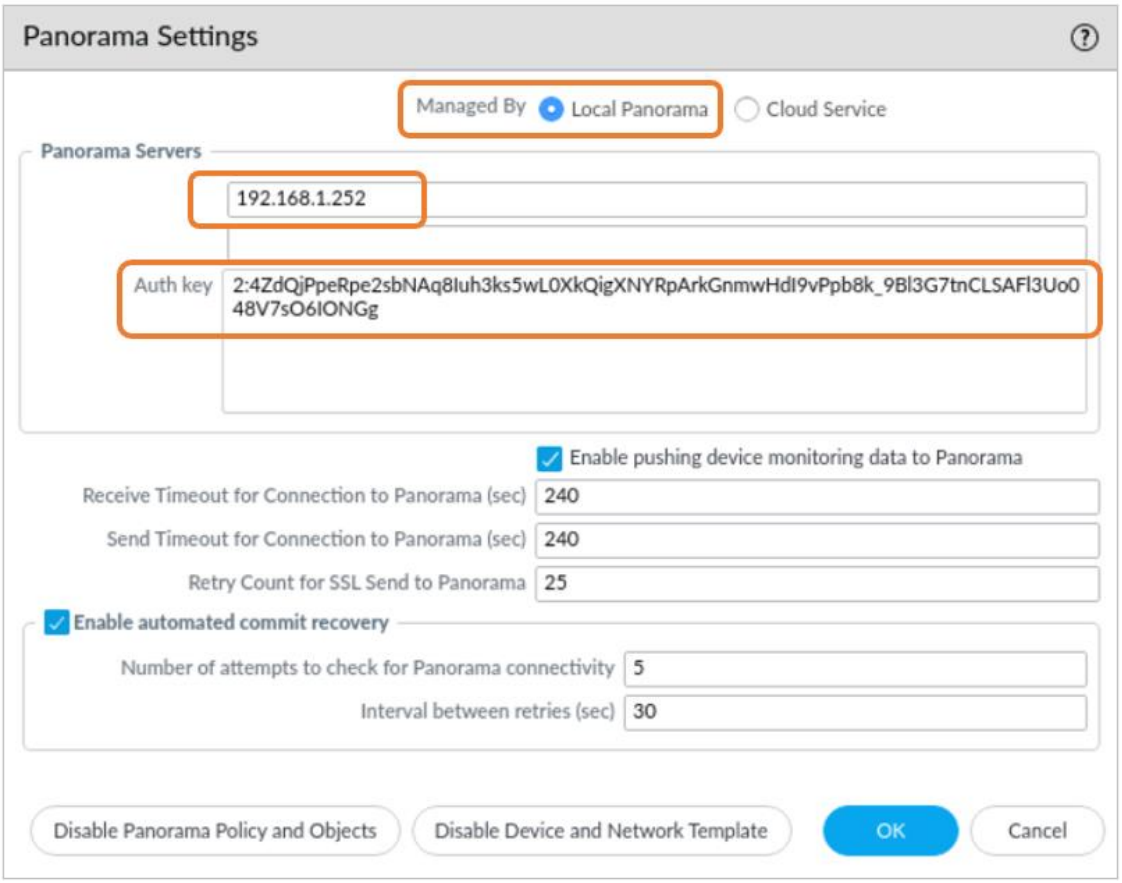
38. Click **OK**.
39. The **Managed Devices** > **Summary** window shows both firewalls listed by serial number, along with information about each one.

Note: Both firewalls will have a **Device State** of **Disconnected** until they establish communication with Panorama.

Configure firewall-a to Communicate with Panorama

Add the Auth Key and the IP address of Panorama to firewall-a.

40. In the web interface for firewall-a, select **Device** > **Setup** > **Management**.
41. Click the gear icon in the **Panorama Settings** section, which allows you to edit these settings.
42. For **Managed By**, select the radio button for **`Local Panorama`**.
43. In the **Panorama Servers** field, enter **`192.168.1.252`**.
44. In the Auth key field, copy the value from the Text Editor file and paste it in:



45. Leave the other settings unchanged.
46. Click **OK**.

Set the Location of firewall-a

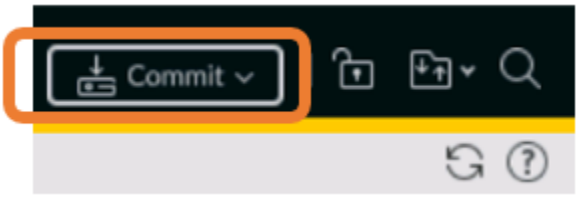
Change the hostname for firewall-a and modify the latitude and longitude to match the location city.

47. In the web interface for firewall-a, navigate to **Device > Setup > Management**.
48. In the **General Settings** section, click the **gear** icon.
49. Set the **Hostname** to **`chicago-fw`**.
50. Set the **Domain** to **`panw.lab`**.
51. Verify that the **Time Zone** is set to **Europe/Dublin**.
52. Set the **Latitude** to **`41.00`**.
53. Set the **Longitude** to **`87.00`**.

These are the latitude and longitude settings for Chicago, Illinois. The correct firewall location allows Panorama to place the firewall properly on maps and reports.

54. Leave the remaining settings unchanged:

55. Click **OK** to close the **General Settings** window.
56. Apply these changes to firewall-a by clicking **Commit** in the upper-right corner of the browser.



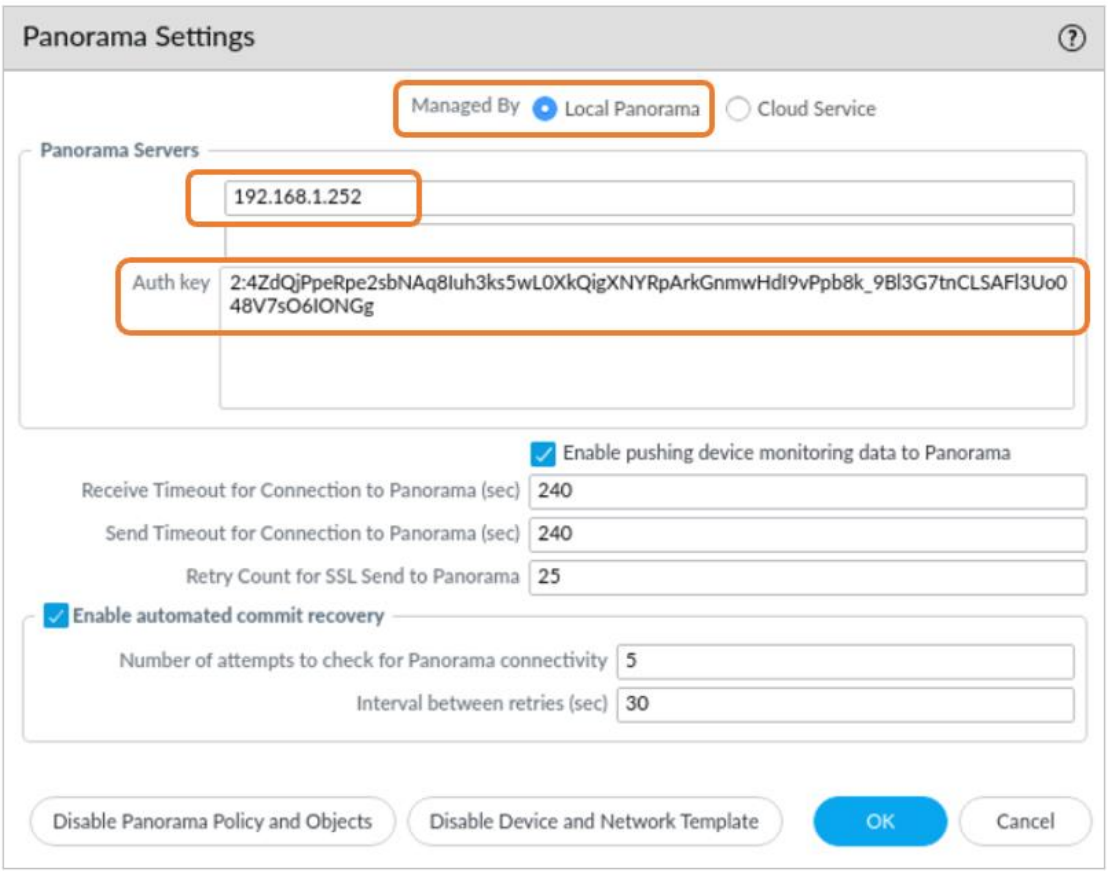
57. When the **Commit** window appears, click the **Commit** button.
58. When the commit status is complete, click **Close**.

Configure firewall-b to Communicate with Panorama

Add the Auth Key and the IP address of Panorama to firewall-b.

59. In the web interface for firewall-b, select **Device > Setup > Management**.
60. Click the gear icon in the **Panorama Settings** section, which allows you to edit these settings.

61. In the **Panorama Servers** field, enter **`192.168.1.252`**.
62. In the Auth key field, copy the value from the Text Editor file and paste it in:



63. Leave the other settings unchanged.
64. Click **OK**.

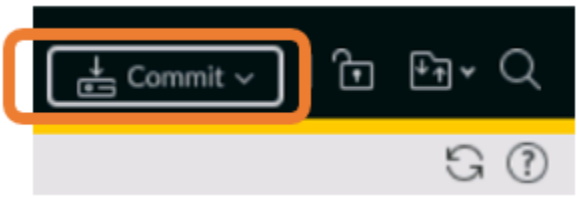
Set the Location of firewall-b

Change the hostname for firewall-b and modify the latitude and longitude to match the location city.

65. In the web interface for firewall-b, navigate to **Device** > **Setup** > **Management**.
66. In the **General Settings** section, click the **gear** icon.
67. Change the **Hostname** from firewall-b to **`berlin-fw`**.
68. Set the **Domain** to **`panw.lab`**.
69. Verify that the **Time Zone** is set to **Europe/Dublin**.
70. Set the **Latitude** to **`52.00`**.
71. Set the **Longitude** to **`13.00`**.

    These are the coordinates for Berlin, Germany.
72. Leave the remaining settings unchanged:

73. Click **OK** to close the **General Settings** window.
74. Apply these changes to firewall-b by clicking **Commit** in the upper-right corner of the browser.



75. When the **Commit** window appears, click the **Commit** button.
76. When the commit status is complete, click **Close**.

Commit the Changes to Panorama

77. In the Panorama web interface, commit these changes to Panorama by clicking the **Commit** option in the upper-right corner.
78. Select **Commit to Panorama**.
79. Click **Commit** in the bottom-right corner.
80. When the commit **Status** is **Completed**, click **Close**.
81. Close the **Text Editor** application.

    You do not need to save the changes.

Verify that Both Firewalls are Connected to Panorama

82. In Panorama, navigate to **Panorama > Managed Devices > Summary**.
83. Periodically click the refresh  icon in the upper-right corner of the window.
84. After a few minutes, the **Device State** for both firewalls will change to **Connected**:

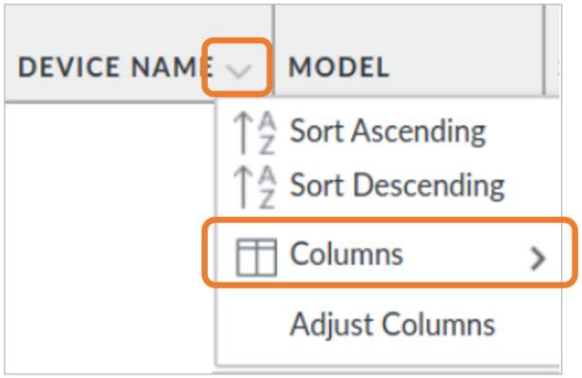
	DEVICE NAME	MODEL	SERIAL NUMBER	IP Address IPV4	VARIABLES	TEMPLATE	DEVICE STATE
	No Device Group Assigned (2/2 Devices Connected)						
	chicago-fw	PA-VM	0070510...	192.168.1.254			Connected
	berlin-fw	PA-VM	0070510...	192.168.1.253			Connected

Several columns in the preceding screenshot have been hidden so that the image will fit better on the page. Notice that the **Device Name** listed in Panorama has changed to the hostnames you assigned instead of the serial numbers.

Modify Columns in the Summary Window

In this section, you will modify the columns available in the **Summary** window of Panorama so that you have quick access to helpful information about the managed firewalls.

85. Navigate to **Panorama** > **Managed Devices** > **Summary**.
86. To the right of any column header, click the small triangle. This example shows the triangle next to the **Device Group** column header:



87. Select **Columns** and notice that many of the options currently are checked.
88. **Select** the following items:

- Device Group
- Model
- Tags
- Serial Number
- IP Address IPV4
- Variables
- Template
- Status Device State
- Status Template
- Status Template Last Commit State
- Software Version
- Apps and Threat
- Antivirus
- URL Filtering
- WildFire
- Backups

Modifying the columns displayed in this **Summary** window is optional. Your choice of columns to display in a production environment obviously will depend on the categories of firewall information you are most concerned about.

89. After you have completed selecting and unselecting the columns, scroll back and forth in the **Summary** window to examine the available information.
90. Drag and drop the **IP Address** column between the **Device Name** and **Model** columns.

Note that you can rearrange the order of columns in the **Summary** table. You may prefer to see columns at the far right without scrolling. All tables in Panorama allow you to rearrange columns to fit your needs.

Verify Firewall Licenses in Panorama

Use Panorama to examine licenses for both firewalls.

91. Navigate to **Panorama > Device Deployment > Licenses**.
92. Verify the licenses for both firewalls:

DEVICE	VIRTUAL SYSTEM	THREAT PREVENTI...	URL	SUPPORT	GLOBALPR... GATEWAY	GLOBALPR... PORTAL	WILDFIRE	VM-SERIES CAPACITY	DNS SECURITY
chicago-fw	⊗	✓ Expires: 2/14/2023	✓ PaloAlto Networks Expires: 2/14/2023	✓ Expires: 2/14/2023	✓ Expires: 2/14/2023	✓	✓ Expires: 2/14/2023	✓	✓ Expires: 2/14/2023
berlin-fw	⊗	✓ Expires: 2/14/2023	✓ PaloAlto Networks Expires: 2/14/2023	✓ Expires: 2/14/2023	✓ Expires: 2/14/2023	✓	✓ Expires: 2/14/2023	✓	✓ Expires: 2/14/2023

Note that the details of each license on your Devices may differ from the example shown.

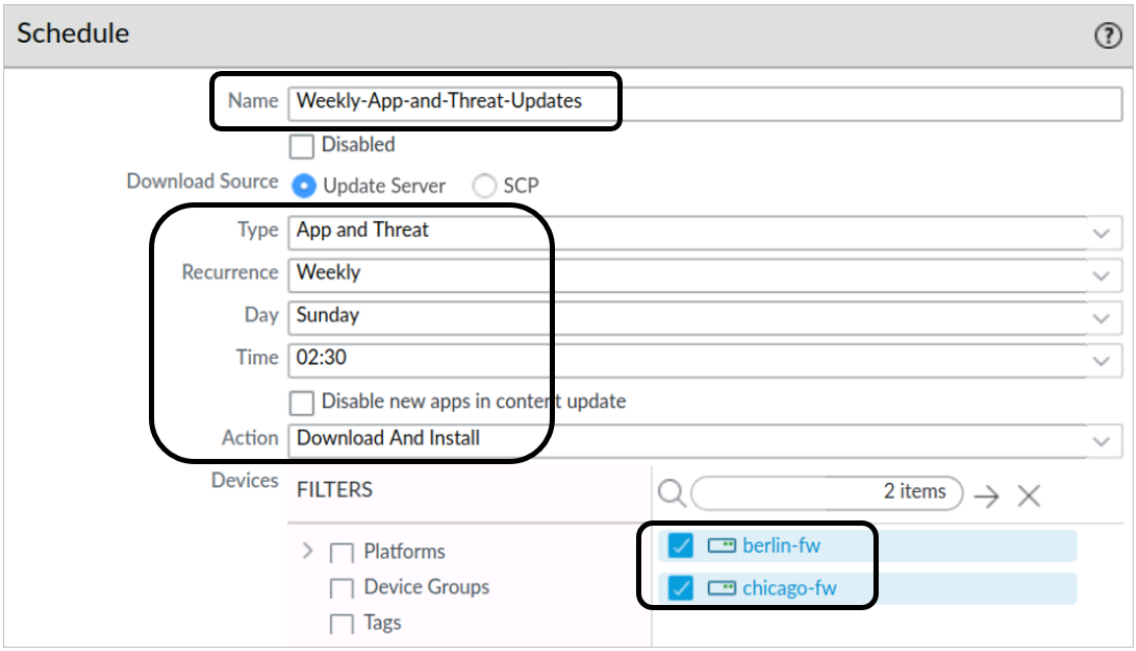
Schedule Dynamic Updates to Firewalls

In this section, you will configure Panorama with schedules to automatically download and install dynamic updates on both managed firewalls. This process is separate from scheduling dynamic updates for Panorama itself (which you configured in Lab 1).

You will configure these schedules to occur every Sunday morning.

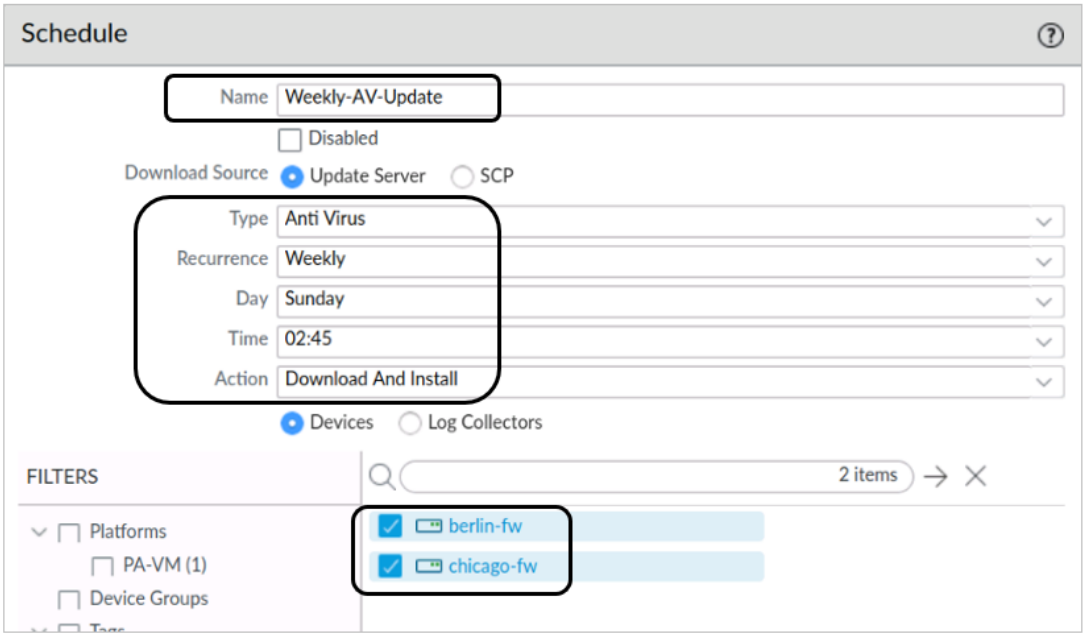
93. Navigate to **Panorama > Device Deployment > Dynamic Updates**.
94. Click the Check Now button in the lower left corner of the window.
    This action instructs Panorama to retrieve the latest Content ID information.
95. Create a **Schedule** for **Applications and Threat** updates by clicking the **Schedules** button at the bottom of the window.
96. In the **Schedules** window, click **Add**.
97. For **Name**, enter **`Weekly-App-and-Threat-Updates`**.
98. For **Type**, select **App and Threat**.
99. For **Recurrence**, select **Weekly**.
100. For **Day**, select **Sunday**.
101. For **Time**, select **02:30**.
102. Select **Download And Install** from the **Action** drop-down list.

103. Check the boxes for both **berlin-fw** and **chicago-fw**:

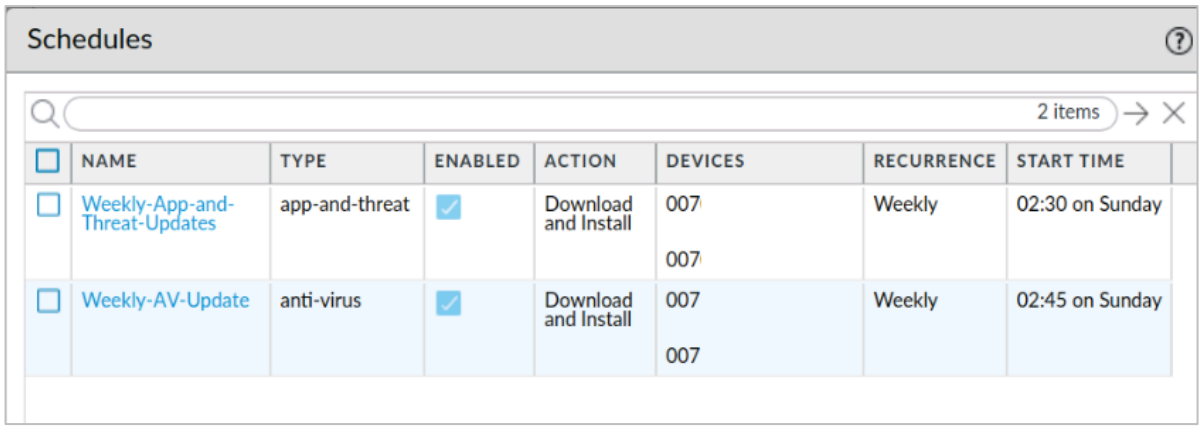


104. Leave the remaining settings unchanged.
105. Click **OK**.
106. In the **Schedules** window, create a **Schedule** for Antivirus by clicking **Add**.
107. For **Name**, enter **`Weekly-AV-Update`**
108. For **Type**, select **Anti Virus**.
109. For **Recurrence**, select **Weekly**.
110. For **Day**, select **Sunday**.
111. For **Time**, select **02:45**.
112. Select **Download And Install** from the **Action** drop-down list.

113. Check the boxes for both **`berlin-fw`** and **`chicago-fw`**:



114. Leave the remaining settings unchanged.
115. Click **OK**.
116. Your **Schedules** window should contain entries for **app-and-threat** and **anti-virus** updates:



You should stagger the **Start Time** for each schedule so that Panorama does not perform these tasks at the same time.

117. Click **Close**.

In this lab environment, you are setting the downloads to occur each week.

In a production environment, you should follow the recommended guidelines for Dynamic Updates provided by Palo Alto Networks.

For more information on this topic, log in to live.paloaltonetworks.com and search for "Best Practices for Applications and Threats Content Updates" to locate the most recent article.

Commit the Changes to Panorama

118. Commit these changes to Panorama by clicking the **Commit** option in the upper-right corner.
119. Select **Commit to Panorama**.
120. Click **Commit** in the bottom-right corner.
121. When the commit **Status** is **Completed**, click **Close**.

Stop. This is the end of the lab.

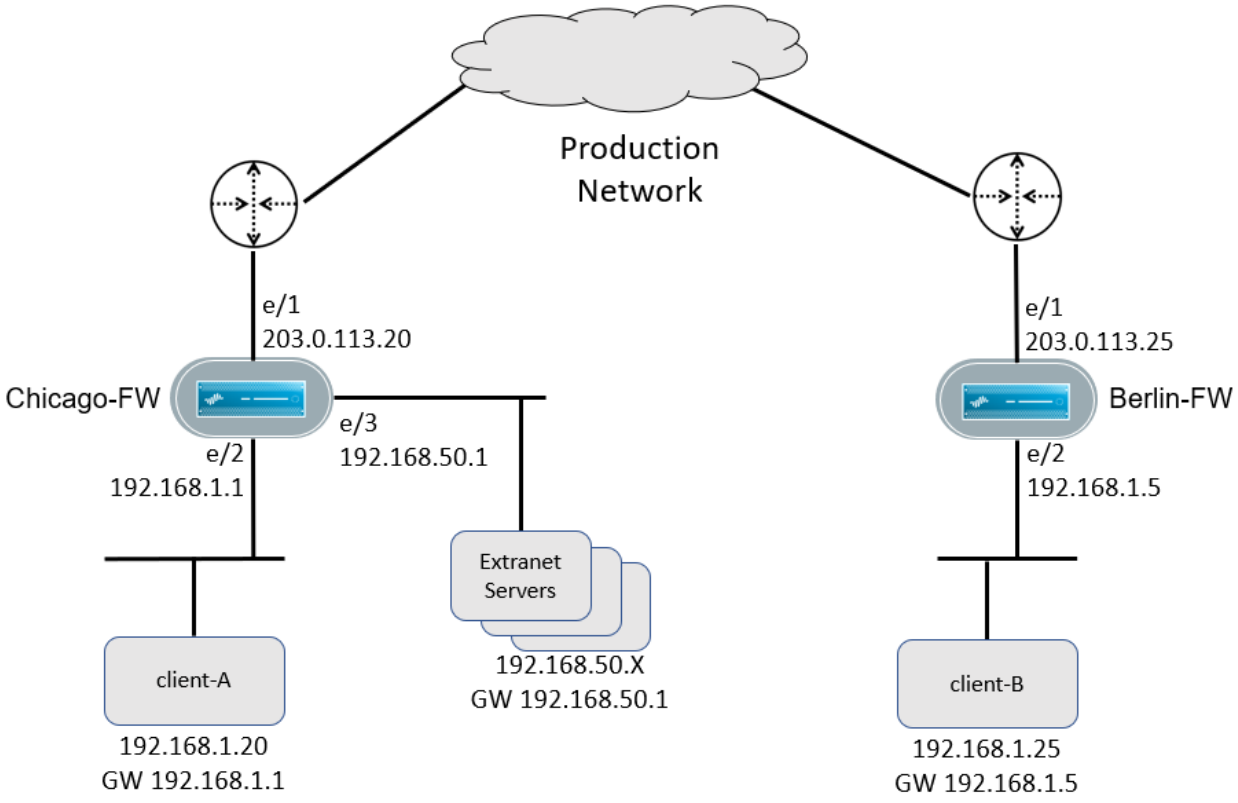
Lab 3 Scenario: Templates

The firewalls managed by Panorama contain several common settings. Rather than configure these common settings separately on each firewall, you want to define them in Panorama Templates. You then can push a Template stack to the firewalls and apply the common settings across both Devices.

As a part of the Template deployment process, you also will use variables to define interface IP addresses for both firewalls.

You will change the default gateway for the management interfaces of Panorama and for the Berlin-FW and Chicago-FW. Management traffic for these hosts will be subject to Security policy rules on each firewall.

For the production network, the client-A traffic will flow through the Chicago firewall. client-B traffic will flow through the Berlin firewall. Traffic from the extranet servers will flow through the Chicago firewall:



Lab Objectives

- Create a Global-Settings Template
- Configure the Global-Settings Template
    - General Settings
    - Log Settings
    - Administrator
    - Interface Management Profiles
    - Interfaces Variables
    - Network Interfaces
    - Firewall Management Interface
    - Logical Router
    - Security Zones
- Create a Template for the Americas region
- Create a Syslog Server Profile in the Region-Americas Template
- Create an Email Server Profile in the Region-Americas Template
- Clone Region-Americas Template to create Region-Europe Template
- Edit settings in the Region-Europe Template
- Change the Header Banner in the Region-Europe Template
- Create a Template Stack for Germany firewalls
- Create a Template Stack for US firewalls
- Modify Variables for firewalls
- Push the Template Stacks to firewalls
- Verify Template settings on the Chicago firewall
- Verify Template settings on the Berlin firewall

High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-3-Start.xml** configuration file on Panorama.

Create a Global-Settings Template

- Use the information below to create a new Template called Global-Settings:

Name	**Global-Settings**
Description	**Network - Interfaces, Zones, Logical Router** **Device – Login Banner, Domain, Panorama Servers, Log Settings**

Configure the Global-Settings Template – General Settings

- Use the information below to configure the Global-Settings Template:

General Settings	
Domain	**panw.lab**
Login Banner	**Authorized access only**
Management	
Panorama Servers	**192.168.1.252**

Configure the Global-Settings Template – Log Settings

- Use the information below to create a new log forwarding entry so that firewalls will send their System log entries to Panorama:

Log Type	**System**
Name	**Firewall_System_Logs_to_Panorama**
Description	**Sends all firewall system log entries to Panorama**
Forward Method	**Panorama/Cortex Data Lake**

- Use the information below to create a new log forwarding entry so that firewalls will send their Configuration log entries to Panorama:

Log Type	**Configuration**
Name	**Firewall_Configuration_Logs_to_Panorama**
Description	**Sends all firewall configuration log entries to Panorama**
Forward Method	**Panorama/Cortex Data Lake**

Commit the Changes to Panorama

- Commit these changes to Panorama.

Configure the Global-Settings Template – Administrator

- Create a new Dynamic Superuser administrator account called **globaladmin** with a password of **Pal0Alt0!**

Create Interface Management Profiles

- Use the information below to create two Interface Management profiles:

Name	**Allow-ping**
Network Services	**Ping**

Name	**Allow-management**
Administrative Management Services	**HTTPS** **SSH**
Network Services	**Ping** **SNMP** **Response Pages**

Create Interface Variables

- Use the information below to create three variables to use for Interfaces in the Global-Settings Template:

Name	**$Internet-Interface**

Type	**IP Netmask**
Type Value	**1.1.1.1/24**
Description	**Internet interface**

Name	**$Users_Net-Interface**
Type	**IP Netmask**
Type Value	**2.2.2.2/24**
Description	**User network interface**

Name	**$Extranet-Interface**
Type	**IP Netmask**
Type Value	**3.3.3.3/24**
Description	**Extranet interface**

Commit the Changes to Panorama

- Commit these changes to Panorama.

Create Network Interfaces

- Use the information below to create three Ethernet Interfaces in the Global-Settings Template:

Slot	**Slot 1**
Interface Name	**ethernet1/1**
Comment	**Internet interface**
Interface Type	**Layer 3**
IPv4 Address	**$Internet-Interface**
Management Profile	**Allow-ping**

Slot	**Slot 1**
Interface Name	**ethernet1/2**
Comment	**Users_Net interface**
Interface Type	**Layer 3**
IPv4 Address	**$Users_Net-Interface**
Management Profile	**Allow-management**

Slot	**Slot 1**
Interface Name	**ethernet1/3**
Comment	**Extranet interface**
Interface Type	**Layer 3**
IPv4 Address	**$Extranet-Interface**
Management Profile	**Allow-management**

Modify Firewall Management Interface Settings

- Set the Default Gateway for the Management interface in the Global-Settings Template to 192.168.1.1
- Limit access to the firewall management address to the 192.168.0.0/16 network.

Create a Logical Router

- Create a **Logical Router** called **LR-1**
- Add **ethernet1/1**, **ethernet1/2** and **ethernet1/3** to the LR-1 Logical Router.
- Create a **Static Route** in the LR-1 Logical Router called **Firewall-Default-Gateway**
    - The default gateway for the firewalls should send traffic through **ethernet1/1** with a **Next Hop IP Address** of **203.0.113.1**

Create Security Zones

- Use the information below to create three Security Zones:

Name	**Internet**
Type	**Layer 3**
Interfaces	**ethernet1/1**

Name	**Users_Net**
Type	**Layer 3**
Interfaces	**ethernet1/2**
Enable User Identification	**Checked**

Name	**Extranet**
Type	**Layer 3**
Interfaces	**ethernet1/3**
Enable User Identification	**Checked**

Commit This New Template to Panorama

- Commit these changes to Panorama.

Create a Template for the Americas Region

- Create a **Template** called **`Region-Americas`** with a **Description** of **`Browser banner and server profiles`**
- Modify the **Banner and Messages** section of the Region-Americas Template so that the **Header Banner** reads **`This is an Americas firewall`**
- Set the **Header Color** for the Region-Americas Template to **`Red`**

Create a Syslog Server Profile in the Region-Americas Template

- Use the information below to create a syslog server profile in the Region-Americas Template:

Name	**Syslog_Servers**
Location	**Shared**
Servers Section	
Name	**US-Syslog-1**
Syslog Server	**192.168.50.55**

Create an Email Server Profile in the Region-Americas Template

- Use the information below to create an email server profile in the Region-Americas Template:

Name	**Email-Servers**
Location	**Shared**
Servers Section	
Name	**US-Mail-1**
Email Display Name	**Chicago Firewall**
From	**chicago-fw@panw.lab**
To	**paloalto42@panw.lab**
Email Gateway	**192.168.50.150**

Commit the Changes to Panorama

- Commit these changes to Panorama.

Clone Region-Americas Template to Create Region-Europe Template

- Clone the Region-Americas Template and rename the clone Region-Europe

Edit Settings in the Region-Europe Template

- In the **Region-Europe** Template, change the server name in the **Syslog_Servers** profile to **`EU-Syslog-1`**
- In the **Region-Europe** Template, change the following settings in the **Email-Servers** profile:
    - Change the **Name** of the server to **`EU-Mail-1`**
    - Change the **Email Display Name** to **`Berlin Firewall`**
    - Change the **From** value to **`berlin-fw@panw.lab`**
    - Leave the remaining settings unmodified.

Change the Header Banner

- In the **Region-Europe** Template, change the **Header Banner** to read **`This is a Europe Firewall`**
- Change the color of the **Header** to **`Orange`**

Commit the Changes to Panorama

- Commit these changes to Panorama.

Create Template Stacks

- Create two Template stacks (see below).

Create a Template Stack for Germany Firewalls

- Use the information below to create a Template Stack:

Name	**`Germany-Stack`**
Description	**`Contains settings for firewalls in Germany`**
Templates	**`Global-Settings`** **`Region-Europe`**
Firewall	**`Berlin`**

Create a Template Stack for US Firewalls

- Use the information below to create a Template Stack:

Name	**US-Stack**
Description	**Contains settings for firewalls in US**
Templates	**Global-Settings** **Region-Americas**
Firewall	**Chicago**

Commit the Changes to Panorama

- Commit these changes to Panorama.

Modify Variables for Firewalls

- Locate the **variables_Germany-Stack.csv** file in the Lab-Files/EDU-220 folder on the client desktop and open the file with the Text editor so you can see the structure.
- Close the file.
- Import the **variables_Germany-Stack.csv** file to the **Germany-Stack** Template Stack.
- Import the **variables_US-Stack.csv** file to the **US-Stack** Template Stack.

Verify the Variables for Each Template Stack

- Use the **Device Key-Value Table** to verify that the appropriate values have been applied to each firewall for the interface variables.

Commit the Changes to Panorama

- Commit these changes to Panorama.

Push the Template Stacks to Firewalls

- Use **Commit > Push to Devices**
- Use the **Edit Selections** option to **Force Template Values**
- Make certain to push the Germany-Stack to the berlin-fw and the US-Stack to the chicago-fw.
- Use the **Task Manager** to confirm that the commit process succeeded for both firewalls.

Verify Template Settings on the Chicago Firewall

- Log out and then log back in to the Chicago firewall web interface with the **admin/Pal0Alt0!** credentials.
- Verify that the following settings have been applied from Panorama to the Chicago firewall:

ethernet1/1 IP Address	**203.0.113.20/24**
ethernet1/2 IP Address	**192.168.1.1/24**
ethernet1/3 IP Address	**192.168.50.1/24**
Extranet Security Zone	**ethernet1/3** **User-ID Enabled**
Internet Security Zone	**ethernet1/1**
Users_Net Security Zone	**ethernet1/2** **User-ID Enabled**
Domain	**panw.lab**
Login Banner	**Authorized access only**
Syslog Server Profile Server Name	**US-Syslog-1**
Email Server Profile Server Name	**US-Mail-1**

Verify Template Settings on the Berlin Firewall

- Log out and then log back in to the Berlin firewall web interface with the **admin/Pal0Alt0!** credentials.
- Verify that the following settings have been applied from Panorama to the Berlin firewall:

ethernet1/1 IP Address	**203.0.113.25/24**
ethernet1/2 IP Address	**192.168.1.5/24**
ethernet1/3 IP Address	**192.168.50.5/24**
Extranet Security Zone	**ethernet1/3**

	`User-ID Enabled`
Internet Security Zone	`ethernet1/1`
Users_Net Security Zone	`ethernet1/2` `User-ID Enabled`
Domain	`panw.lab`
Login Banner	`Authorized access only`
Syslog Server Profile Server Name	`EU-Syslog-1`
Email Server Profile Server Name	`EU-Mail-1`

Detailed Lab Steps

Load the Lab Start Configuration File

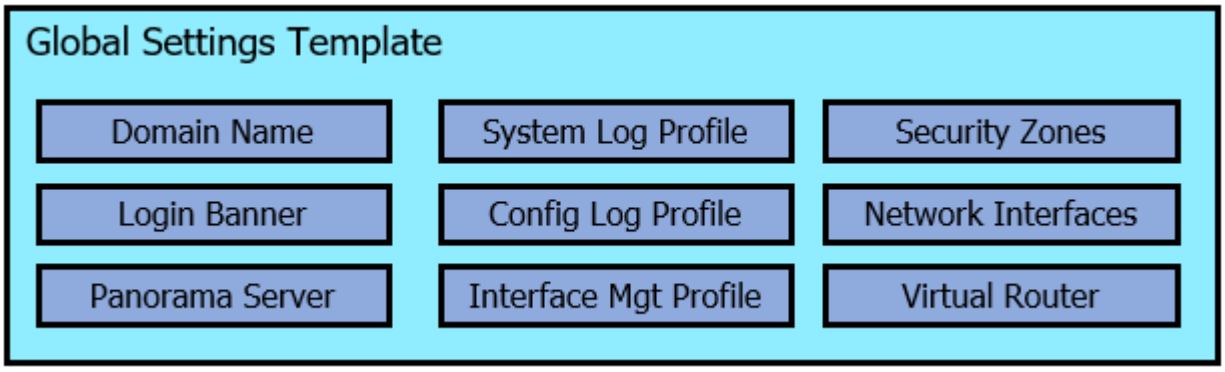
1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-3-Start.xml**.

Leave the remaining settings unchanged.

4. Click **OK** to close the **Load Named Configuration** window.
5. Click **Close** on the **Loading Configuration** window.
6. Commit the changes to Panorama by selecting **Commit** > **Commit to Panorama** in the upper-right corner of the window.
7. In the **Commit to Panorama** window, click **Commit**.
8. Allow the process to complete.
9. Click **Close** in the **Commit Status** window.

Create a Global-Settings Template

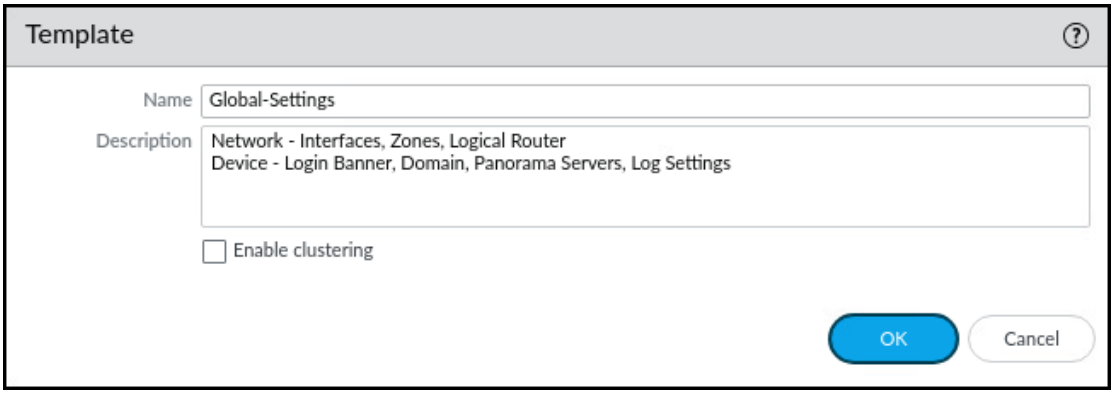
In this section, you will create the first of several Templates. This Template will contain general settings to be applied to all firewalls. Configuring common management settings in a dedicated template allows you to use the same management settings for all of your firewalls regardless of how those devices are deployed.



10. Select **Panorama** > **Templates**.
11. In the bottom-left corner of the window, click **Add**. The **Template** window opens.
12. In the **Name** field, enter **`Global-Settings`**.
13. In the **Description** field, enter the following:

    `Network - Interfaces, Zones, Logical Router`

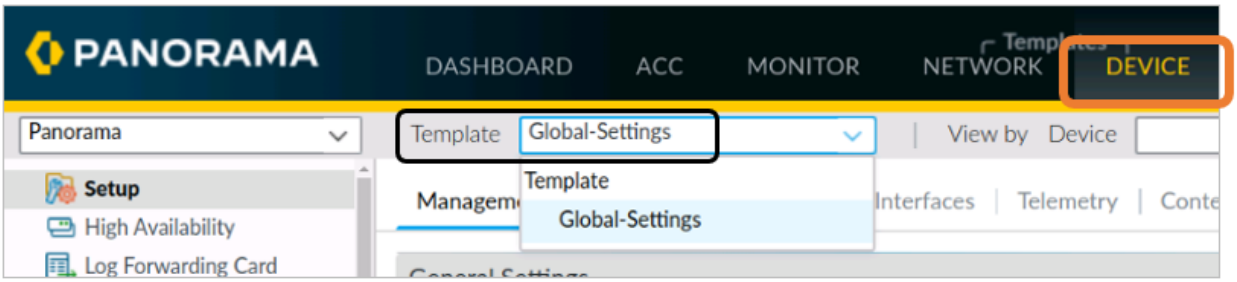
    `Device – Login Banner, Domain, Panorama Servers, Log Settings`



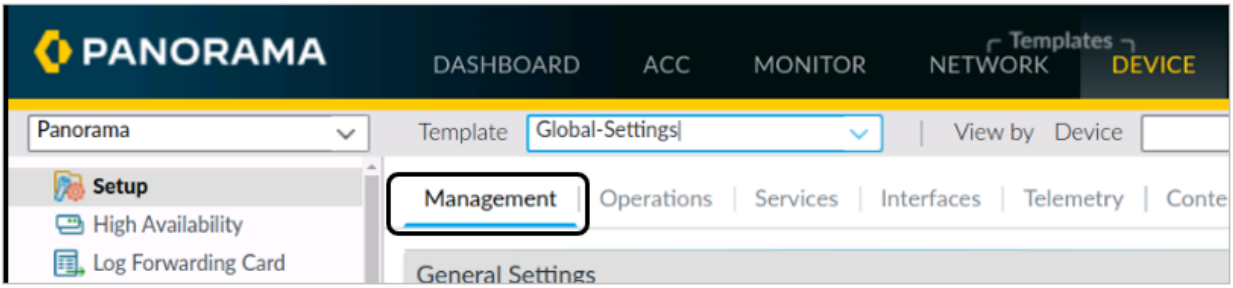
14. Click **OK**.
15. Notice that the **Network** tab and **Device** tab now appear:

Configure the Global-Settings Template – General Settings

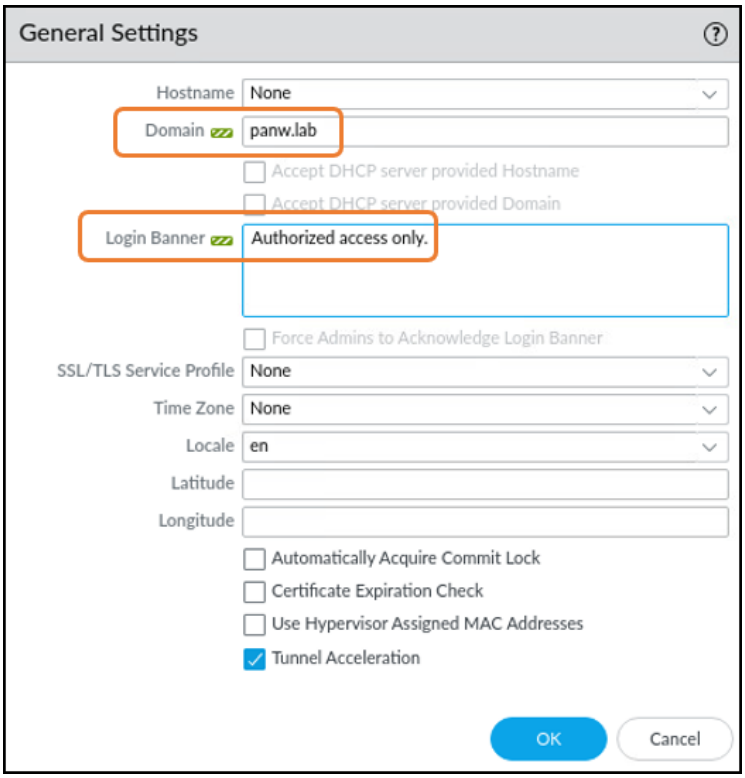
16. In Panorama, select the new tab under the **Templates** heading for **Device**.
17. Select **Setup**.
18. From the **Templates** drop-down list, select **Global Settings**:



19. Select the **Management** tab:

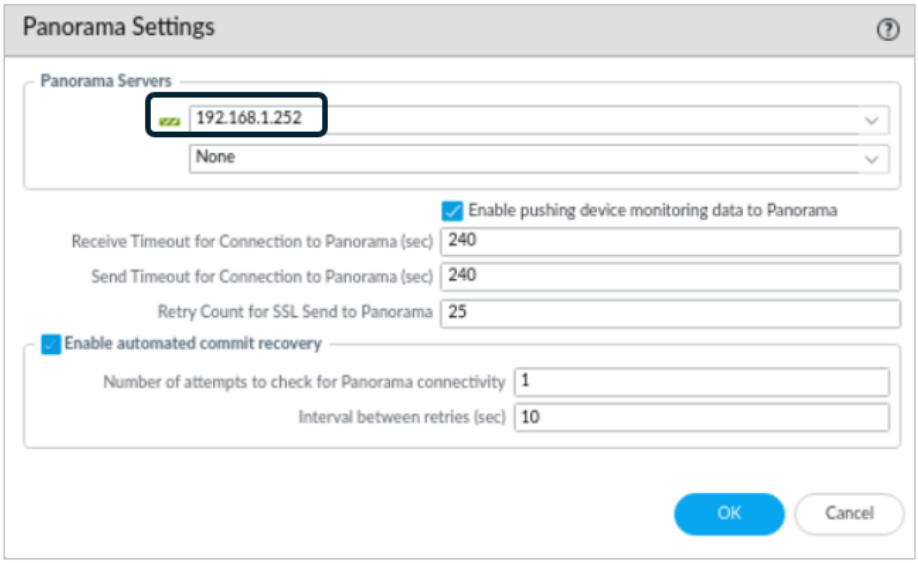


20. Click the **gear** icon to edit **General Settings**, and then enter the following values:
    - Domain: **`panw.lab`**
    - Login Banner: **`Authorized access only.`**
    - Leave the remaining settings unchanged:



21. Click **OK**.

22. In the right column of the **Management** tab, click the gear icon for **Panorama Settings**.
23. In the first field below **Panorama Servers**, enter **`192.168.1.252`**.
24. Leave the remaining fields unchanged:

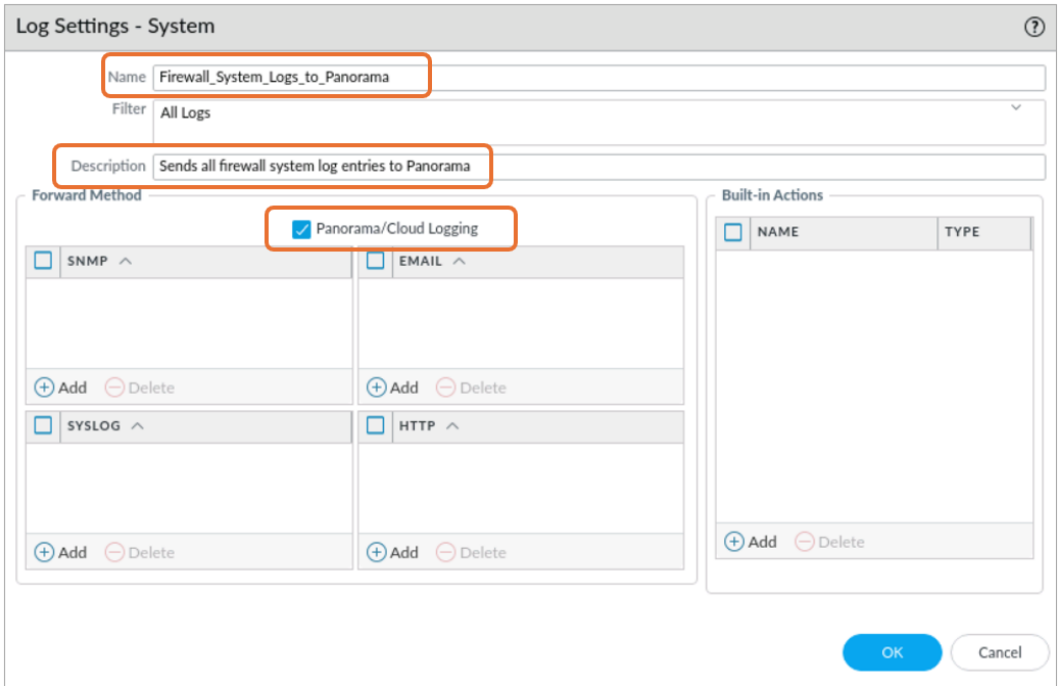


25. Click **OK**.

Configure the Global-Settings Template – Log Settings

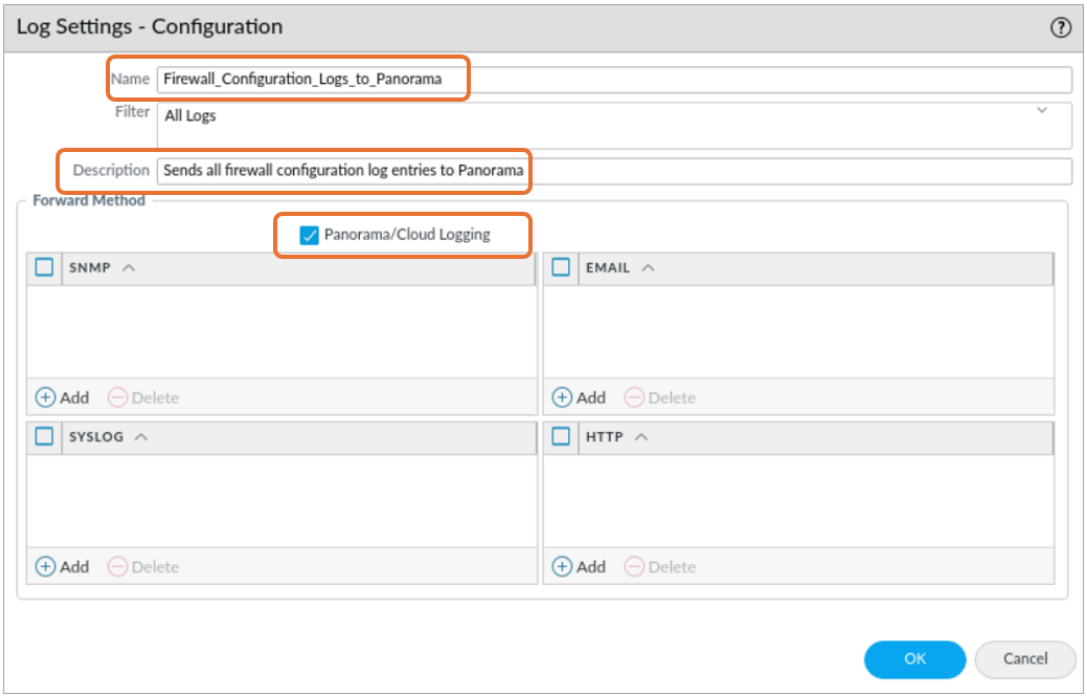
26. Select **Device > Log Settings**.
27. Under the section for **System**, click **Add**.
28. For **Name**, enter **`Firewall_System_Logs_to_Panorama`**.
29. For **Description**, enter **`Sends all firewall system log entries to Panorama`**.
30. In the **Forward Method** section, place a check in the box for **Panorama/Cloud Logging**.

31. Leave the remaining settings unchanged:

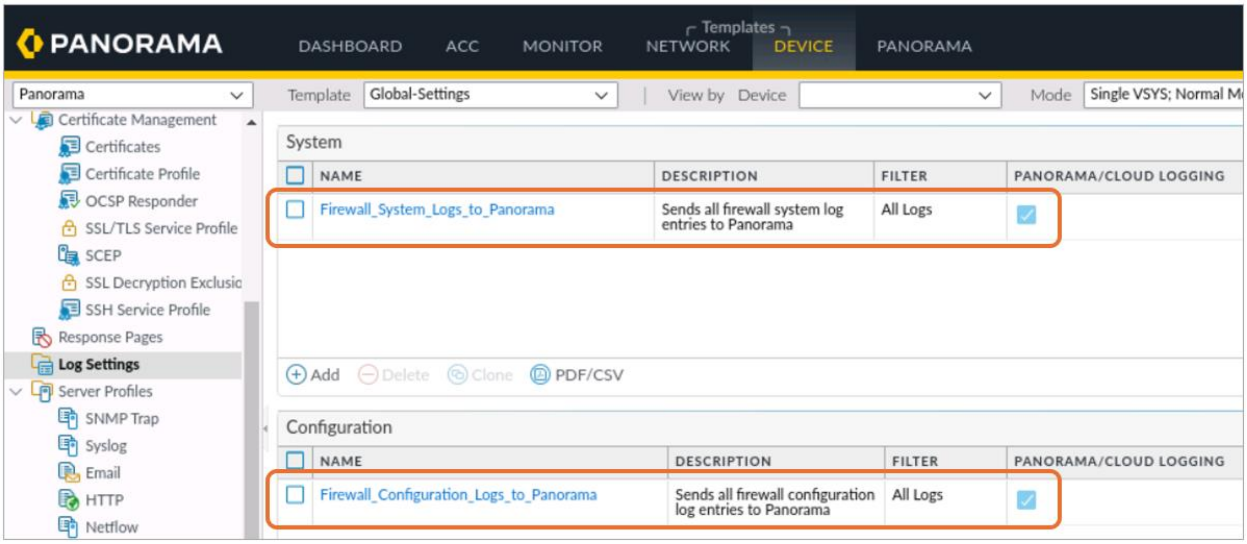


32. Click **OK**.
33. In the **Log Settings** window, under the section for **Configuration**, click **Add**.
34. For **Name**, enter **`Firewall_Configuration_Logs_to_Panorama`**.
35. For **Description**, enter **`Sends all firewall configuration log entries to Panorama`**.
36. In the **Forward Method** section, place a check in the box for **`Panorama/Cloud Logging`**.

37. Leave the remaining settings unchanged:



38. Click **OK**.
39. When the configuration process is complete, your **Log Settings** window should have an entry under **System** and an entry under **Configuration**:



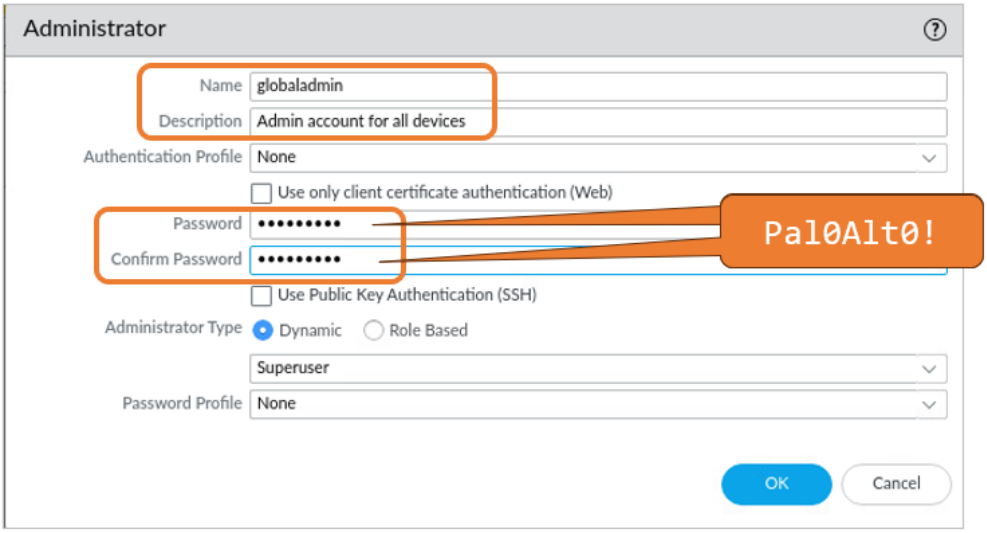
These log file settings are for firewall configuration and system entries. Firewall log forwarding for Threat, Traffic, and URL Filtering entries is configured in a different location. You will configure these settings later in the course.

Commit the Changes to Panorama

40. Commit these changes to Panorama by clicking the **Commit** option in the upper-right corner.
41. Select **Commit to Panorama**.
42. Click **Commit** in the bottom-right corner.
43. When the commit **Status** is **Completed**, click **Close**.

Configure the Global-Settings Template – Administrator

44. Select **Device > Administrators**.
45. Click **Add**.
46. For **Name**, enter **`globaladmin`**.
47. For **Description**, enter **`Admin account for all devices`**.
48. For **Password** and **Confirm Password**, enter **`Pal0Alt0!`**
49. Leave the remaining settings unchanged:



This administrator account will be pushed down to all firewalls and will allow you to log in to a managed Device as a last resort if all other accounts are unavailable.

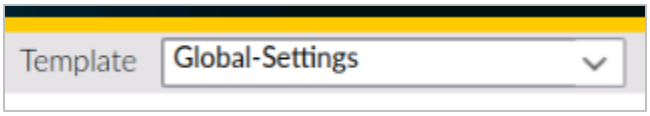
50. Click **OK**.

Create Interface Management Profiles

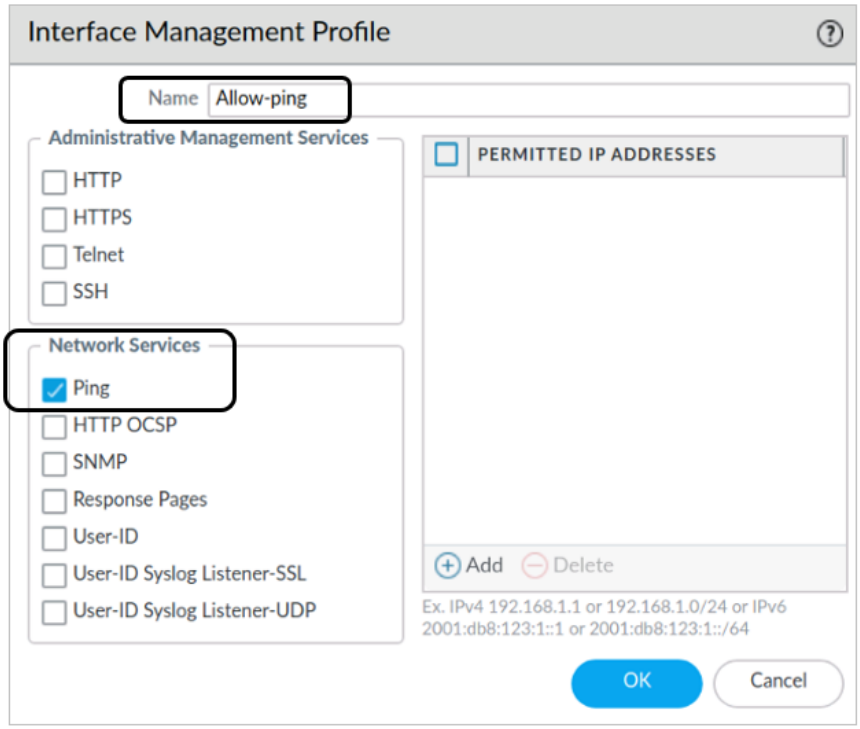
In this section, you will define Interface Management Profiles that dictate which services a firewall traffic interface will respond to. You define the profile and then apply it to one or more interfaces.

51. Select **Network > Network Profiles > Interface Mgmt**.

52. Verify that you have selected the **Global-Settings** Template from the **Template** drop-down list:

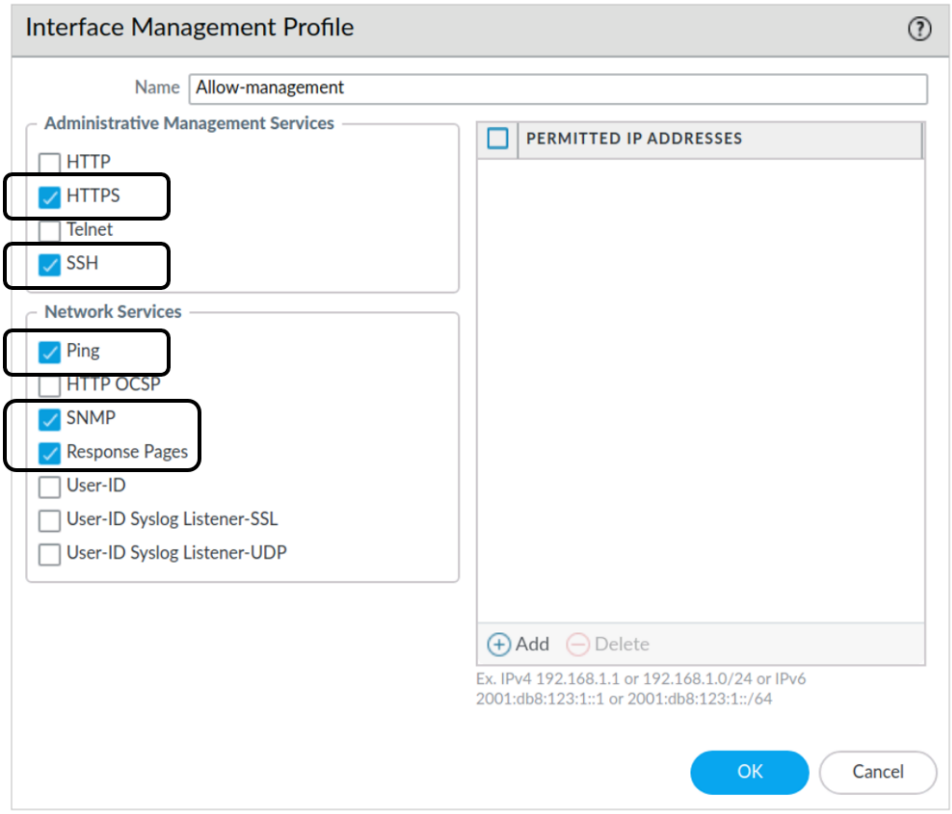


53. Click **Add**.
54. For **Name**, enter **`Allow-ping`**.
55. Place a check in the box for **Ping** under the **Network Services** area.
56. Leave the remaining settings unchanged:



57. Click **OK**.
58. Click **Add**.
59. For **Name**, enter **`Allow-management`**.
60. Check the boxes for **HTTPS** and **SSH** under the **Administrative Management Services** section.
61. Check the boxes for **Ping**, **SNMP**, and **Response Pages** under the **Network Services** area.

62. Leave the remaining settings unchanged:



63. Click **OK**.
64. You should have two entries in the **Interface Management** table:

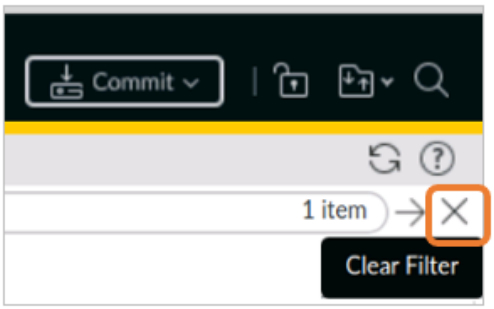
NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES
Allow-ping	☑	☐	☐	☐	☐	☐	☐	☐
Allow-management	☑	☐	☑	☐	☐	☑	☑	☑

Create Interfaces Variables

In this section, you will define variables that will be used for network interfaces instead of specific IP addresses.

65. Navigate to **Panorama** > **Templates**.

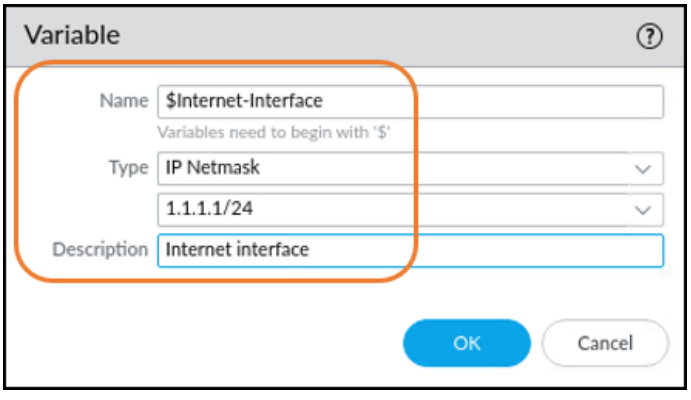
66. Clear any filters that might be in place by clicking the **Clear Filters** button in the upper-right corner of the window:



67. In the row for the **Global-Settings** Template, click the link for **`Manage…`** in the **Variables** column:

NAME	DESCRIPTION	TYPE	STACK	DEVICES	VARIABLES
Global-Settings	Network - Interfaces, Zones, Logical Router Device – Login Banner, Domain, Panorama Servers, Log Settings	template			Manage...

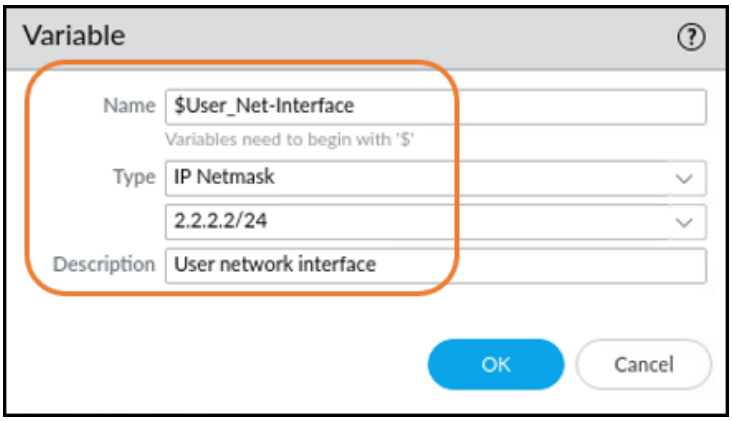
68. In the **Template Variables** window, click **Add**.
69. For **Name**, enter **`$Internet-Interface`**
70. Set the **Type** to **IP Netmask**.
71. In the field below the **Type**, enter **`1.1.1.1/24`** as the value.
72. Enter **`Internet interface`**, for **Description**:



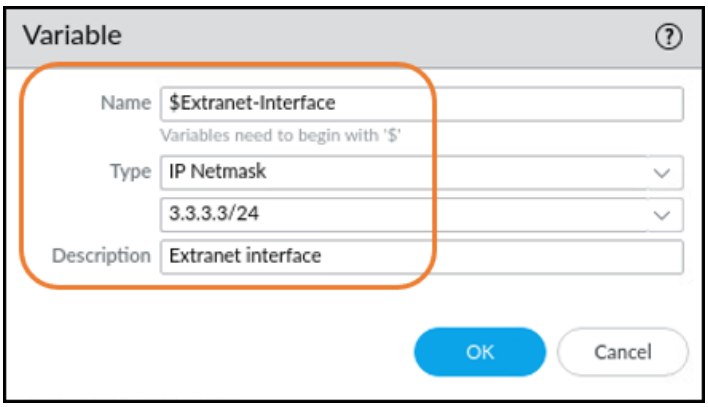
1.1.1.1/24 is a default value for this variable. Later in the lab, you will modify this default value for each firewall.

73. Click **OK**.
74. In the **Template Variables** window, click **Add**.

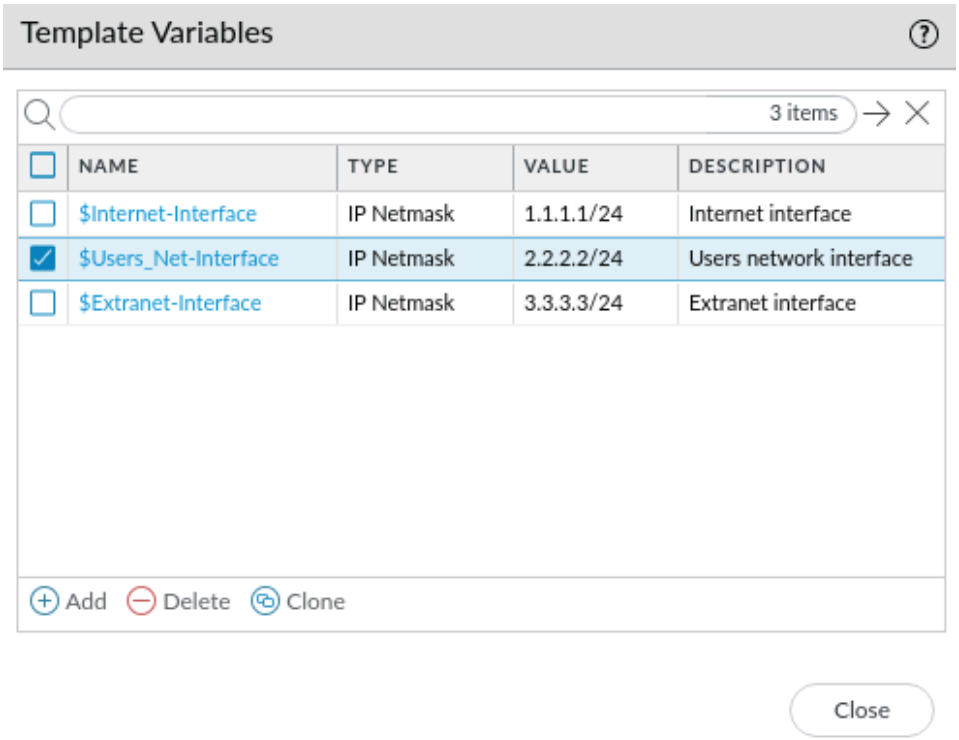
75. For **Name**, enter **`$Users_Net-Interface`**
76. Set the **Type** to **IP Netmask**.
77. In the field below the **Type**, enter **`2.2.2.2/24`** as the value.
78. Enter **`Users network interface`** for **Description**:



79. Click **OK**.
80. In the **Template Variables** window, click **Add**.
81. For **Name**, enter **`$Extranet-Interface`**
82. Set the **Type** to **IP Netmask**.
83. In the field to the right of the **Type**, enter **`3.3.3.3/24`** as the value.
84. Enter **`Extranet interface`** for **Description**:



85. Click **OK**.
86. When the configuration is complete, your **Template Variables** window should have three entries:



You will use these three variables when you define the network interfaces for your firewalls in the next section. The value you have assigned to each entry is a default setting; you cannot leave the **Value** field blank when you create variables.

87. Click **Close** in the **Template Variables** window.

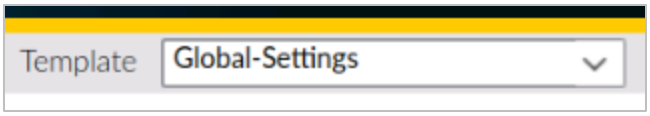
Commit the Changes to Panorama

88. Commit these changes to Panorama by clicking the **Commit** option in the upper-right corner.
89. Select **Commit to Panorama**.
90. Click **Commit** in the bottom-right corner.
91. When the commit **Status** is **Completed**, click **Close**.

Create Network Interfaces

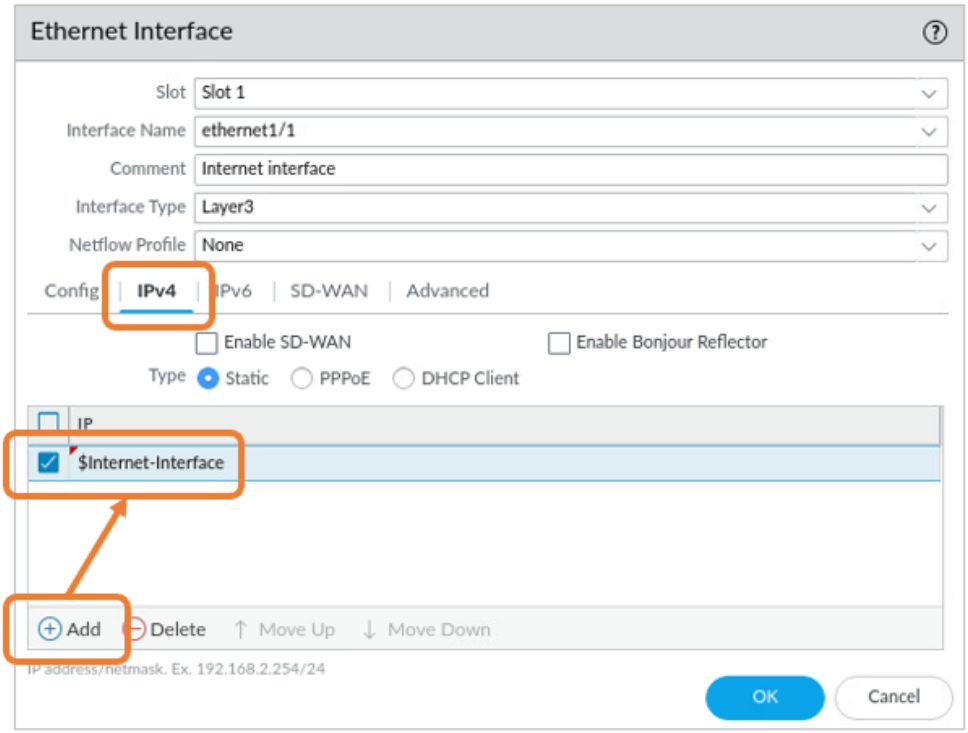
Now that you have defined the variables you will use for interfaces, you will create the network interface settings for your managed firewalls.

92. Select **Network** > **Interfaces** > **Ethernet**.
93. Verify that you have selected **Global-Settings** from the **Template** drop-down list:



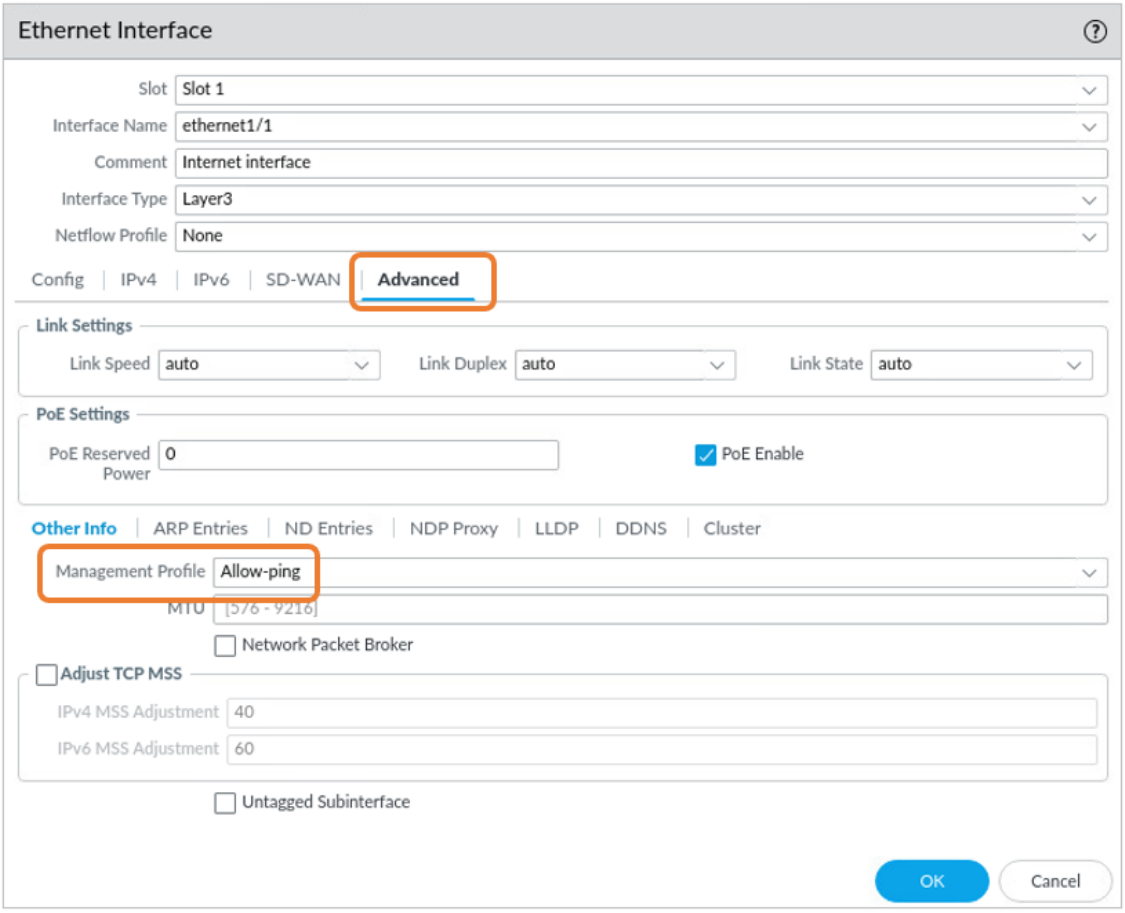
94. Click **Add Interface**.
95. For **Slot**, choose **Slot 1**.
96. For **Interface Name**, choose **ethernet1/1**.
97. For **Comment**, enter **`Internet interface`**.
98. For **Interface Type**, choose **Layer 3**:

99. Select the tab for **IPv4**.
100. Below the **IP** section, click **Add**.
101. Select **$Internet-Interface**:



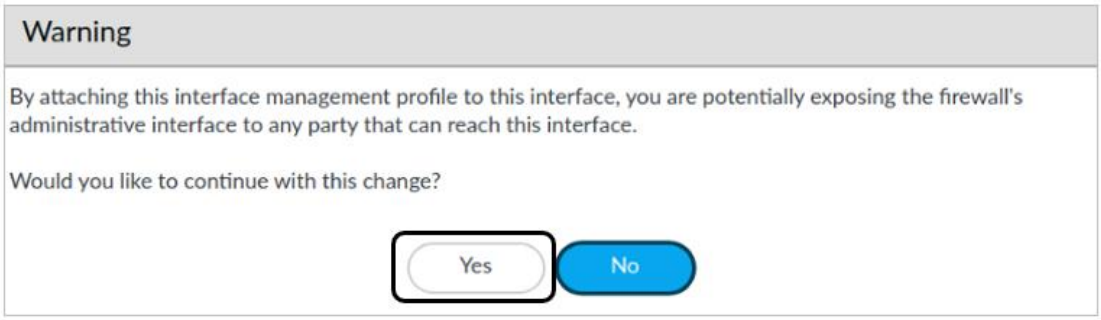
102. Select the tab for **Advanced**.

103. For **Management Profile**, select **Allow-ping**:

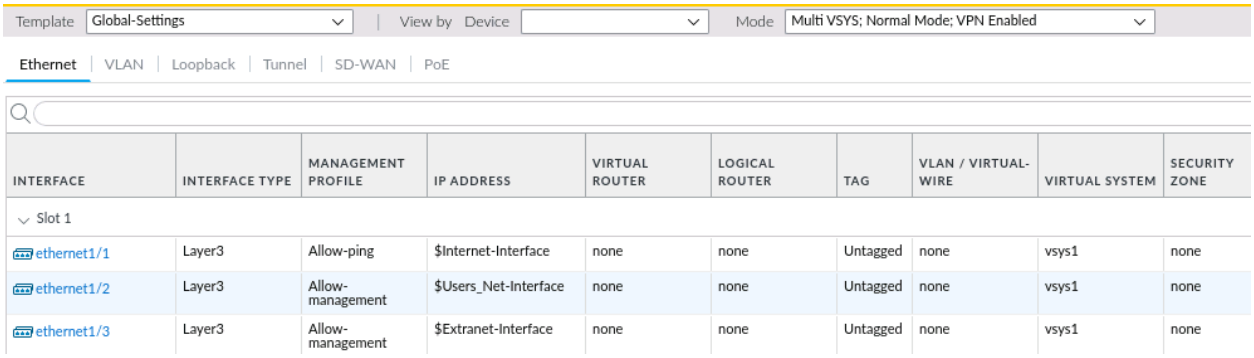


104. Click **OK** to return to the **Ethernet** window.
105. Click **Add Interface**.
106. For **Slot**, choose **Slot 1**.
107. For **Interface Name**, choose **ethernet1/2**.
108. For **Comment**, enter **`Users-Net interface`**.
109. For **Interface Type**, choose **Layer 3**.
110. In the **Ethernet Interface** window, select the tab for **IPv4**.
111. Below the **IP** section, click **Add**.
112. Select **$Users_Net-Interface**.
113. Select the tab for **Advanced**.
114. For **Management Profile**, select **Allow-management**.
115. Click **OK** to return to the **Ethernet** window.

116. Read the **Warning** message and then click **`Yes`** on the window:



117. In the **Ethernet** window, click **Add Interface** again.
118. For **Slot**, choose **Slot 1**.
119. For **Interface Name**, choose **ethernet1/3**.
120. For **Comment**, enter **`Extranet interface`**.
121. For **Interface Type**, choose **Layer 3**.
122. In the **Ethernet Interface** window, select the tab for **IPv4**.
123. Below the **IP** section, click **Add**.
124. Select **$Extranet-Interface**.
125. Select the tab for **Advanced**.
126. For **Management Profile**, select **Allow-management**.
127. Click **OK** to return to the **Ethernet** window.
128. Read the **Warning** message and then click **Yes** on the window.
129. When the configuration is complete, your **Global-Settings** Template should have three entries under the **Ethernet** tab:

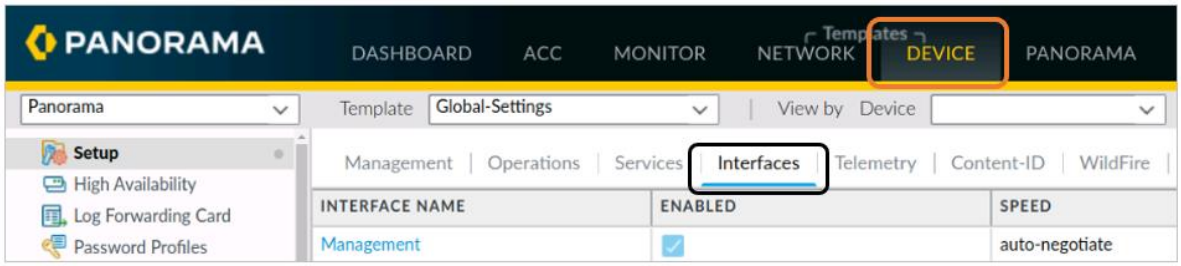


Note that some columns have been hidden in the previous screenshot.

Modify Firewall Management Interface Settings

In this section, you will create an entry in the Global-Settings Template that limits access to the firewall management interface from only hosts on the 192.168.0.0/16 network. You also will change the management interface gateway to 192.168.1.1 (ethernet1/1 of the chicago-fw).

130. Select **Device > Setup > Interfaces**:
131. From the **Template** drop-down list, select **Global-Settings**.

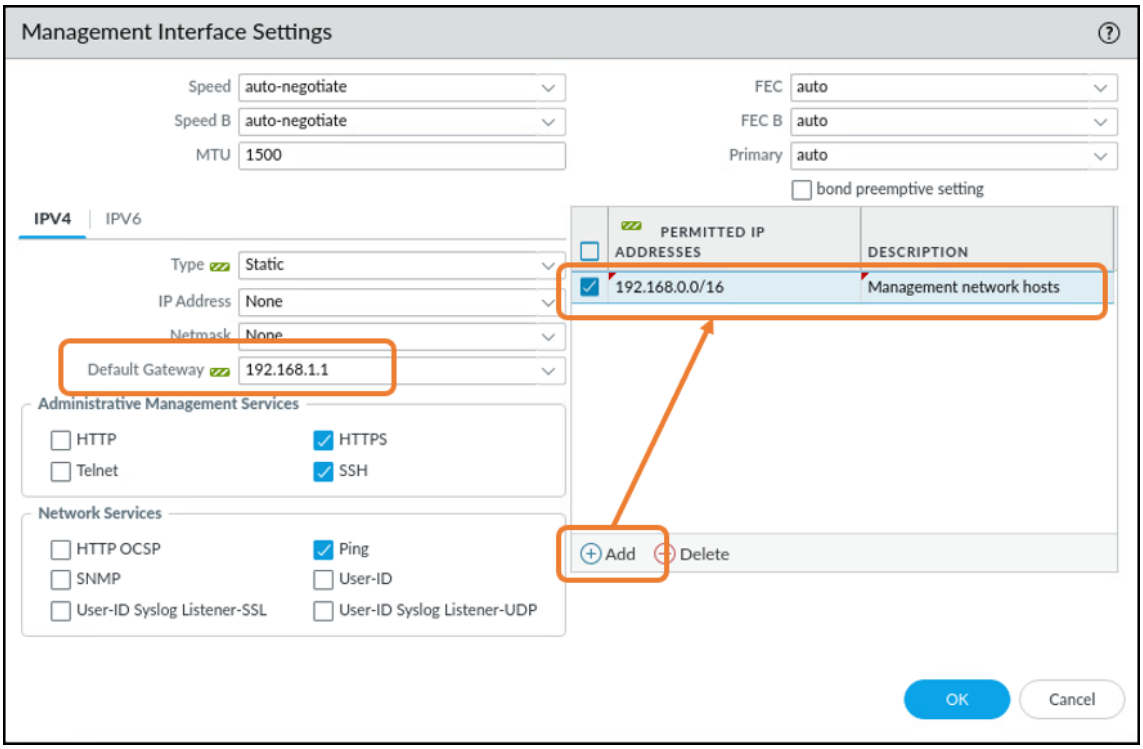


132. Click the link for **Management**.
133. Select the tab for **IPV4**.
134. In the field for **Default Gateway**, enter **`192.168.1.1`**.
135. In the **Permitted IP Addresses** section, click **Add**.
136. Under the **Permitted IP Addresses** field, manually enter **`192.168.0.0/16`**.
137. Under the **Description** field, enter **`Management network hosts`**.
138.

This entry limits management access to your firewalls from hosts on the 192.168.0.0/16 network.

A best practice is to specify the networks from which hosts can manage your firewalls.

139. Leave the remaining settings unchanged:

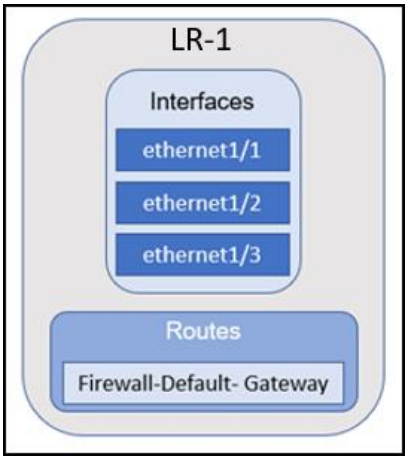


The **Default Gateway** entry will send management traffic from both firewalls through ethernet1/1 of the chicago-fw. This action allows you to provide security services for traffic to and from firewall management interfaces.

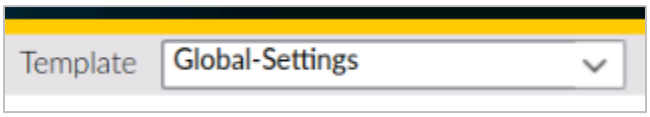
140. Click **OK**.

Create a Logical Router

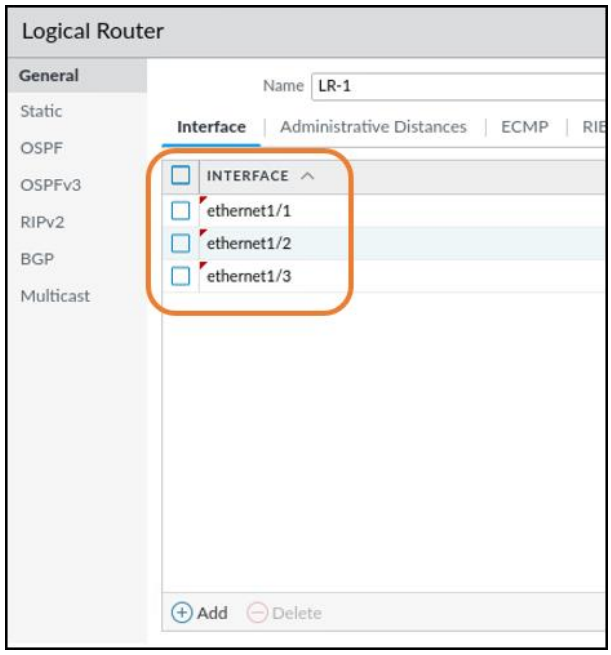
In this section, you will create a logical router in the Global-Settings Template. You will add the Ethernet interfaces that connect the firewall to networks and a default route statement.



141. Select **Network > Routing > Logical Routers**.
142. Click **Add**.
143. Verify that you have selected **Global-Settings** from the **Template** drop-down list:

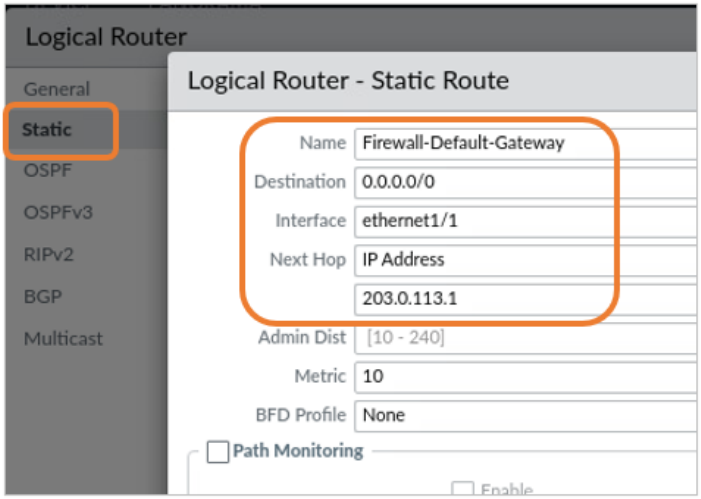


144. Under the **General** section, enter **`LR-1`** for **Name**.
145. Under the **General** section verify that you have selected the **Interface** tab.
146. At the bottom of the **General** section, click **Add**.
147. Select **ethernet1/1**.
148. Click **Add** again.
149. Select **ethernet1/2**.
150. Click **Add** again.
151. Select **ethernet1/3**.
152. When the process is complete, you should have all three interfaces added to the list under the **General** tab:



153. Click the **Static** section on the left side of the **Logical Router** window.
154. Under the **IPv4** tab, click **Add**.
155. For **Name**, enter **`Firewall-Default-Gateway`**.
156. Enter **`0.0.0.0/0`** for **Destination**.
157. For **Interface**, select **ethernet1/1**.
158. For **Next Hop**, select **IP Address**.

159. In the field below **Next Hop**, enter **`203.0.113.1`**.
160. Leave the remaining settings unchanged:



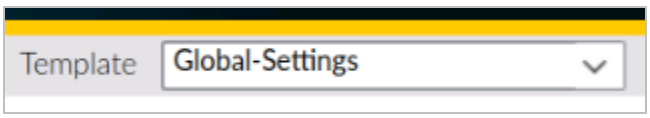
161. Click **OK** on the **Logical Router - Static Route** window.
162. Click **OK** on the **Logical Router** window.

Note that in our lab environment both firewalls share the same default gateway (203.0.113.1). In a production environment, each firewall in your organization likely will have a different upstream router acting as its default gateway. If so, you could define another variable (such as $FW-Default-GW) to supply unique IP addresses for the **Next Hop** address for different firewalls.

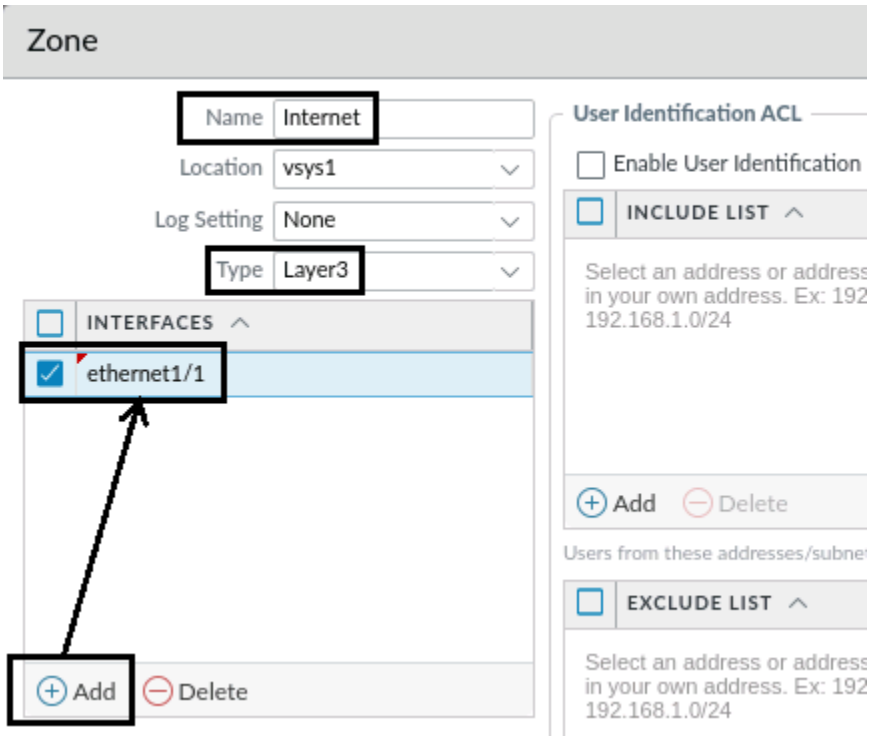
Create Security Zones

With your interfaces defined, you now will create security zones and assign the appropriate interface to them.

163. Select **Network** > **Zones**.
164. Verify that you have selected **Global-Settings** from the **Template** drop-down list:

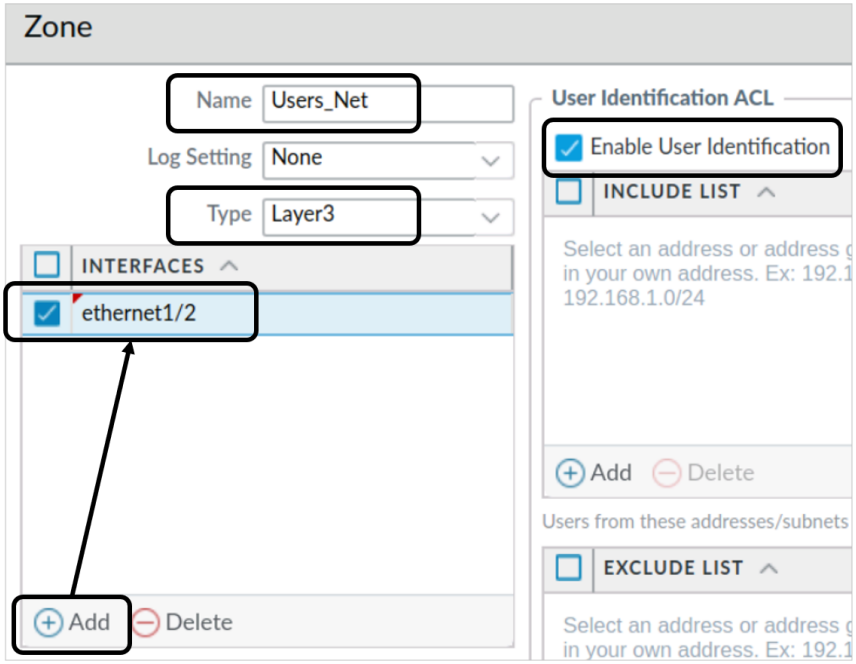


165. Click **Add**.
166. For **Name**, enter **`Internet`**.
167. Change the **Type** to **Layer3**.
168. Under the **Interfaces** section, click **Add**.
169. Select **ethernet1/1**.
170. Leave the remaining settings unchanged:



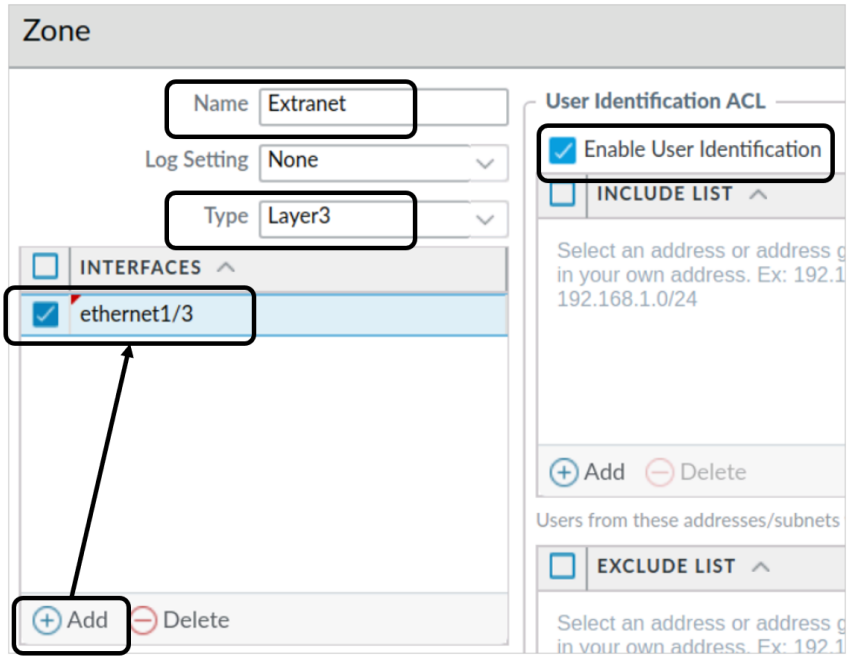
171. Click **OK** to return to the **Zones** window.
172. Click **Add** to create another zone.
173. For **Name**, enter **`Users_Net`**.
174. Set the **Type** to **Layer3**.
175. Under the **Interfaces** section, click **Add**.
176. Select **ethernet1/2**.
177. Check the **box** for **Enable User Identification**.

178. Leave the remaining settings unchanged:



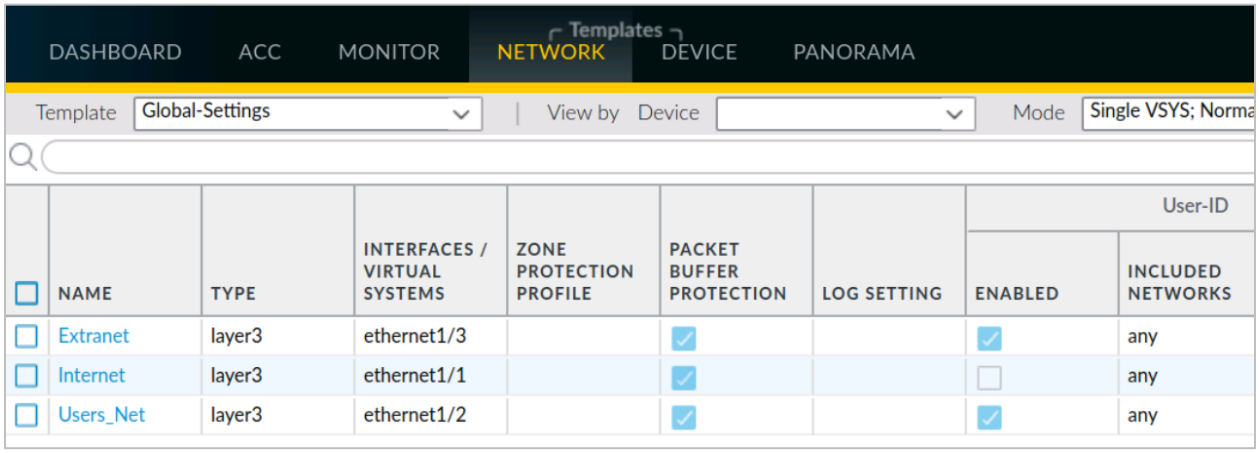
179. Click **OK** to return to the **Zones** window.
180. Click **Add** to create another zone.
181. For **Name**, enter **`Extranet`**.
182. Set the **Type** to **Layer3**.
183. Under the **Interfaces** section, click **Add**.
184. Select **ethernet1/3**.
185. Check the **box** for **Enable User Identification**.

186. Leave the remaining settings unchanged:



187. Click **OK** to return to the **Zones** window.

188. Your **Global-Settings** Template now has three **Security Zones** listed:

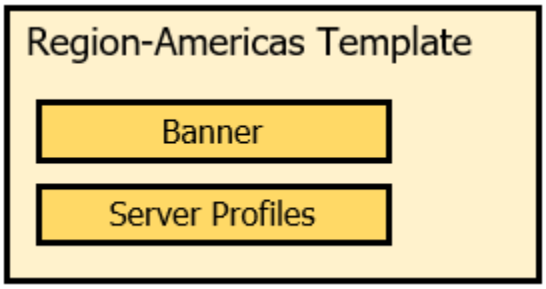


Commit This New Template to Panorama

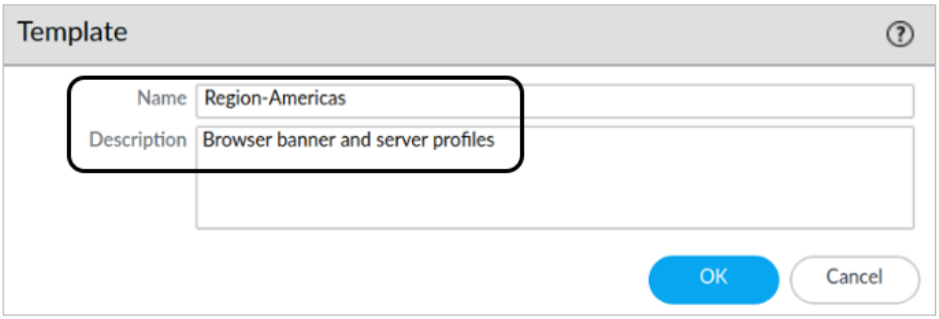
189. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
190. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
191. Monitor the status of the commit.
192. When the commit status is complete, click **Close**.

Create a Template for the Americas Region

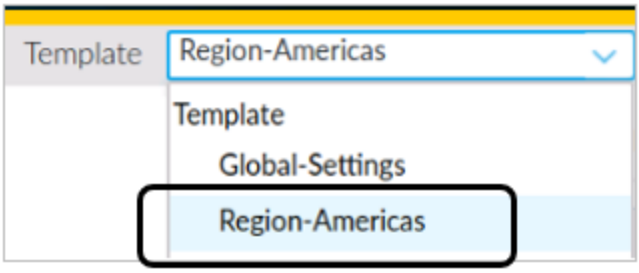
In this section, you will create another Template that contains settings that are specific to the Americas region. This Template will include a firewall banner and server profiles:



193. Select **Panorama** > **Templates**.
194. Click **Add**.
195. For **Name**, enter **`Region-Americas`**.
196. For **Description**, enter **`Browser banner and server profiles`**:



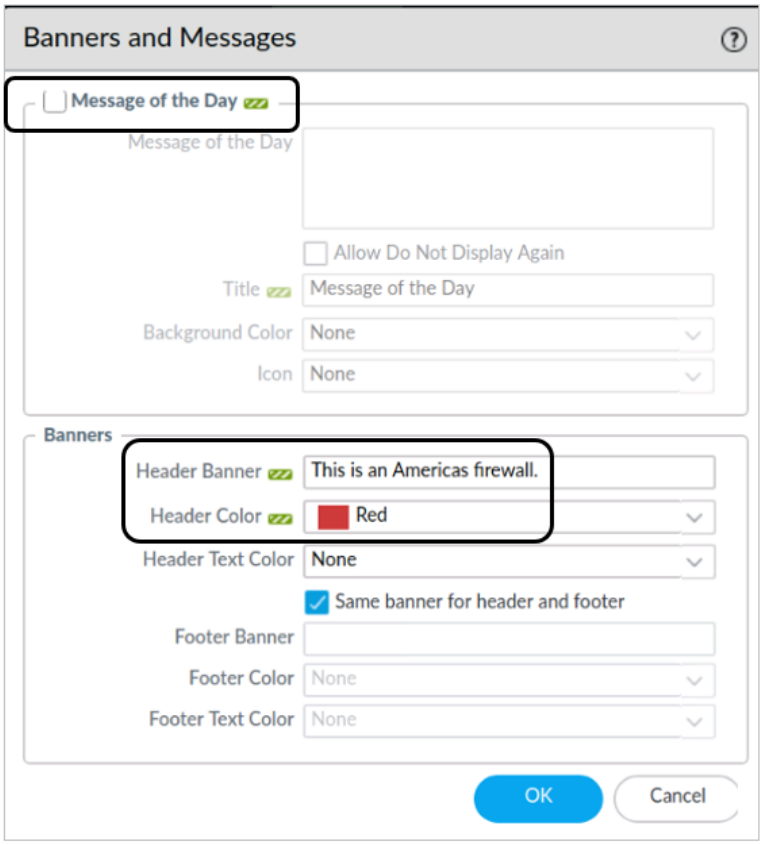
197. Click **OK**.
198. Select **Device** > **Setup** > **Management**.
199. From the drop-down list for **Templates** at the top of the window, select **Region-Americas**:



Now that you have more than one Template defined in Panorama, you must pay careful attention to the **Template** drop-down list. Whenever you edit or add items to a Template, verify that you have selected the correct one before you begin.

200. In the right-hand column of the **Management** settings, locate and edit **Banners and Messages** (this area is in the right-hand column toward the bottom).
201. Enter (or select) the following values:
    - Uncheck the box for Message of the Day.
    - Type the following text in the **Header Banner** field: **`This is an Americas firewall.`**
    - Click the drop-down list next to **Header Color**.
    - Choose **Red** to differentiate your firewall web interface from the Panorama web interface.

- Leave the remaining settings unchanged:

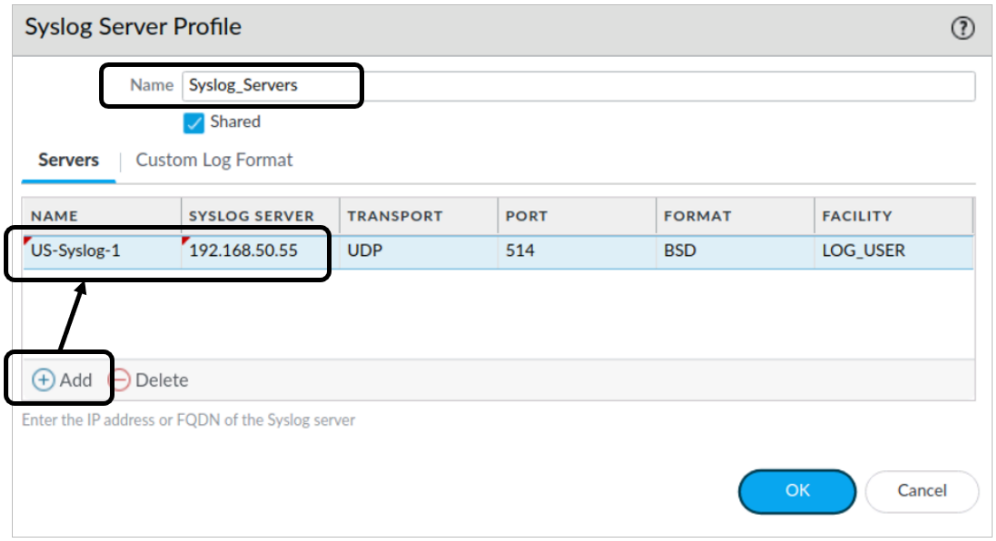


202. Click **OK**.

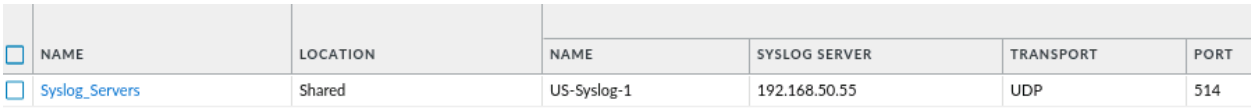
Create a Syslog Server Profile in the Region-Americas Template

203. Select **Device** > **Server Profiles** > **Syslog**.
204. Click **Add**.
205. For **Name**, enter **`Syslog_Servers`** as the value.
206. Leave box checked for **Shared**.
207. At the bottom of the **Servers** tab, click **Add**.
208. For **Name**, enter **`US-Syslog-1`**.
209. For **Syslog Server**, enter **`192.168.50.55`** as the value.

210. Leave the remaining settings unchanged:



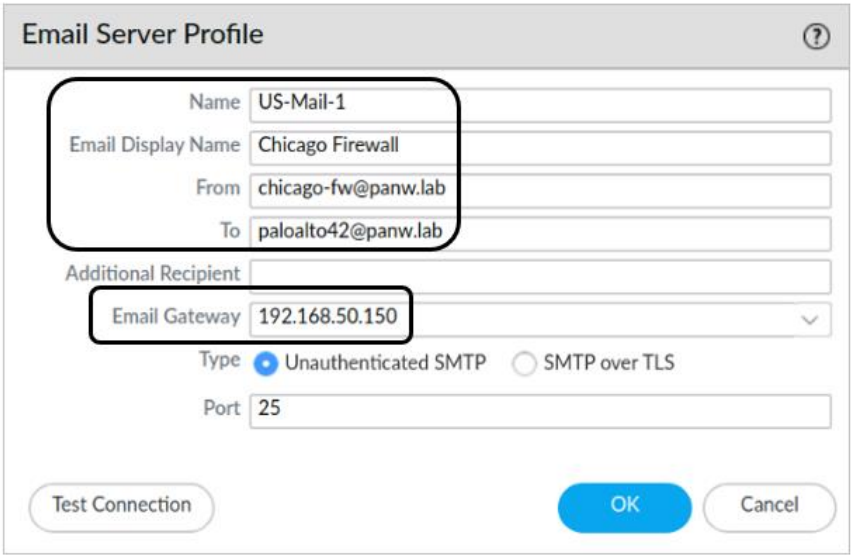
211. Click **OK**.
212. Your **Syslog Server Profile** window will contain the new entry:



Create an Email Server Profile in the Region-Americas Template

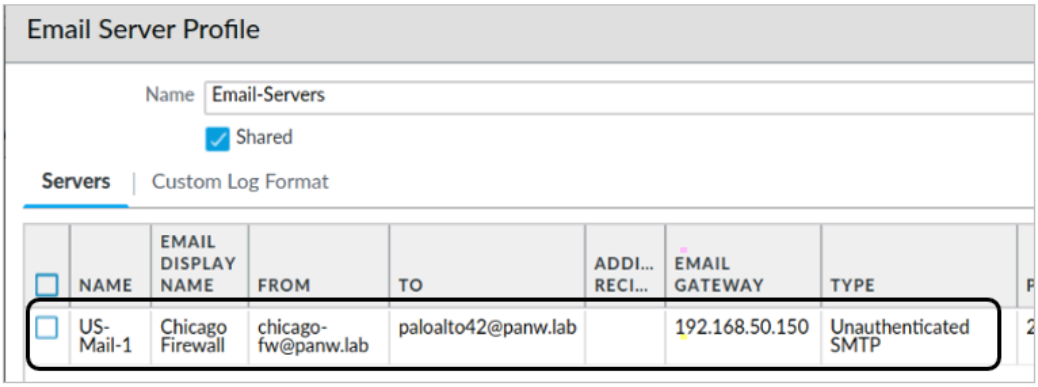
213. Select **Device** > **Server Profiles** > **Email**.
214. Click **Add**.
215. For **Name**, enter **`Email-Servers`**.
216. At the bottom of the **Server** tab, click **Add**:
    - For **Name**, enter **`US-Mail-1`**.
    - For **Email Display Name**, enter **`Chicago Firewall`** as the value.
    - For **From**, enter **`chicago-fw@panw.lab`** as the value.
    - For **To**, enter **`paloalto42@panw.lab`** as the value.
    - Leave the **Additional Recipient** field blank.

- For **Email Gateway**, enter **192.168.50.150**.



Do not click the **Test Connection** button. The **Test Connection** button will return an error now because the appropriate firewall configurations are not yet in place.

217. Click **OK**.
218. Your **Email Server Profile** window will contain the new entry:



219. Click **OK**.
220. Your **Email Servers** list will contain the new entry:

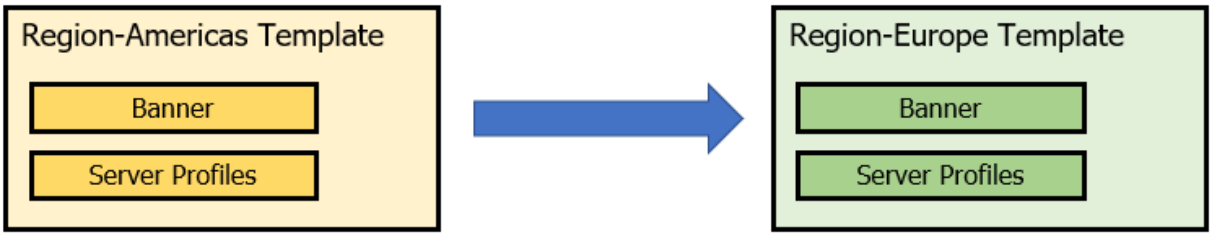
NAME	LOCAT...	Servers						
		NAME	EMAIL DISPLAY NAME	FROM	TO	A... R...	EMAIL GATEWAY	PROTOCOL
Email-Servers	Shared	US-Mail-1	Chicago Firewall	chicago-fw@panw.lab	paloalto42@panw.lab		192.168.50.150	Unauthenticated SMTP

Commit the Changes to Panorama

221. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
222. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
223. Monitor the status of the commit.
224. When the commit status is complete, click **Close**.

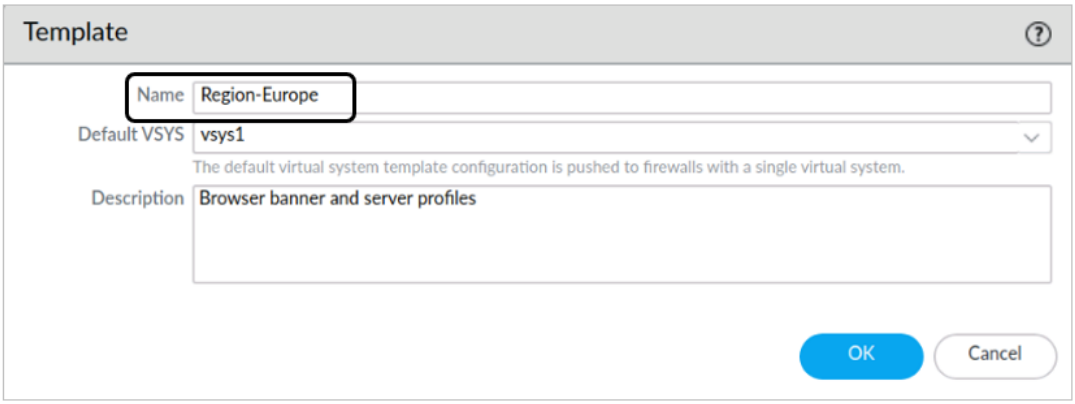
Clone Region-Americas Template to Create Region-Europe Template

In this section, you will clone the Region-Americas Template to serve as the basis for a new Template called Region-Europe:



After you have created the clone, you will edit the new Template and make the appropriate changes to match settings for firewalls in the Region-Europe.

225. Select **Panorama** > **Templates**.
226. Check the **box** for the **Region-Americas** Template.
227. Click the **Clone** button at the bottom of the window.
228. Panorama will create a new entry called **Region-Americas-1**.
229. Click the **Region-Americas-1** Template to edit it.
230. Change the **name** to **`Region-Europe`**.
231. Leave the remaining settings unchanged:



232. Click **OK**.

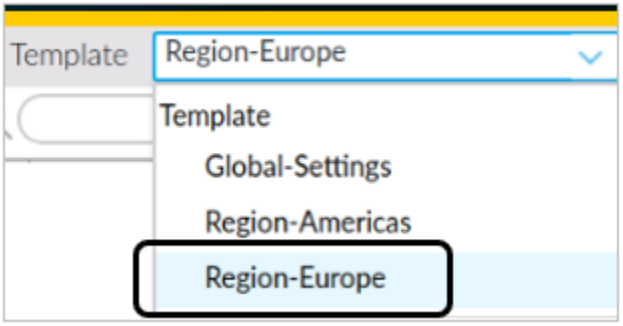
233. When the configuration is complete, you should have a new **Template** entry called **Region-Europe**:

NAME	DESCRIPTION	TYPE
Global-Settings	Network - Interfaces, Zones, Logical Router Device – Login Banner, Domain, Panorama Servers, Log Settings	template
Region-Americas	Browser banner and server profiles	template
Region-Europe	Browser banner and server profiles	template

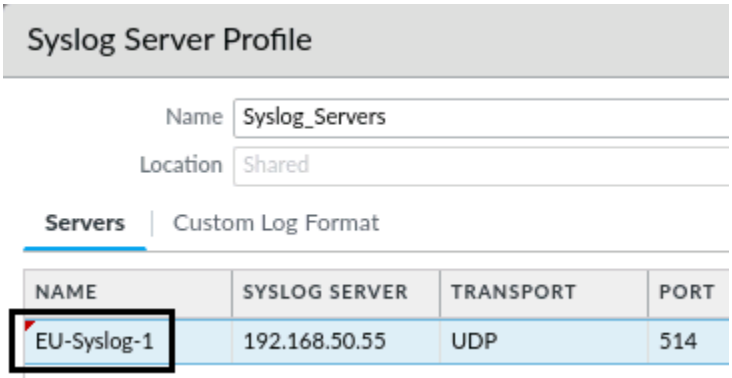
Edit Settings in the Region-Europe Template

The Europe Region firewalls use different servers from the Americas firewalls. In this section, you will edit each Server Profile and make the appropriate changes. You also need to change the browser banner.

234. Change the **Syslog Server Profile** by selecting **Device > Server Profiles > Syslog**.
235. Verify that **Region-Europe** is selected from the **Template** drop-down list:

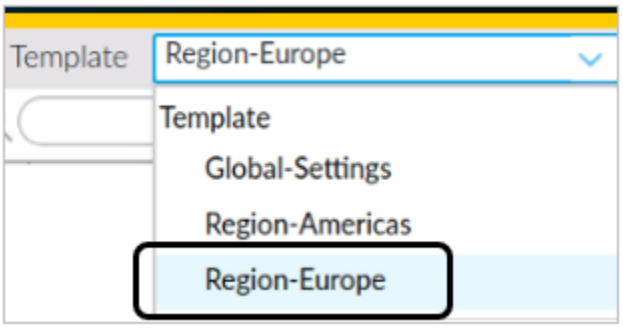


236. Edit the entry for **Syslog_Servers**.
237. Change the **Name** field to **`EU-Syslog-1`**.
238. Leave the remaining settings unchanged:

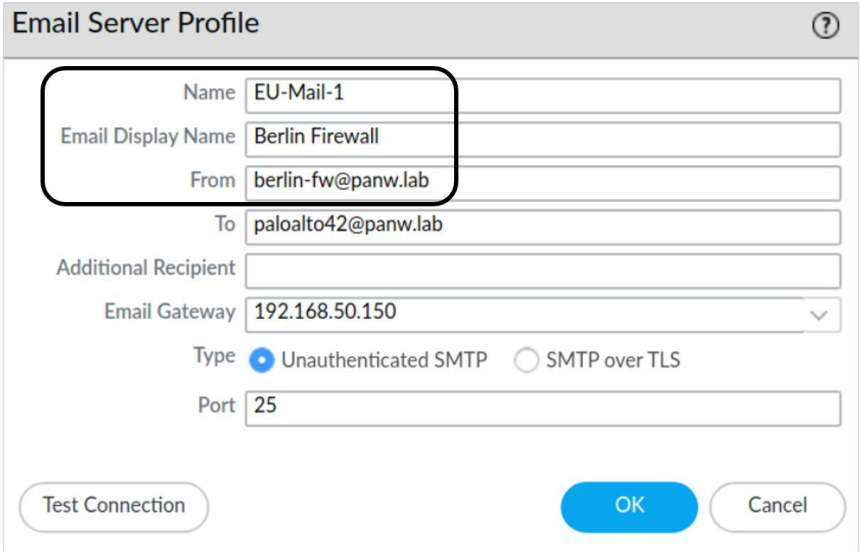


Note that in our lab environment EU-Syslog-1 and US-Syslog-1 use the same IP address, which is why you are not changing that Syslog Server value. In a production environment, if you do have different hosts in different regions performing server tasks such as syslog, you also would change the IP address (or hostname).

239. Click **OK**.
240. Change the Email Server Profile by selecting **Device > Server Profiles > Email**.
241. Verify that the **Region-Europe** Template is selected from the drop-down list:



242. Click the entry for **Email-Servers** to edit it.
243. Under the **Servers** tab, click the entry for **US-Mail-1** to edit it.
244. Change the **Name** value to **`EU-Mail-1`**.
245. Change the **Email Display Name** to **`Berlin Firewall`**.
246. Change the **From** value to **`berlin-fw@panw.lab`**.
247. Leave the remaining settings unchanged.



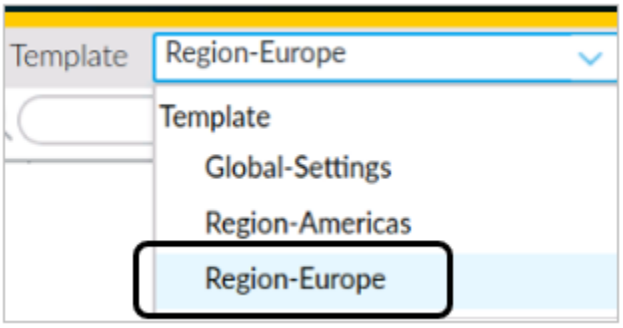
248. Click **OK** to close the first Email Server Profile window.

249. Click **OK** to close the second Email Server Profile window.

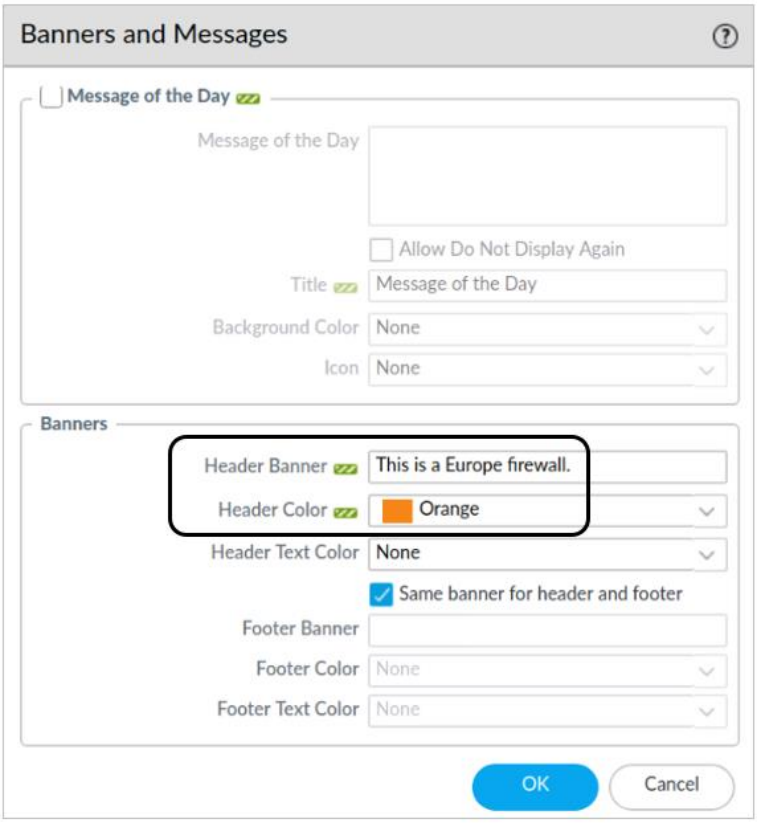
Change the Header Banner

In this section, you will modify the banner for Region-Europe firewalls so you can easily distinguish them from firewalls in the Region-Americas.

250. Select **Device > Setup** and select the **Management** tab.
251. Verify that the **Region-Europe** Template is selected from the drop-down list:



252. Edit the **Banners and Messages** section.
253. Change the **Header Banner** text to **`This is a Europe firewall`**.
254. Change the **Header Color** to **`Orange`**.
255. Leave the remaining settings unchanged:



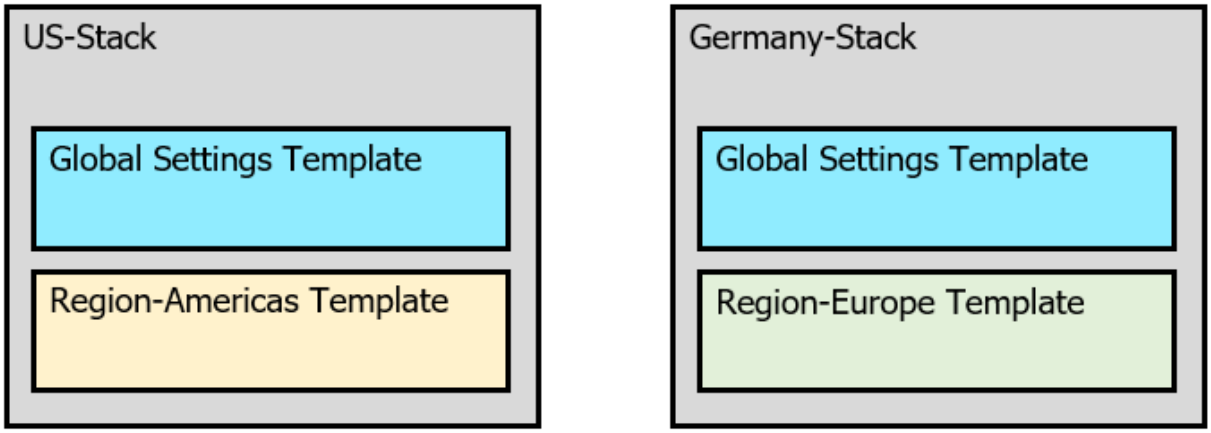
256. Click **OK**.

Commit the Changes to Panorama

257. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
258. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
259. Monitor the status of the commit.
260. When the commit status is complete, click **Close.**

Create Template Stacks

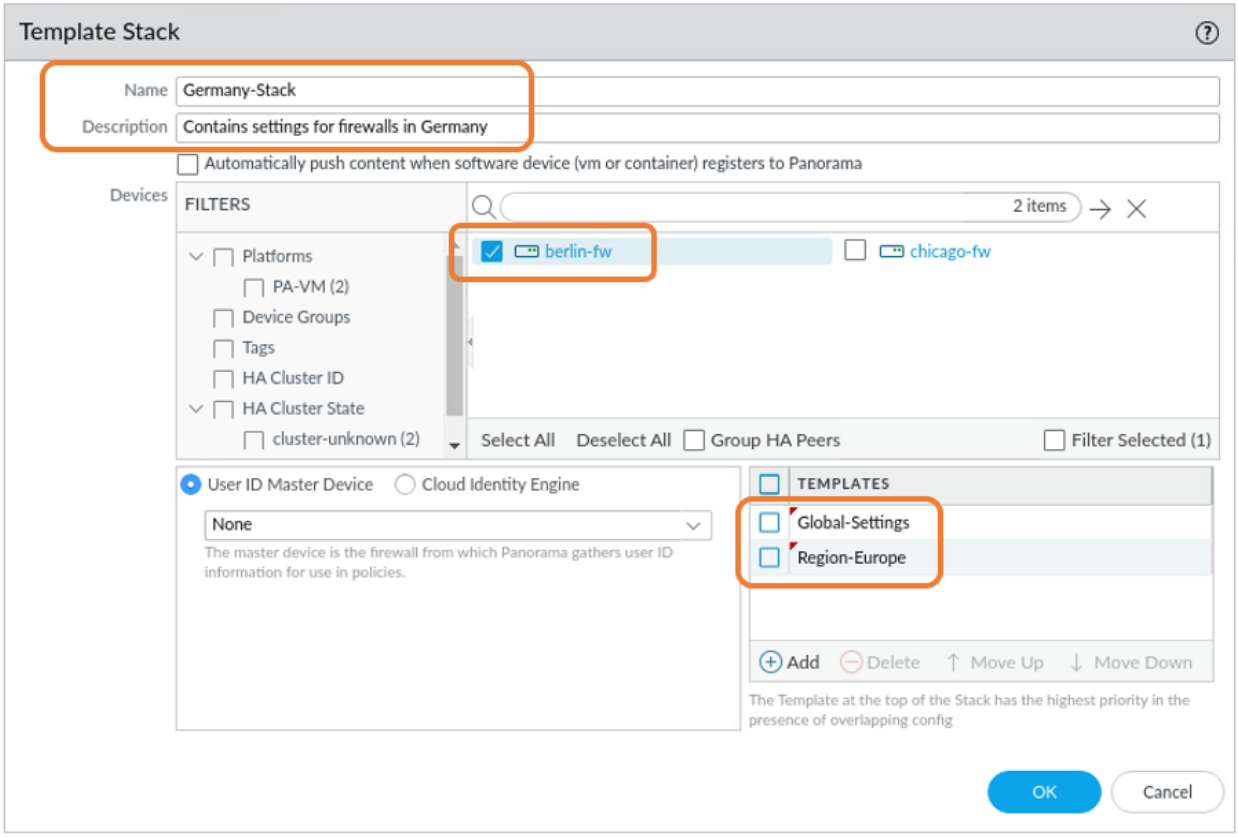
In this section, you will create two Template stacks. One stack will be for firewalls in Germany and the other stack will be for the United States. You will use the Templates you created as the building blocks for both Template stacks:



Both stacks will contain the Global-Settings Template, but each stack will contain the appropriate Region Template.

Create a Template Stack for Germany Firewalls

261. Select **Panorama** > **Templates**.
262. At the bottom of the window, click **Add Stack**.
263. For **Name**, enter **`Germany-Stack`**.
264. For **Description**, enter **`Contains settings for firewalls in Germany`**.
265. Under the **Templates** section, click the **Add** button.
266. Select **Global-Settings**.
267. Click **Add** again, under the **Templates** section.
268. Select **Region-Europe**.
269. Place a **check mark** in the **box** beside **berlin-fw**.
270. Leave the remaining settings unchanged:



271. Click **OK**.
272. Panorama updates the list of entries under **Templates** to include the new Template Stack:

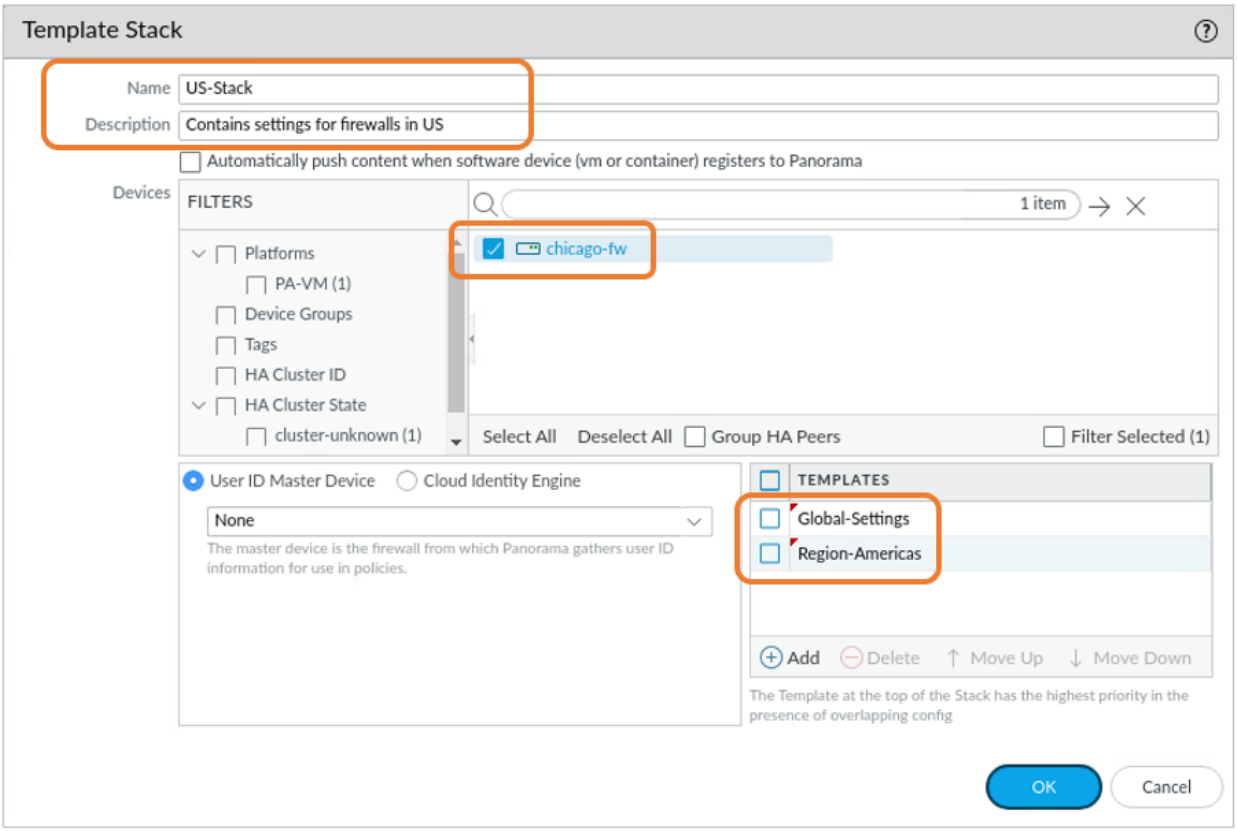
NAME	DESCRIPTION	TYPE	STACK	DEVICES
Global-Settings	Network - Interfaces, Zones, Virtual Router Device - Login Banner, Domain, Panorama Settings, Log Settings	template		
Region-Americas	Browser banner and server profiles	template		
Region-Europe	Browser banner and server profiles	template		
Germany-Stack	Contains settings for firewalls in Germany.	template-stack	Global-Settings Region-Europe	berlin-fw

For Template stack entries, the Stack column shows you the individual Templates that are used in the stack. The order of entries is important for inheritance of settings that occur in multiple Templates.

The **Devices** column shows you which firewalls have been assigned to this Template stack.

Create a Template Stack for US Firewalls

273. Select **Panorama** > **Templates**.
274. At the bottom of the window, click **Add Stack**.
275. For **Name**, enter **`US-Stack`**.
276. For **Description**, enter **`Contains settings for firewalls in US`**.
277. Under the **Templates** section, click the **Add** button.
278. Select **Global-Settings**.
279. Click **Add** again, under the **Templates** section.
280. Select **Region-Americas**.
281. Place a **check mark** in the **box** beside **chicago-fw**.
282. Leave the remaining settings unchanged:



283. Click **OK**.
284. Panorama updates the list of entries under **Templates** to include the new Template stack:

NAME	DESCRIPTION	TYPE	STACK	DEVICES
Global-Settings	Network - Interfaces, Zones, Virtual Router Device - Login Banner, Domain, Panorama Settings, Log Settings	template		
Region-Americas	Browser banner and server profiles	template		
Region-Europe	Browser banner and server profiles	template		
Germany-Stack	Contains settings for firewalls in Germany.	template-stack	Global-Settings Region-Europe	berlin-fw
US-Stack	Contains settings for firewalls in US.	template-stack	Global-Settings Region-Americas	chicago-fw

Commit the Changes to Panorama

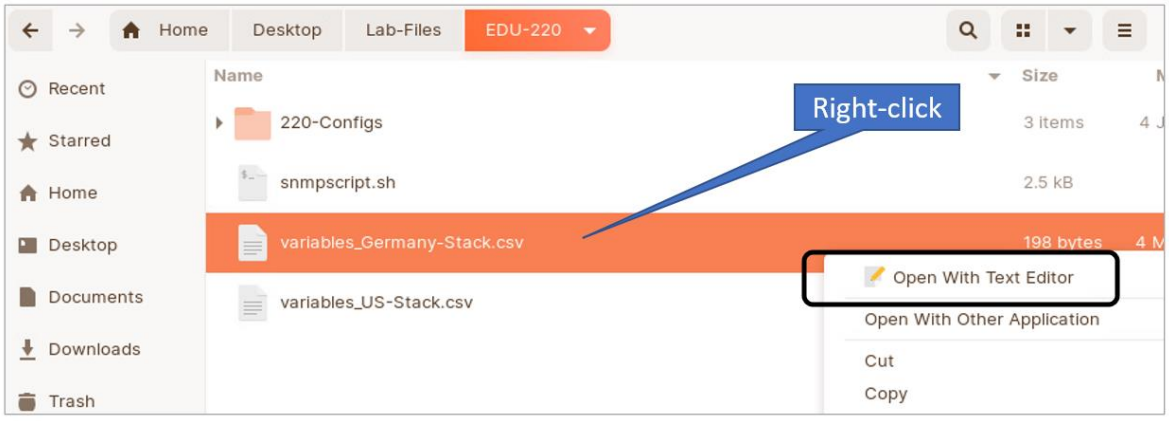
285. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
286. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
287. Monitor the status of the commit.
288. When the commit status is complete, click **Close**.

Modify Variables for Firewalls

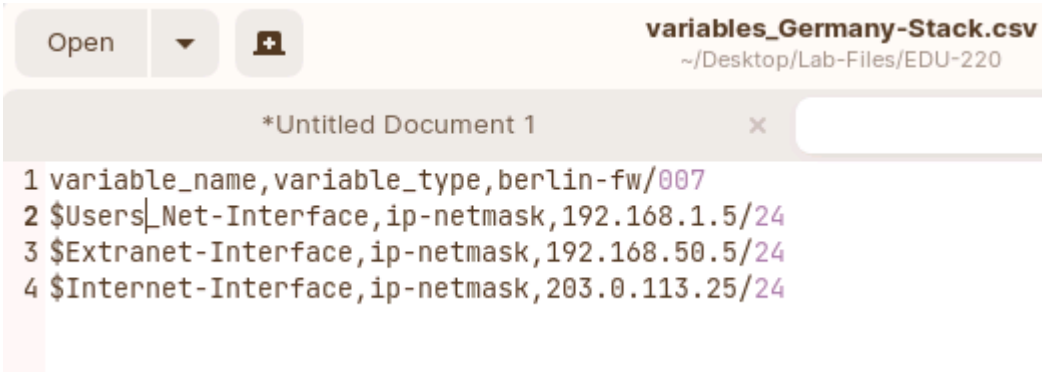
You defined variables for each firewall interface as part of the Global-Settings Template. In this section, you import a CSV file for each Template Stack that will replace each variable with a specific value for each firewall in each stack.

These CSV files have been predefined for you and are stored on the client-A host.

289. On the client-A Desktop, open the **`Lab-Files/EDU-220`** folder.
290. Locate the file called **`variables_Germany-Stack.csv`**.
291. Right-click on the file and choose **`Open With "Text Editor"`**:

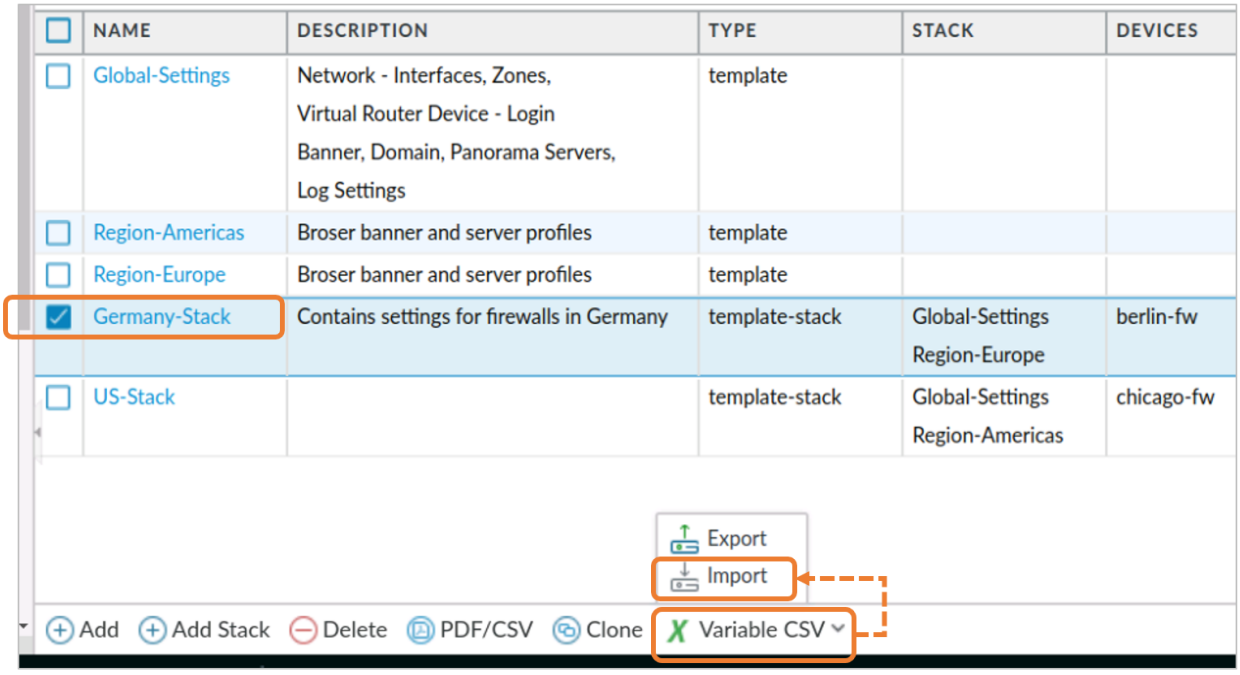


292. The file will open in a text editor, and you can see how the file is structured:



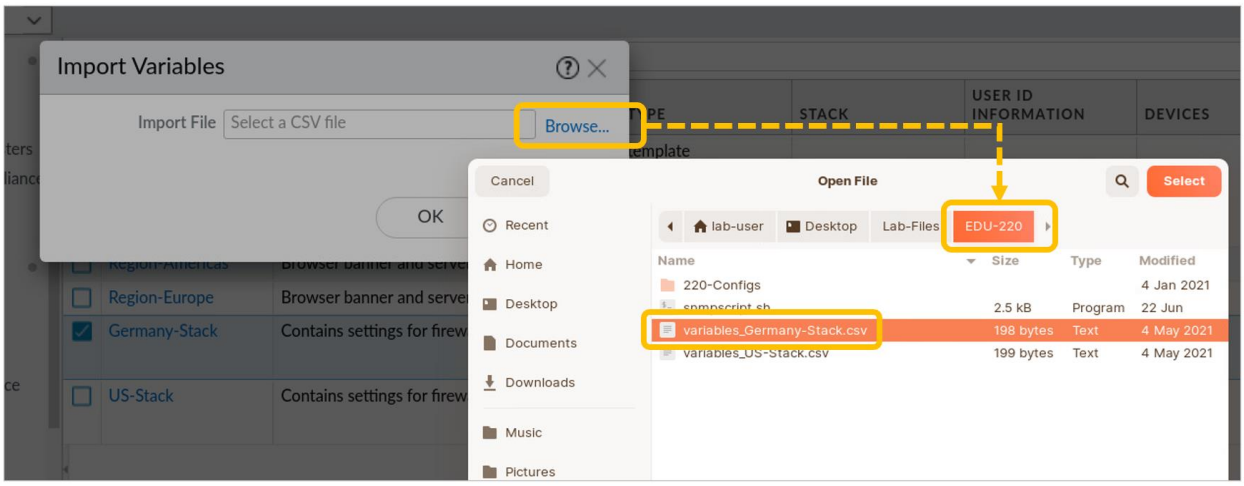
Note that the first row defines the structure of each entry, as well as which firewall the variables apply to. In this example, there is only a single firewall (berlin-fw) in the Template stack. For a Template stack with numerous entries, these four lines would be repeated along with a unique firewall name and individual values for each listed variable. Make certain that there are no blank lines at the end of the file.

293. Close the text editor and close any open folder windows you have on the client desktop.
294. Select **Panorama** > **Templates**.
295. Place a **check** in the box beside **Germany-Stack**.
296. From the **Variable CSV** selection at the bottom of the window, choose **Import**.



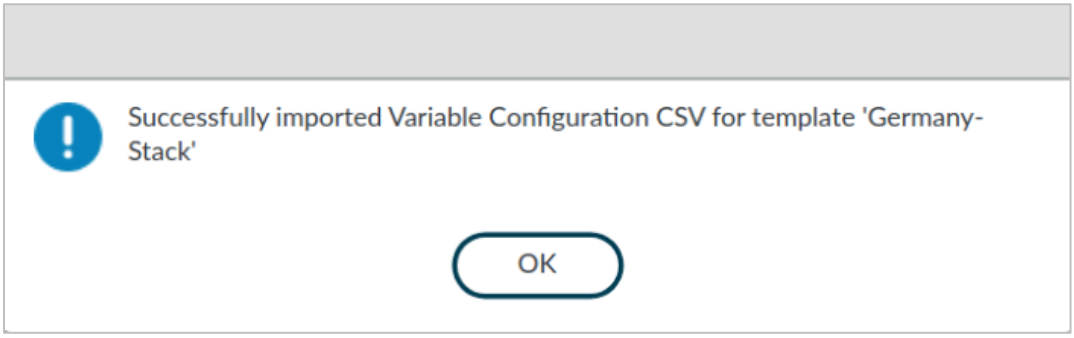
297. In the **Import Variables** window that appears, click the **Browse** button.

298. Navigate to the **Desktop** > **Lab Files** > **EDU-220** folder.
299. Double click on the file called **`variables_Germany-Stack.csv`**.

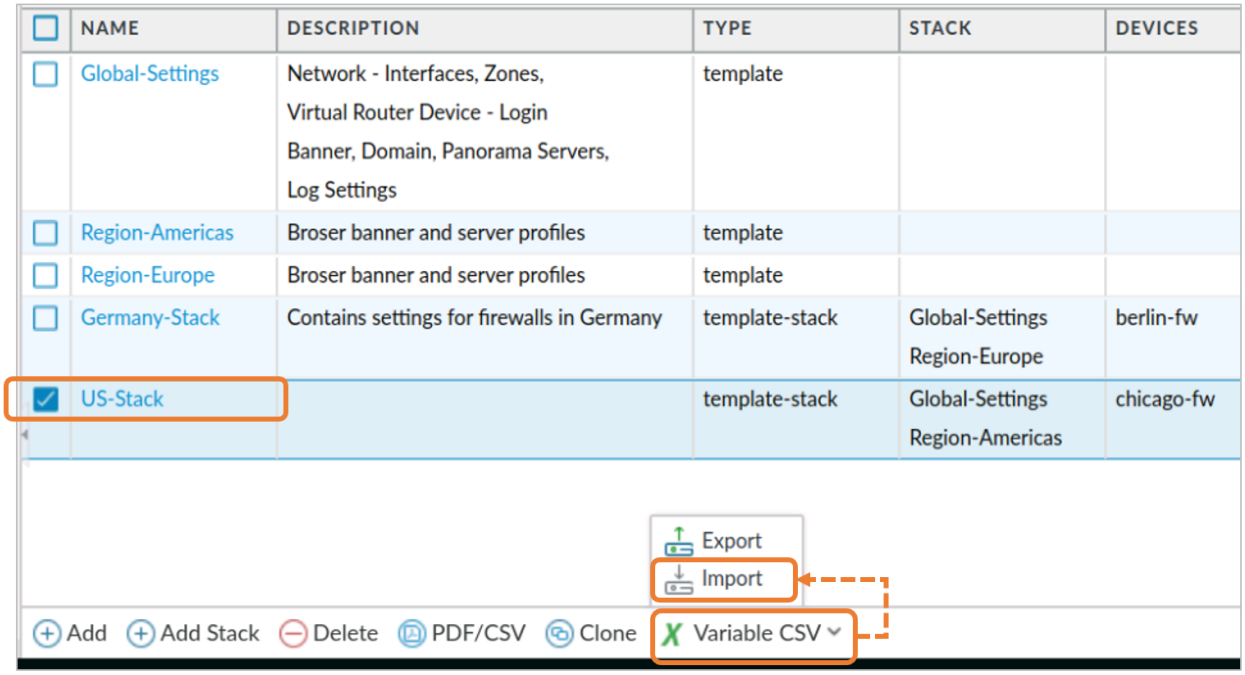


300. The **Import Variables** window will display the file to import.

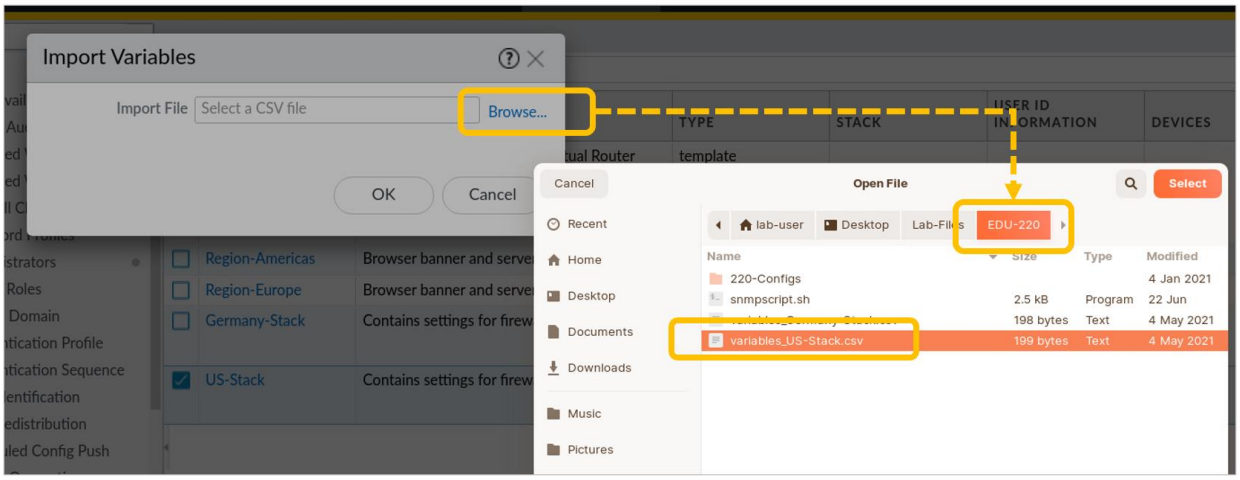
301. Click **OK**.
302. Panorama will indicate that it has successfully imported the file.



303. Click **OK**.
304. **Uncheck** the box next to the Germany-Stack and place a **check** mark in the box for **US-Stack**.
305. From the **Variable CSV** selection at the bottom of the window, choose **Import**.

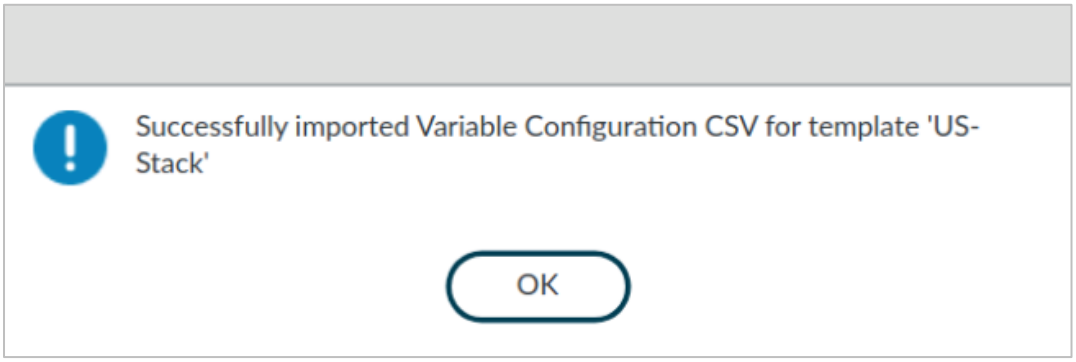


306. In the **Import Variables** window that appears, click the **Browse** button.
307. Navigate to the **Desktop > Lab Files > EDU-220** folder.
308. Double click on the file called **`variables_US-Stack.csv`**.



309. The **Import Variables** window will display the file to import.

310. Click **OK**.
311. Panorama will indicate that it has successfully imported the file.

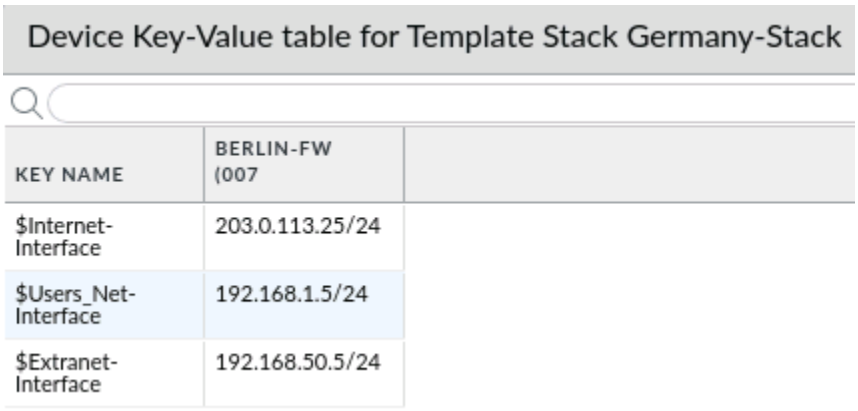


312. Click **OK**.

Verify the Variables for Each Template Stack

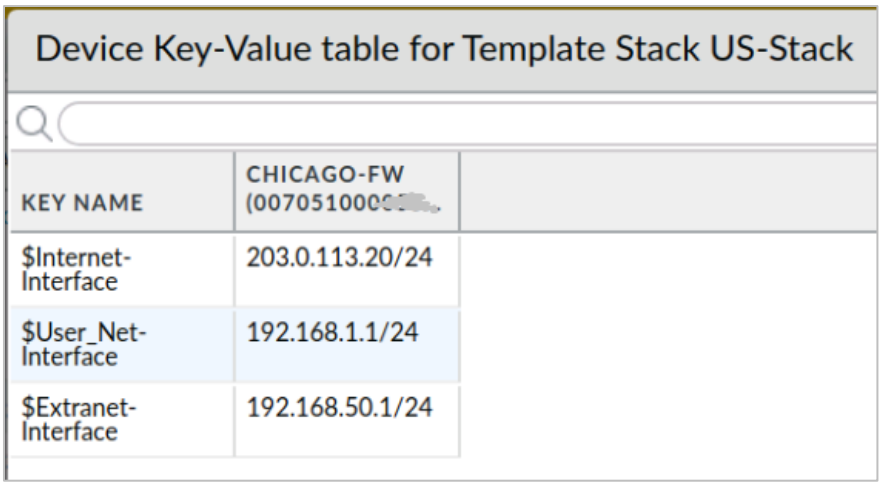
After importing the variables from the CSV file to each Template Stack, you can view the values that will be assigned to those variables for each firewall.

313. In the **Panorama > Template** section, locate the column for **Device Key-Value Table**.
314. In that column, click the link for **View** in the row for **Germany-Stack**.
315. Panorama displays a window with a column for each firewall (in our environment, we have only a single firewall in this Template Stack):



Each row includes the variable you created and the value that will be pushed down to the firewall from Panorama for that variable.

316. Click **Close** to close this window.
317. In the **Panorama** > **Template** section, locate the column for **Device Key-Value Table**.
318. In that column, click the link for **`View`** in the row for **US-Stack**.
319. Panorama displays a window with a column for each firewall (in our environment, we have only a single firewall in this Template Stack):



Each row includes the variable you created and the value that will be pushed down to the firewall from Panorama for that variable.

320. Click **Close** to close this window.

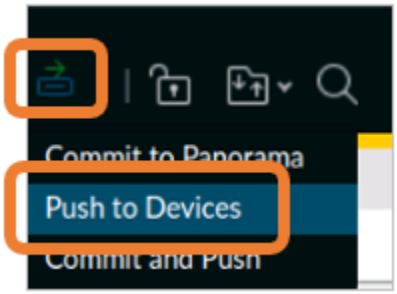
Commit the Changes to Panorama

321. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
322. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
323. Monitor the status of the commit.
324. When the commit status is complete, click **Close.**

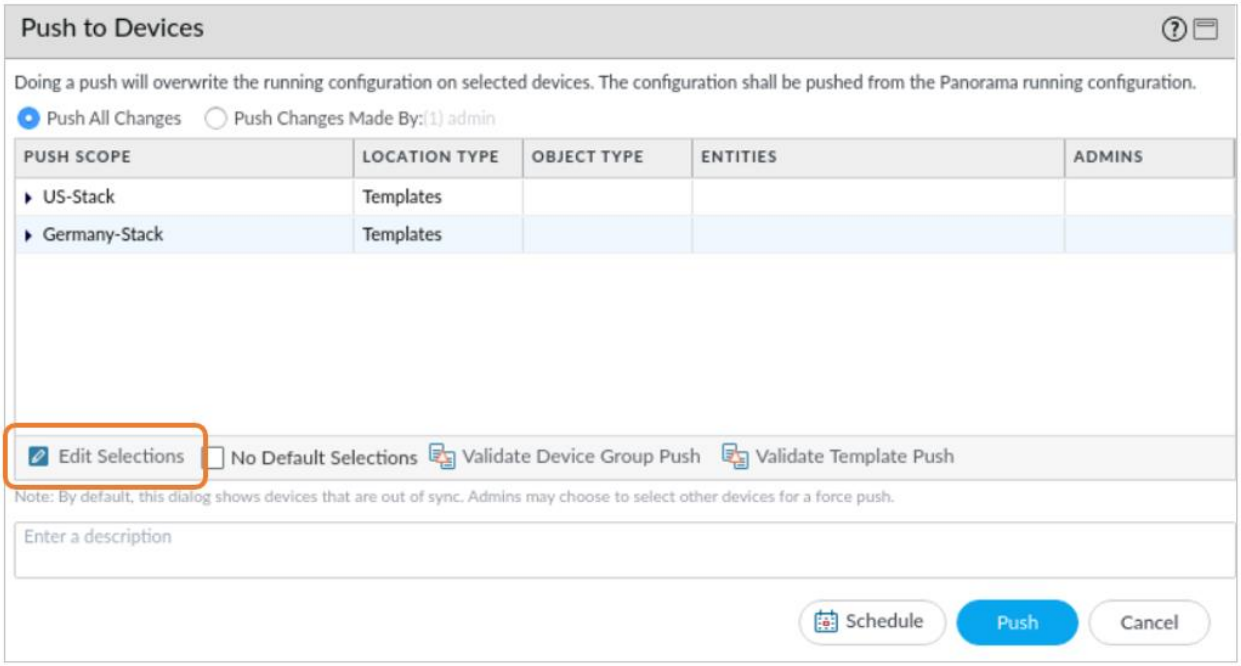
Push the Template Stacks to Firewalls

You now will push the settings you have defined within your Template stacks down to the firewalls.

325. In the upper-right corner of Panorama, select **Commit > Push to Devices**:



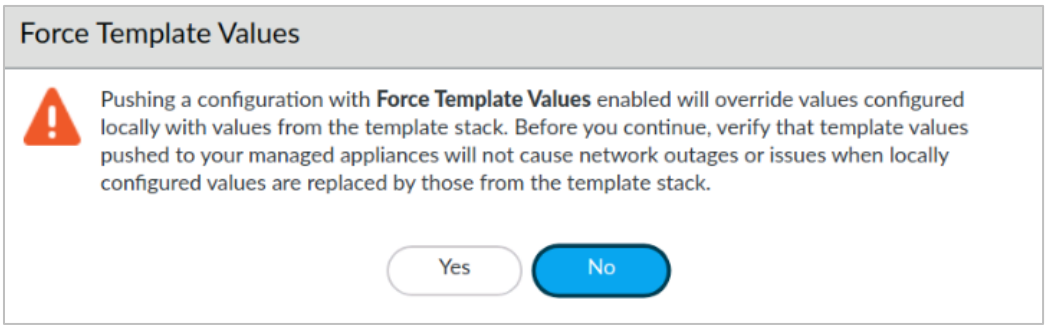
326. In the **Push to Devices** window, click the button for **Edit Selections**:



327. In the **Push Scope Selection** window that appears, select the tab for **Templates**.

328. Place a **check mark** in the **box** for **Force Template Values** at the bottom of the window:

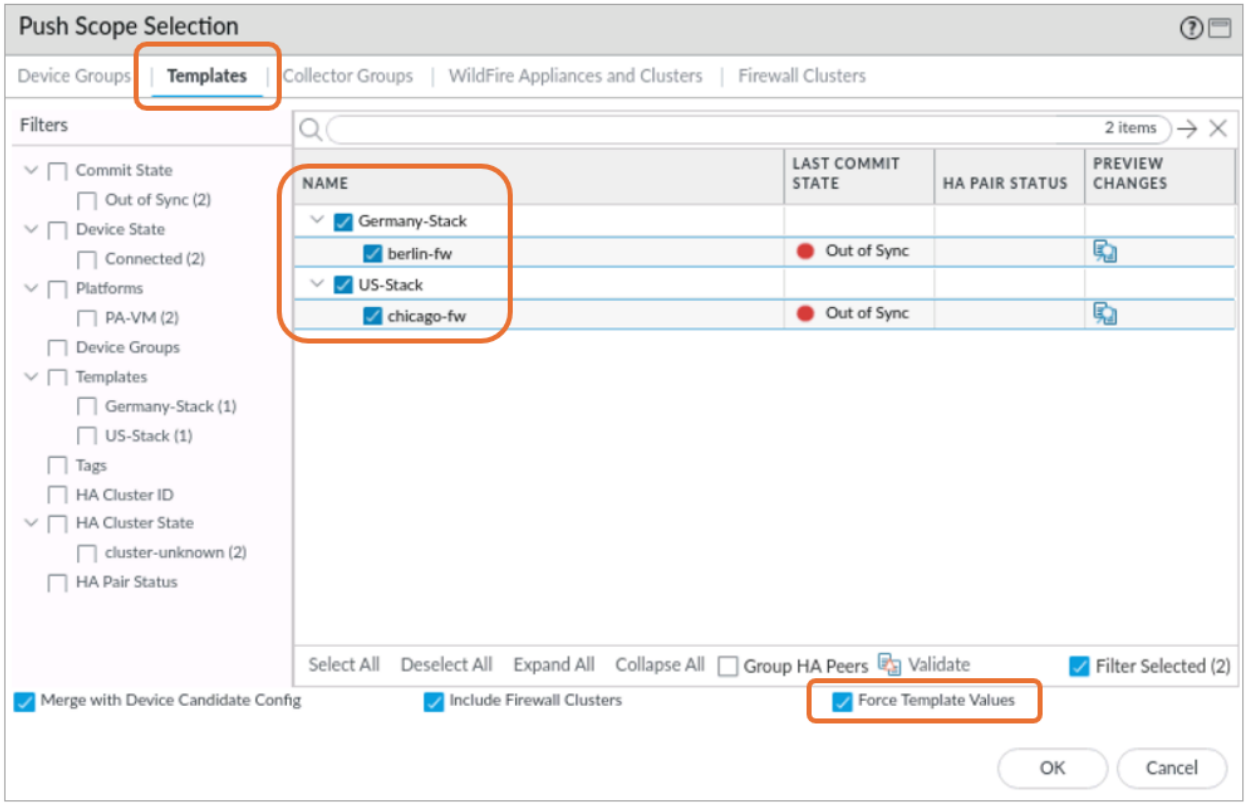
329. Click **Yes** on the **Force Template Values** box to return to the Push Scope Selection window:



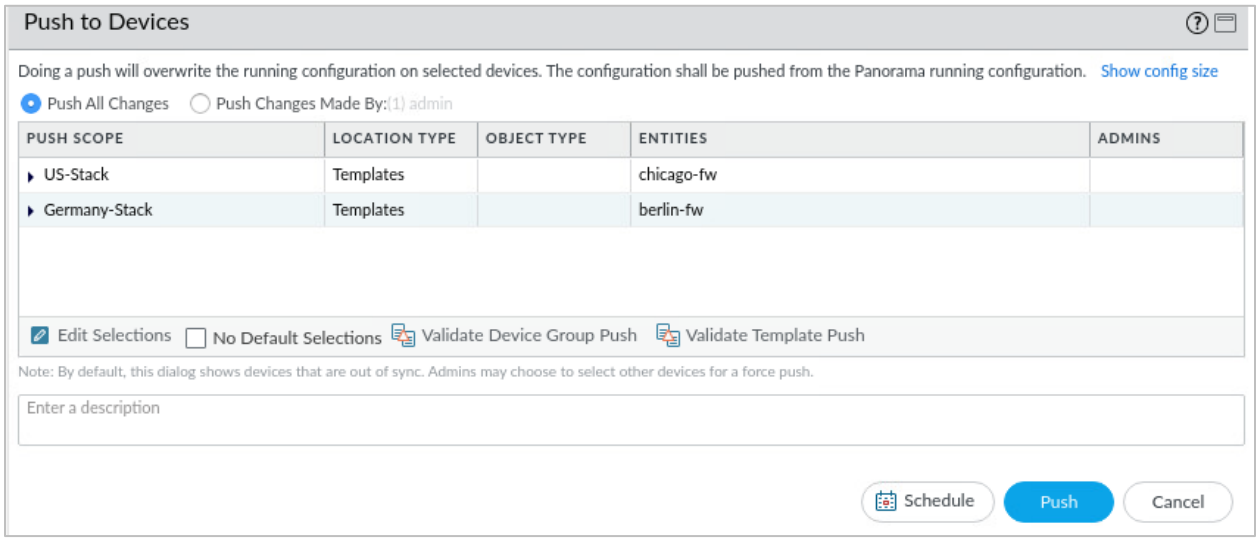
Force Template Values instructs Panorama to replace any settings that have been applied on a firewall locally with the values from the Templates. In our case, we have not modified any settings for network or Devices directly on the firewalls, so there will be no effect.

The warning is a reminder that when you force Template values from Panorama to one or more firewalls, the process overwrites any of the network and Device settings in place on the target firewalls. We will consistently enable the **Force Template Values** throughout these labs, but in a production environment, you should verify that you do not overwrite network or Device settings on firewalls unless you intend to do so.

330. In the **Push Scope Selection** window, under the **Templates** tab, note that both Devices are selected under their respective Templates:

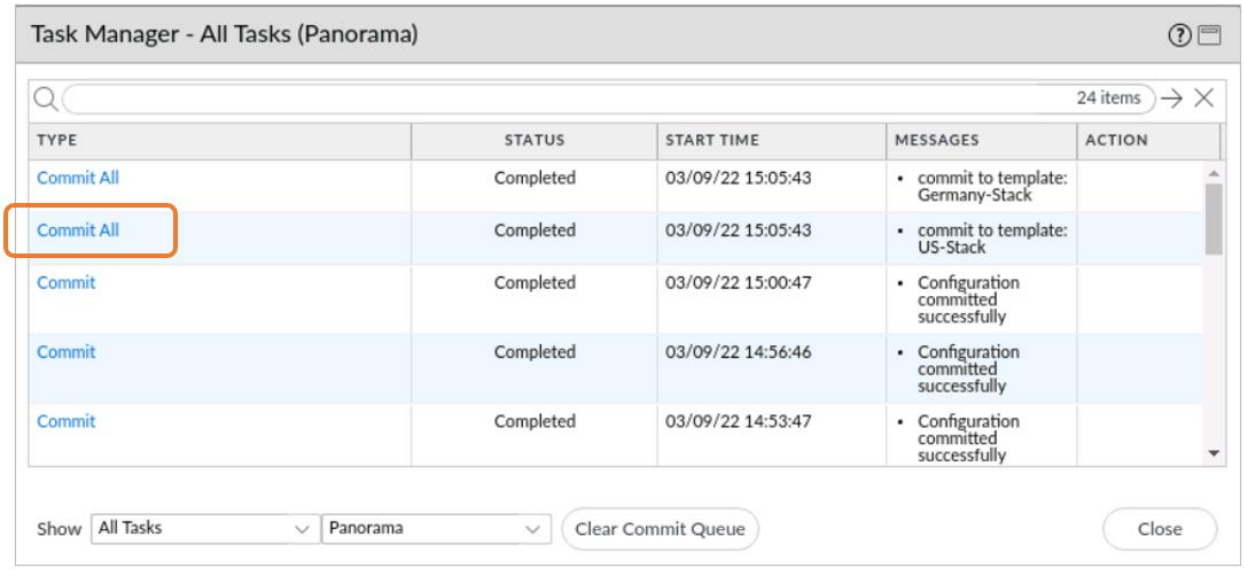


331. Click **OK** to close the **Push Scope Selection** window and return to the **Push to Devices** window:

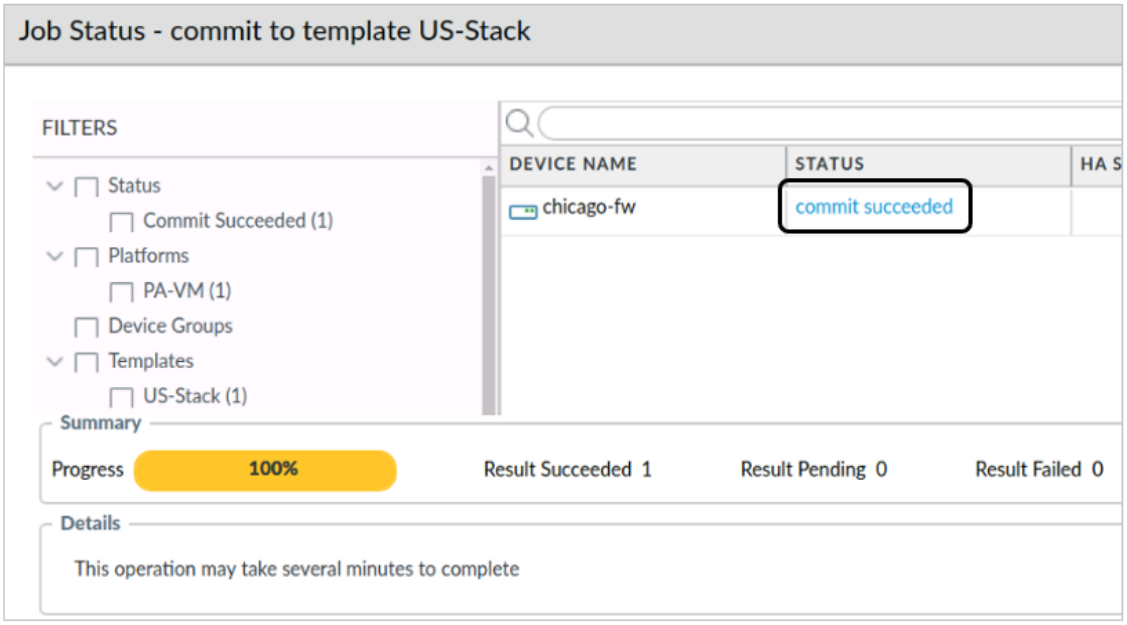


In the **Push to Devices** window, the **Push Scope** and **Location Type** provide information about the kinds of changes that will be pushed. The **Entities** column shows the affected firewalls.

332. Click **Push** in the **Push to Devices** window to send these changes to the firewalls.
333. The **Task Manager** window provides information about the status of the configuration push.
334. Wait until the **Status** for the first entry changes to **Completed**.
335. Then, click the link for **Commit All**:

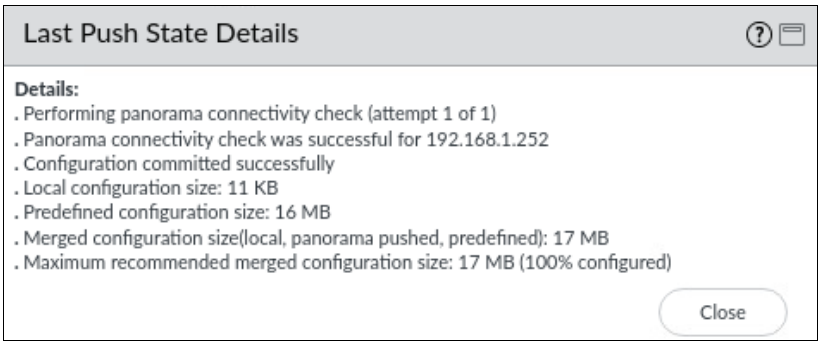


336. Click the link in the **Status** column:



The status may not change to **commit succeeded** immediately. If not, close the **Job Status – commit…** window and wait a few moments before trying again.

337. Panorama provides you with details about the commit process:



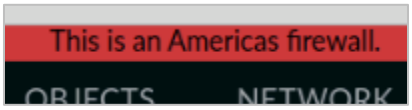
Ignore any warning messages you see about the API KeyGen algorithm or configuration size.

338. Click **Close** on the **Last Push State Details** window.
339. Click **Close** in the **Job Status – commit…** window.
340. Close the **Task Manager** window.

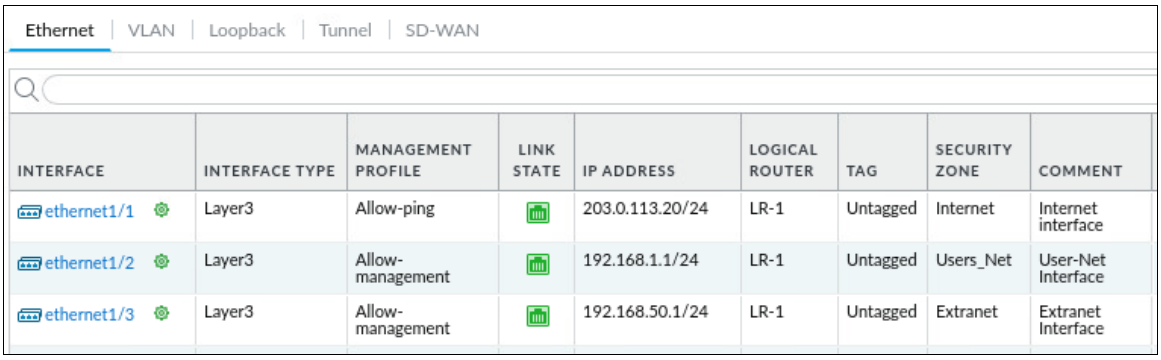
Verify Template Settings on the Chicago Firewall

In this section, you will examine the Chicago firewall to verify that Panorama has successfully pushed down the appropriate settings under network and Device.

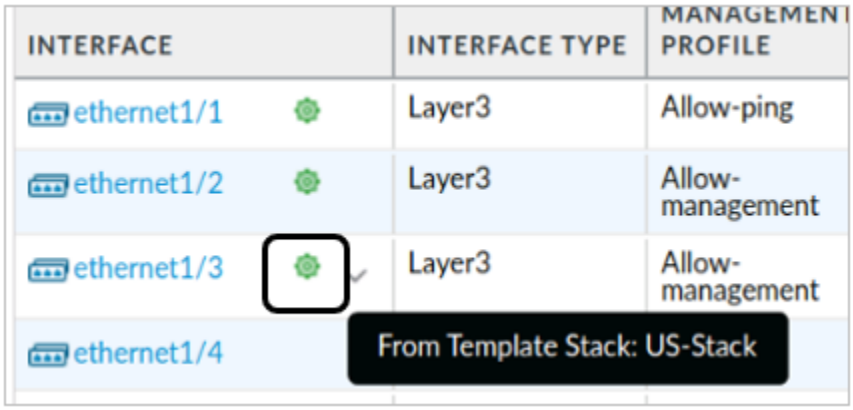
341. Select the browser tab for the Chicago firewall.
342. Log out of the Chicago firewall by clicking the **Logout** button in the bottom-left corner of the window.
343. Log back in with **`admin/Pal0Alt0!`** so you can see the changes applied from Panorama.
344. Note the red banner with text surrounding the browser page. This banner can help you distinguish firewall web interfaces from one another and from the Panorama web interface when you are working in multiple devices:



345. Select **Network** > **Interfaces**.
346. Note that Panorama has pushed down IP addresses for **ethernet1/1**, **ethernet1/2**, and **ethernet1/3**:

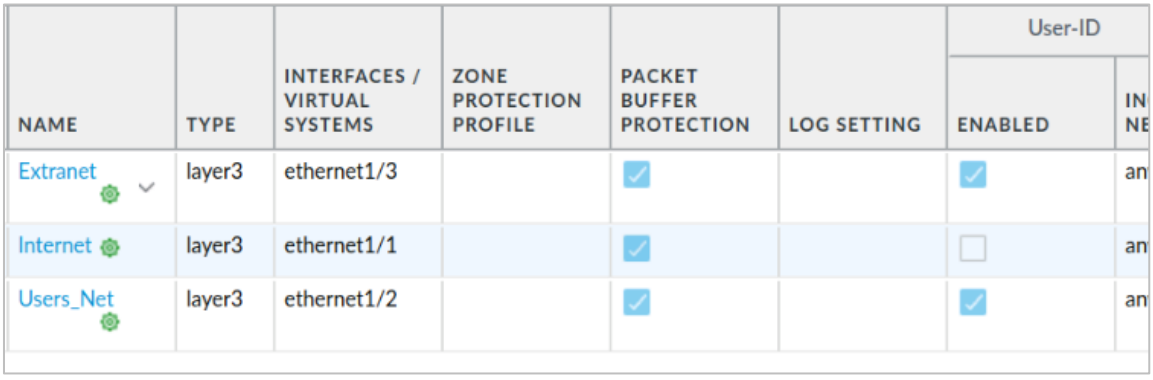


347. Hover your pointer over the small green gear icon next to **ethernet1/3** to see where this setting came from:



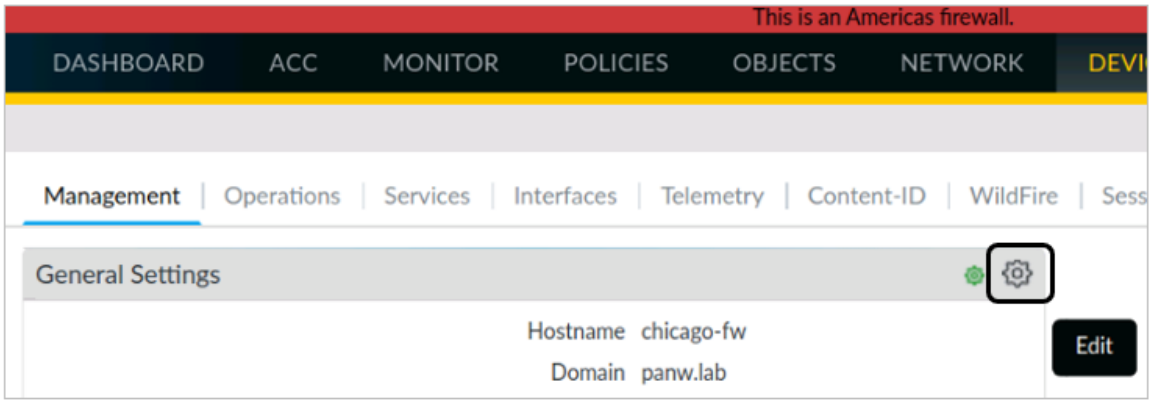
In this example, ethernet1/3 was pushed down by the US-Stack Template stack.

348. Select **Network > Zones**.
349. Panorama has pushed down three security zones, each attached to the appropriate Ethernet interface:

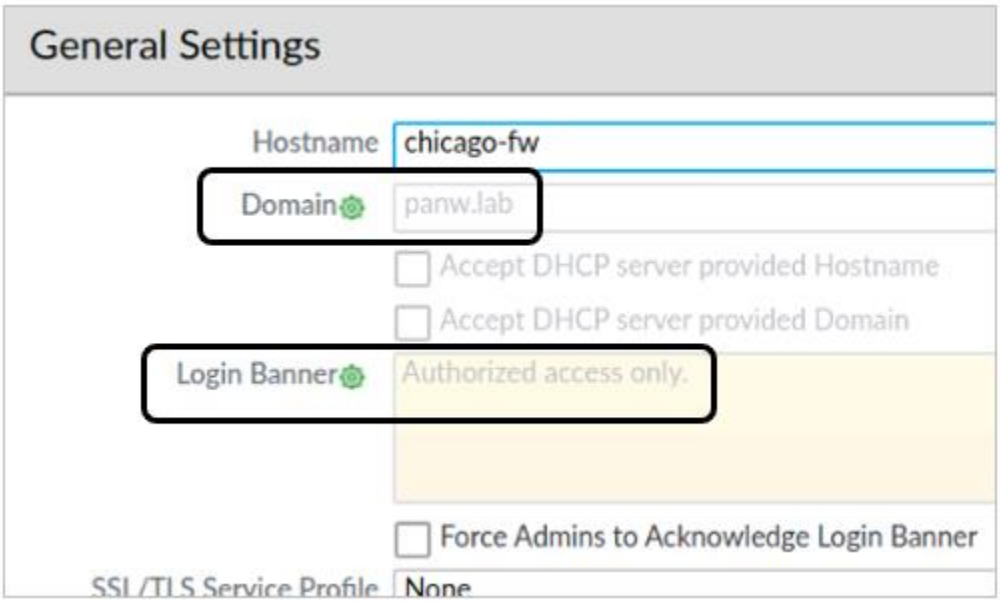


350. Note that **ethernet1/3** and **ethernet1/2** both have **User-ID** enabled.
351. Select **Device > Setup > Management**.
352. For each of the areas that have been modified by a Template stack from Panorama, you will see a small green gear icon:

353. Click the **Edit** icon in the **General Settings** section:



354. Note that **Domain** and **Login Banner** have small green icons next to them:



These identifiers let you quickly determine which specific items have been pushed down from Panorama.

355. Click **OK**.
356. Select **Device > Server Profiles > Syslog**.
357. Note that the Chicago firewall uses the **US-Syslog-1** server.
358. Select **Device > Server Profiles > Email**.

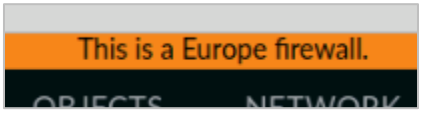
359. Note that the Chicago firewall uses the **US-Mail-1** server and the **Email Display Name** and **From** fields reference **Chicago**:

	NAME	L...	Servers						
			NAME	EMAIL DISPLAY NAME	FROM	TO	ADDITIONAL RECIPIENT	EMAIL GATEWAY	PROTOCOL
☐	Email-Servers		US-Mail-1	Chicago Firewall	chicago-fw@panw.lab	paloalto42@pan...		192.168.50.150	Unauthentic... SMTP

360. Close the Configuration browser tab for the Chicago firewall.

Verify Template Settings on the Berlin Firewall

361. Log out of the Berlin firewall by clicking the **Logout** button in the bottom-left corner of the window.
362. Log in to the Berlin firewall using **`admin`** as the **Username** and **`Pal0Alt0!`** as the **Password** so you can see the changes applied from Panorama.
363. Note the orange banner surrounding the browser page:

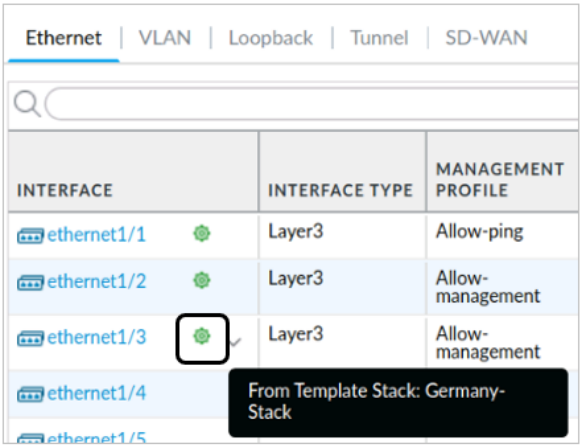


364. Select **Network** > **Interfaces**.
365. Note that Panorama has pushed down IP addresses for **ethernet1/1**, **ethernet1/2**, and **ethernet1/3**:

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	LOGICAL ROUTER	TAG	SECURITY ZONE	COMMENT
ethernet1/1	Layer3	Allow-ping		203.0.113.25/24	LR-1	Untagged	Internet	Internet interface
ethernet1/2	Layer3	Allow-management		192.168.1.5/24	LR-1	Untagged	Users_Net	User-Net Interface
ethernet1/3	Layer3	Allow-management		192.168.50.5/24	LR-1	Untagged	Extranet	Extranet Interface

366. Hover your pointer over the small green gear icon next to ethernet1/3 to see where this setting came from:



In this example, ethernet1/3 was pushed down by the **Germany-Stack** Template stack.

367. Select **Network > Zones**.
368. Panorama has pushed down three security zones, each attached to the appropriate Ethernet interface:

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	User-ID ENABLED	User-ID IN NE
Extranet	layer3	ethernet1/3		☑		☑	any
Internet	layer3	ethernet1/1		☑		☐	any
Users_Net	layer3	ethernet1/2		☑		☑	any

369. Select **Device > Server Profiles > Syslog**.
370. Note that the Berlin firewall uses the **EU-Syslog-1** server.
371. Select **Device > Server Profiles > Email**.
372. Note that the Berlin firewall uses the **EU-Mail-1** server and the **Email Display Name** and **From** fields reference Berlin:

NAME	L...	Servers: NAME	EMAIL DISPLAY NAME	FROM	TO	ADDITIONAL RECIPIENT	EMAIL GATEWAY	PROTOCOL
Email-Servers		EU-Mail-1	Berlin Firewall	berlin-fw@panw.lab	paloalto42@panw.lab		192.168.50.150	Unauthenticated SMTP

373. Close the Configuration browser tab for the Berlin firewall.

Stop. This is the end of the lab.

Lab 4 Scenario: Device Groups

You have identified common settings among the managed firewalls and want to capture them in Device Groups.

Certain Security policy rules and NAT policy rules will be needed on all firewalls. You will create a Device Group to contain these policy rules.

You also will create and apply a consistent set of Security Profiles on all firewalls. You will create a Security Profile Group to contain Security Profiles for the following:

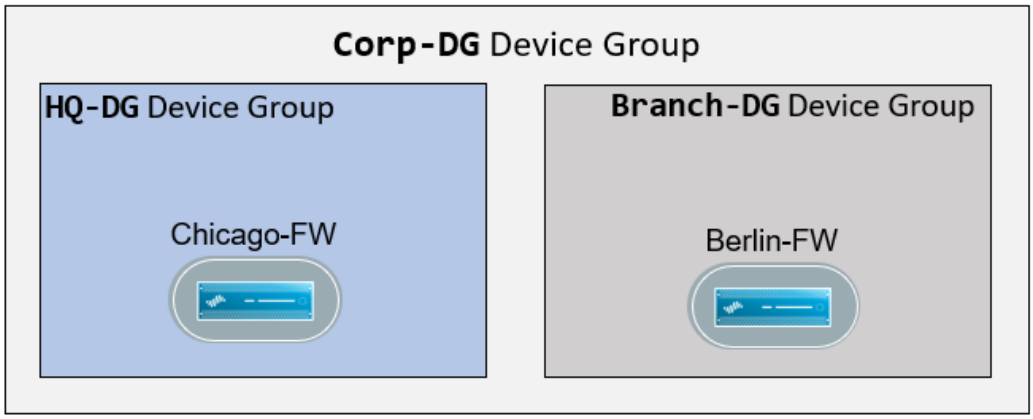
- Antivirus
- Anti-Spyware
- File-Blocking
- Vulnerability Protection
- URL Filtering
- WildFire Analysis

You want all firewalls to send log entry information to Panorama. You will create a default Log Forwarding Profile and make it available for all firewalls.

You will create a Device Group called Corp-DG to contain all these common settings for firewalls throughout your company.

However, there are functional differences between the firewalls in your company. Firewalls in the Branch offices require different Security policy and NAT policy rules from the firewalls in your headquarters offices. To account for these differences, you will create a Device Group for the firewalls in the Branch offices called Branch-DG. You also will create a separate Device Group for the firewalls in the headquarters offices called HQ-DG.

The managed firewall in Chicago is at one of your company's regional headquarters, so you will assign this firewall to the HQ-DG Device Group. The managed firewall in Berlin is located at one of your branch locations, so you will assign this firewall to the Branch-DG Device Group. The following diagram illustrates the Device Groups you will create:

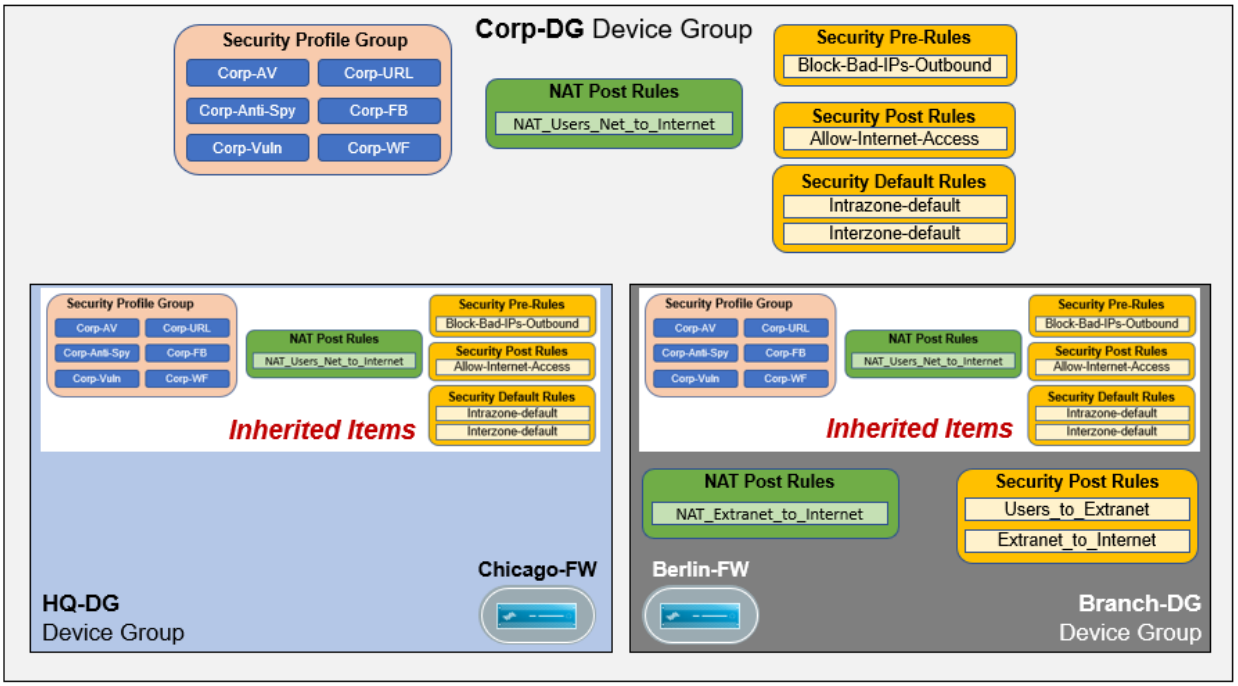


Lab Objectives

In this lab, you will perform the following tasks:

- Create Device Groups
- Create Security Profiles
- Create a Security Profile Group
- Configure Security Policy Pre-Rules
- Configure Security Policy Post-Rules
- Modify Default Security Policy rules
- Create NAT Post Rules for Users_Net traffic
- Preview the rules in Panorama
- Test Internet access
- Confirm the configurations on each firewall

The following diagram provides an overview of the elements you will create in the Device Groups:



The Branch-DG and the HQ-DG are descendants of the Corp-DG. All the objects and policy rules you create in the Corp-DG are inherited by the Branch-DG and the HQ-DG.

High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-4-Start.xml** configuration file on Panorama.

Create a Device Group Called Corp-DG

- Create a Device Group called **Corp-DG**.
- For **Description**, use **`Contains common Objects and Policies for all firewalls`**.

Create a Device Group Called Branch-DG

- Create a descendant Device Group of **Corp-DG** called **Branch-DG**.
- For **Description**, use **`Contains common Objects and Policies for Branch firewalls`**.

Create a Device Group called HQ-DG

- Create a descendant Device Group of **Corp-DG** called **HQ-DG**

- For **Description**, use **`Contains common Objects and Policies for HQ firewalls`**.

Create Security Profiles in the Corp-DG Device Group

- Create **Security Profiles** in the **Corp-DG** Device Group.

Create an Antivirus Security Profile

- Clone the **default Antivirus** profile and rename the clone **`Corp-AV`**.
- For **Description**, use **`Default Antivirus profile used for security policy rules`**.

Create an Anti-Spyware Security Profile

- Clone the **strict Anti-Spyware** profile and rename the clone **`Corp-Anti-Spy`**.
- For **Description**, use **`Default Anti-Spyware profile used for security policy rules.`**

Create a Vulnerability Protection Security Profile

- Clone the **strict Vulnerability Protection** profile and rename the clone **`Corp-Vuln`**.
- For **Description**, use **`Default vulnerability profile used for security policy rules`**.

Create a URL Filtering Security Profile

- Clone the **default URL Filtering** profile and rename the clone **`Corp-URL`**.
- For **Description**, use **`Default URL Filtering profile used for security policy rules`**.
- Set the action for all categories to **alert**.

Create a File Blocking Security Profile

- Clone the entry for **Strict file blocking** profile and rename the clone **`Corp-FB`**.
- For **Description**, use **`Default file blocking profile used for security policy rules`**.

Create a WildFire Analysis Security Profile

- Clone the **default Wildfire** profile and rename the clone **`Corp-WF`**.
- For **Description**, use **`Default Wildfire profile used for security policy rules`**.

Create a Security Profile Group in the Corp-DG Device Group

- Create a Security Profile Group called **`Corp-Profiles`**.
- For each of the categories, select the **Corp-** profile you created.
- Leave the **Data Filtering Profile** set to **None**.

Commit the Configuration

- Commit these changes to Panorama.
- Allow the process to complete.
- Push the changes to the firewalls using **`Force Template Values`**.

Configure Security Policy Pre-Rules

- Create a Security Policy Pre-Rule in the Corp-DG using the following information:

Parameter	Value
Name	`Block-Bad-IPs-Outbound`
Description	`Blocks traffic to bad IP addresses based on PANW lists.`
Source Zone	`Users_Net` `Extranet`
Destination Zone	`Internet`

Destination Address	`Bulletproof IP addresses`
	`High Risk IP addresses`
	`Known Malicious IP addresses`

Application	`Any`
Service	`application-default`
Actions	`Deny`

Configure Security Policy Post-Rules

- Create a Security Policy Post Rule in the Corp-DG using the following information:

Parameter	Value
Name	`Allow-Internet-Access`
Description	`Allows hosts in the Users_Net zone access to the Internet for all applications.`

Parameter	Value
Source Zone	Users_Net
Destination Zone	Internet
Application	Any
Service	application-default
Actions	Allow
Profile Type	Group
Group Profile	Corp-Profiles

Modify the intrazone-default Security Policy Rule

- Override the entry for intrazone-default Security Policy rule and enable Log at Session End
- Apply the Corp-Profiles Group Profile to the rule

Modify the interzone-default Security Policy Rule

- Override the entry for interzone-default Security Policy rule and enable Log at Session End

Create a Security Policy Post-Rule for Users to Extranet

- Use the information below to create a Security Policy Post Rule in the HQ-DG:

Parameter	Value
Name	Users_to_Extranet
Description	Allows Users_Net to Extranet.
Source Zone	Users_Net
Destination Zone	Extranet
Application	Any
Service	application-default
Actions	Allow
Profile Type	Group
Group Profile	Corp-Profiles

Create a Security Policy Rule for Extranet Traffic

- Use the information below to create a Security Policy Post Rule in the HQ-DG:

Parameter	Value
Name	**Extranet_to_Internet**
Description	**Allows Extranet to Internet traffic.**
Source Zone	**Extranet**
Destination Zone	**Internet**
Application	**Any**
Service	**application-default**
Actions	**Allow**
Profile Type	**Group**
Group Profile	**Corp-Profiles**

Create a NAT Post-Rule for Users_Net Traffic

- Create a NAT Post-Rule in the Corp-DG using the following information:

Parameter	Value
Name	**NAT_Users_Net_to_Internet**
Description	**Translates traffic from Users_Net to Internet using e1/1 from firewall.**
NAT Type	**ipv4**
Source Zone	Click **Add** and select **Users_Net**
Destination Zone	Select **Internet**
Source Address Translation Section	Set **Translation Type** to **Dynamic IP and Port**
Address Type	Select **Interface Address**
Interface	**ethernet1/1**
IP Type	**IP**
Field below IP Type	**$Internet-Interface**

Create a NAT Post-Rule for Extranet Traffic

- Create a NAT Post-Rule in the HQ-DG using the following information:

Parameter	Value
Name	**`NAT_Extranet_to_Internet`**
Description	**`Translates traffic from Extranet to Internet using e1/1 from firewall.`**
NAT Type	**`ipv4`**
Source Zone	Click **Add** and select **Extranet**
Destination Zone	Select **Internet**
Source Address Translation Section	Set **Translation Type** to **Dynamic IP and Port**
Address Type	Select **Interface Address**
Interface	**ethernet1/1**
IP Type	**IP**
Field below IP Type	**$Internet-Interface**

Commit the Configuration to Panorama

- Commit these changes to Panorama

Preview the Rules in Panorama

- Use the Preview Rules feature to examine the Security Rules for the Branch-DG firewall and then for the HQ-DG

Push the Configuration to the Firewalls

- Push the changes to the firewalls using **`Force Template Values`**

Test Internet Access from User Hosts

- On client-A, use the Testing web browser to connect to **https://www.paloaltonetworks.com** and **http://www.panw.l**ab to verify that you have configured the chicago-fw correctly for access to hosts in the Internet and Extranet security zones.
- Use Remmina to connect to the Server-Extranet host and ping **www.paloaltonetworks.com**
- Use Remmina to log in to client-B and use ping **www.paloaltonetworks.com**.

Confirm the Configurations on Each Firewall

- Log in to the Chicago firewall and verify that Panorama has pushed down the appropriate Security policy and NAT policy rules.
- Log in to the Berlin firewall and verify that Panorama has pushed down the appropriate Security policy and NAT policy rules.

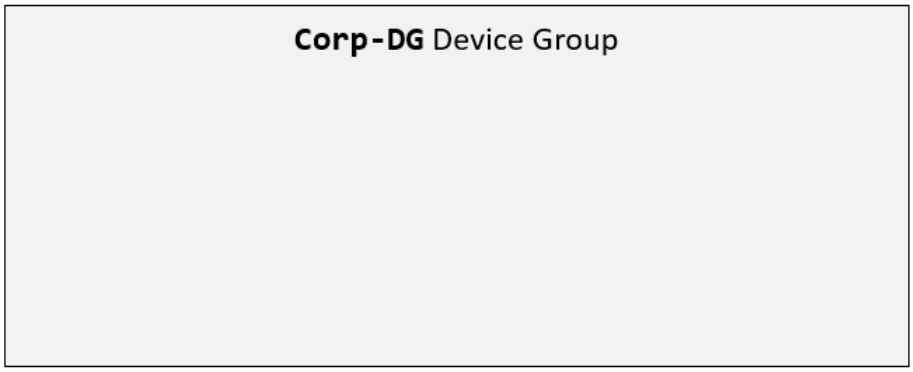
Detailed Lab Steps

Load the Lab Start Configuration File

1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-4-Start.xml**.
4. Leave the remaining settings unchanged.
5. Click **OK** to close the **Load Named Configuration** window.
6. Click **Close** on the **Loading Configuration** window.
7. Commit the changes to Panorama by selecting **Commit** > **Commit to Panorama** in the upper-right corner of the window.
8. In the **Commit to Panorama** window, click **Commit**.
9. Allow the process to complete.
10. Click **Close** in the **Commit Status** window.

Create a Device Group Called Corp-DG

In this section, you will create a Device Group named **Corp-DG**. You then will create two more Device Groups within the Corp-DG Device Group: the **Branch-DG** Device Group and the **HQ-DG** Device Group. You will add the **Chicago** firewall to the **HQ-DG** Device Group and the **Berlin** firewall to the **Branch-DG** Device Group:



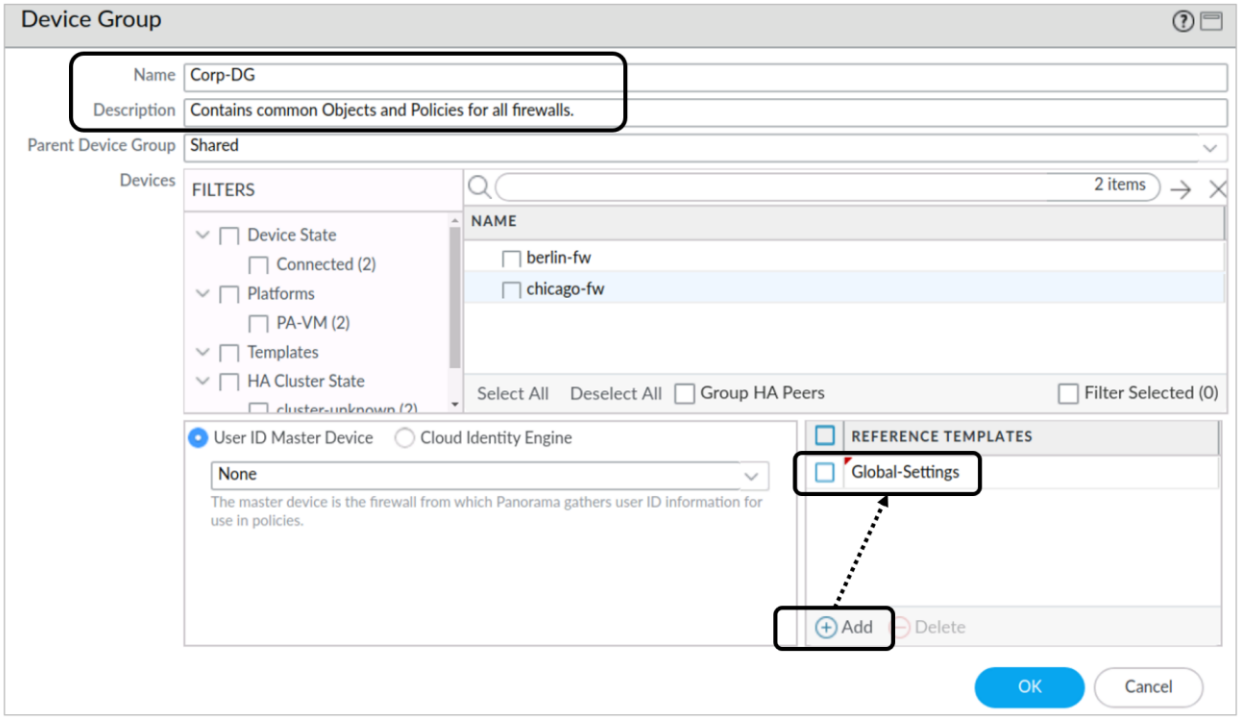
11. Select **Panorama** > **Device Groups**.
12. Click **Add**, and then create a new Device Group named **Corp-DG**.
13. Under the section for **Reference Templates**, click **Add**.
14. Select **Global-Settings**.

Panorama uses the Reference Template to obtain security zones (which are defined in Panorama Templates). We need security zones to create Security policy and NAT policy rules, so we are using the Global-Settings Template, which contains our security zones.

15. For **Description**, enter the following:

    `Contains common Objects and Policies for all firewalls.`

16. Leave the remaining settings unchanged.

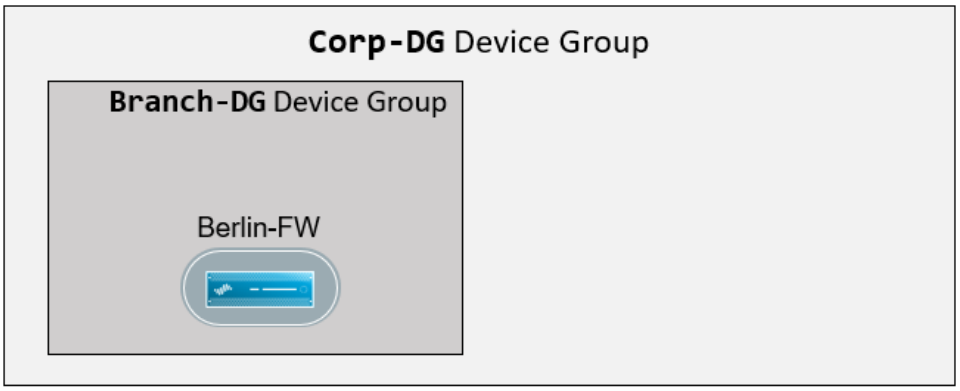


Do not check the box beside either firewall. You will assign each firewall to a descendant Device Group later in this lab.

17. Click **OK**.
18. Notice that the **Policies** and **Objects** tabs now appear in the Panorama web interface:

Create a Device Group Called Branch-DG

In this section, you will create a new Device Group called Branch-DG. This new Device Group will be a descendant of the **Corp-DG** Device Group. You will place the Berlin-FW in the Branch-DG Device Group:



19. In the **Device Groups** window, highlight the entry for **Corp-DG** without opening it.
20. Click **Add**.
21. Enter the name **`Branch-DG`**.
22. Check the **box** beside the **berlin-fw**.
23. In the third line of the window, verify that the **Parent Device Group** is set to **Corp-DG**.
24. For **Description**, enter the following:

    `Contains Objects and Policies for branch firewalls.`

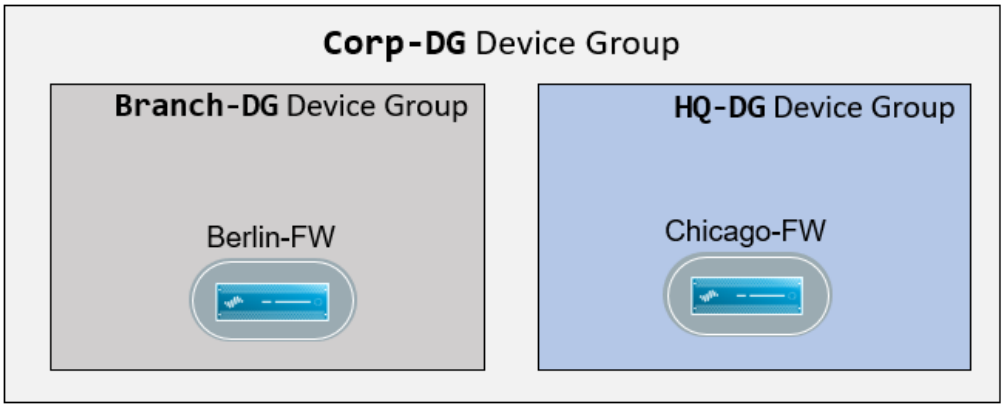
25. Leave the remaining settings unchanged.
26. Click **OK**.
27. The Device Group **Branch-DG** is listed as a subordinate of **Corp-DG**:

NAME	DESCRIPTION	DEVICES/VIRTUAL SYSTEM
Shared		
Corp-DG	Contains common Object and Policies for all firewalls.	
Branch-DG	Contains Objects and Policies for branch firewalls.	berlin-fw

Verify that you have defined the Branch-DG Device Group as a descendant of the Corp-DG. If not, delete the entry for Branch-DG and perform the preceding steps again.

Create a Device Group called HQ-DG

This Device Group will be a descendant of the Corp-DG Device Group. You will place the Chicago-FW in this HQ-DG Device Group:



28. Highlight the **Corp-DG** entry without opening it.
29. Click **Add**.
30. Enter the name **HQ-DG**.
31. Select **chicago-fw**.
32. In the third line of the window, verify that the **Parent Device Group** is set to **Corp-DG**.
33. For **Description**, enter the following:

    Contains common Objects and Policies for HQ firewalls.

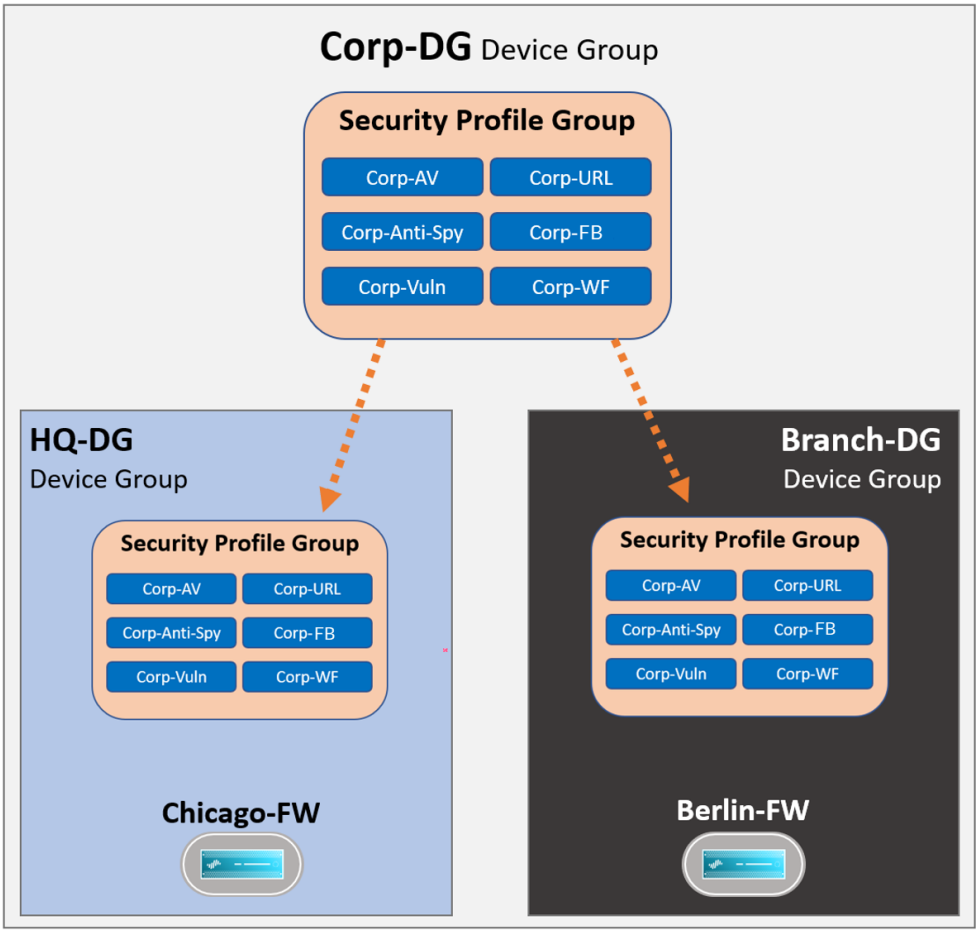
34. Leave the remaining settings unchanged.
35. Click **OK**.
36. The Device Group **Branch-DG** is listed as a subordinate of **Corp-DG**:

NAME	DESCRIPTION	DEVICES/VIRTUAL SYSTEM
Shared		
Corp-DG	Contains common Object and Policies for all firewalls.	
Branch-DG	Contains Objects and Policies for branch firewalls.	berlin-fw
HQ-DG	Contains common Objects and Policies for HQ firewalls.	chicago-fw

Elements you create in the Corp-DG Device Group will be inherited in the HQ-DG and in the Branch-DG Device Groups.

Create Security Profiles in the Corp-DG Device Group

You want all firewalls in your organization to apply a consistent set of Security Profiles for Antivirus, Anti-Spyware, File-Blocking, Vulnerability Protection, URL Filtering, and WildFire Analysis. You will create a Security Profile for each category and then place each Security Profile into a single Security Profile Group. You then can easily apply the Security Profile Group to your Security policy rules:



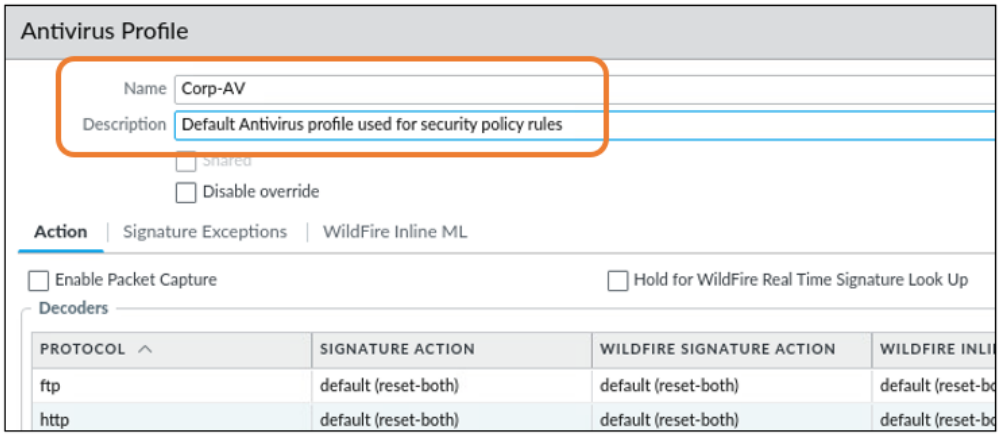
Create an Antivirus Security Profile

In this section, you will create a new Antivirus Security Profile.

37. In the Panorama web interface, select **Objects > Security Profiles > Antivirus**.
38. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

39. At the bottom of the window, click **Add**.

40. For **Name**, enter **`Corp-AV`**.
41. For **Description**, enter **`Default Antivirus profile used for security policy rules`**.
42. Leave the remaining settings unchanged:



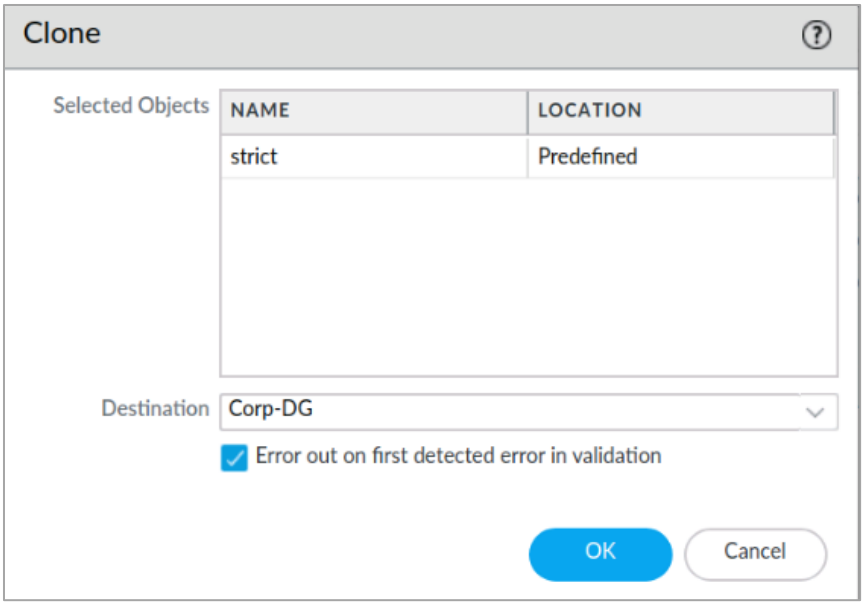
43. Click **OK**.

Create an Anti-Spyware Security Profile

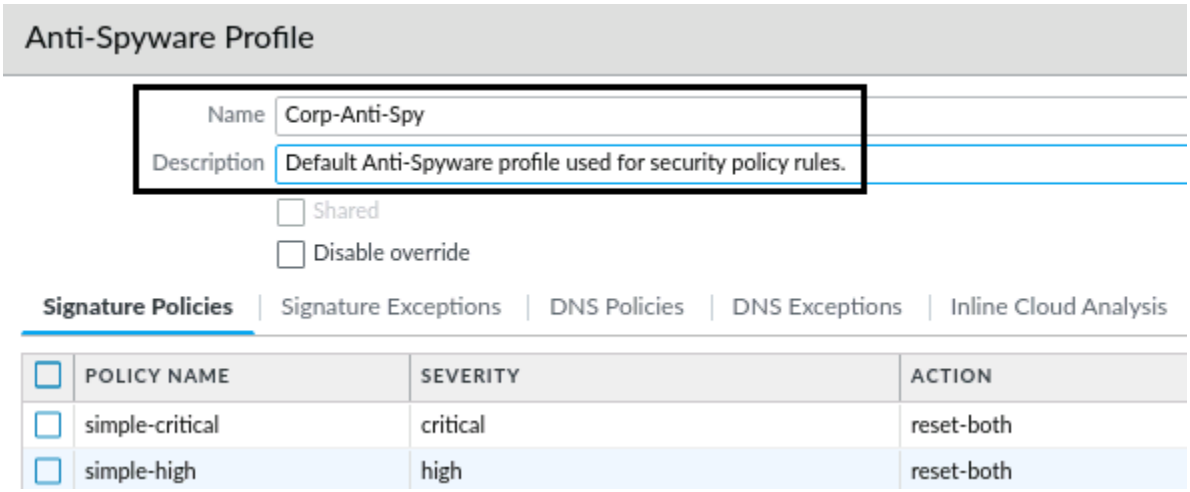
In this section, you will clone the predefined Anti-Spyware Security Profile called **strict**. You then will make changes to your cloned copy.

44. Select **Objects > Security Profiles > Anti-Spyware**.
45. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

46. Highlight the entry for **strict**.
47. Click **Clone**.
48. In the **Clone** window, leave the settings unchanged:



49. Click **OK** to create a new profile called **strict-1**.
50. Click the link for the **strict-1** entry.
51. Change the **Name** to **`Corp-Anti-Spy`**.
52. For **Description**, enter **`Default Anti-Spyware profile used for security policy rules`**.
53. Leave the remaining settings unchanged:



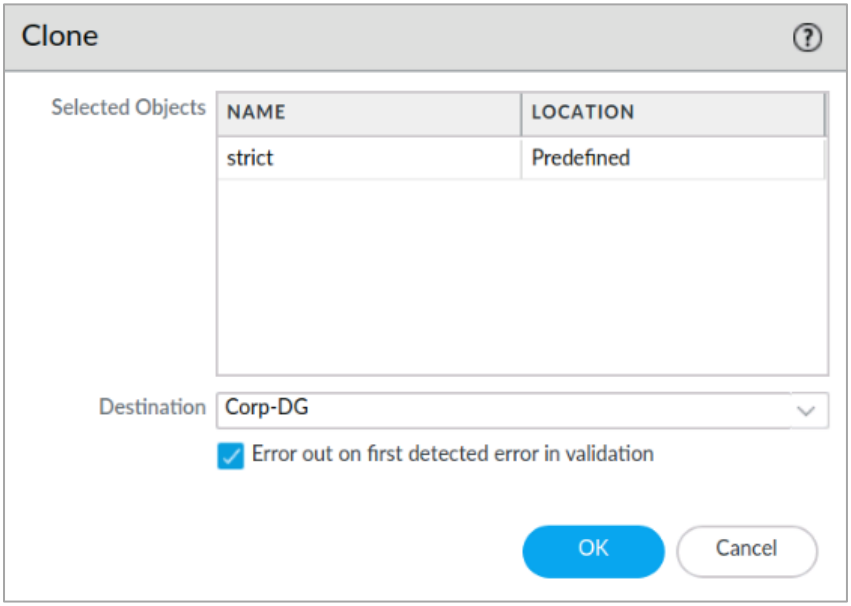
54. Click **OK**.

Create a Vulnerability Protection Security Profile

In this section, you will clone the predefined Vulnerability Security Profile called **strict**. You then will be able to make changes to your cloned copy.

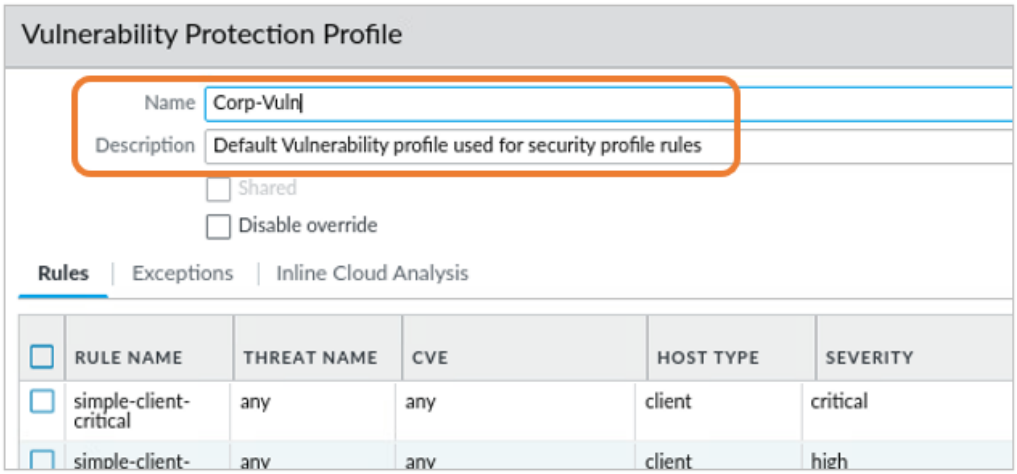
55. Select **Objects > Security Profiles > Vulnerability Protection**.
56. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

57. Highlight the entry for **strict**.
58. Click **Clone**.
59. In the **Clone** window, leave the settings unchanged:



60. Click **OK** to create a new profile called **strict-1**.
61. Edit the entry for **strict-1**.
62. Change the name to **`Corp-Vuln`**.
63. For **Description**, enter **`Default Vulnerability profile used for security policy rules`**.

64. Leave the remaining settings unchanged:



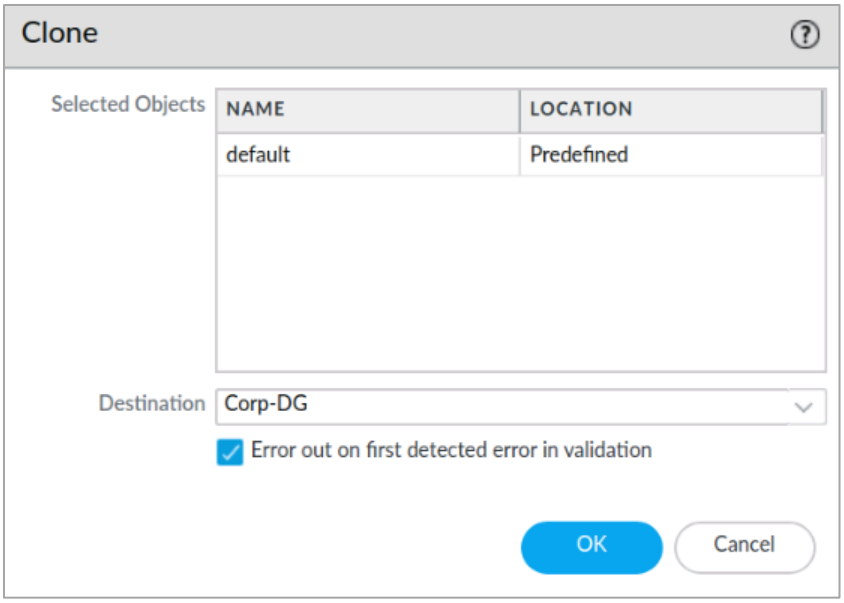
65. Click **OK**.

Create a URL Filtering Security Profile

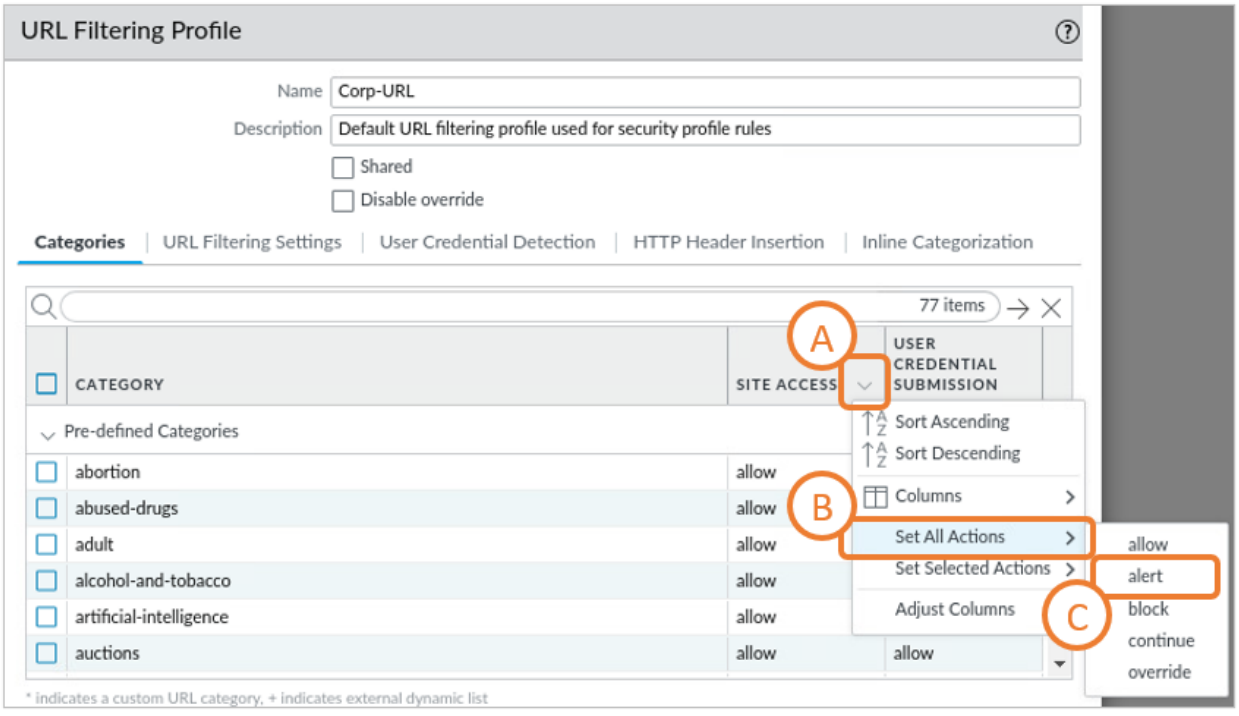
In this section, you will clone the predefined URL Filtering Security Profile called **default**. You then can make changes to your cloned copy.

66. Select **Objects > Security Profiles > URL Filtering**.
67. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

68. Highlight the entry for **default**.
69. Click **Clone**.
70. In the **Clone** window, leave the settings unchanged:



71. Click **OK** to create a new profile called **default-1**.
72. Edit the entry for **default-1**.
73. Change the **Name** to **`Corp-URL`**.
74. For **Description**, enter **`Default URL filtering profile used for security policy rules`**.
75. Click the small down arrow in the right side of the **Site Access** column and choose **Set All Actions**.
76. Choose **alert**:



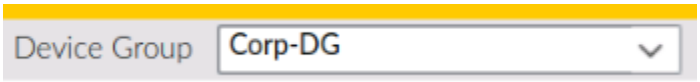
This setting instructs firewalls to allow all URL requests for each category and to log each request in the URL Filtering log. The “allow” action only allows a request but does not log it.

77. Click **OK** to create a new URL Filtering profile.

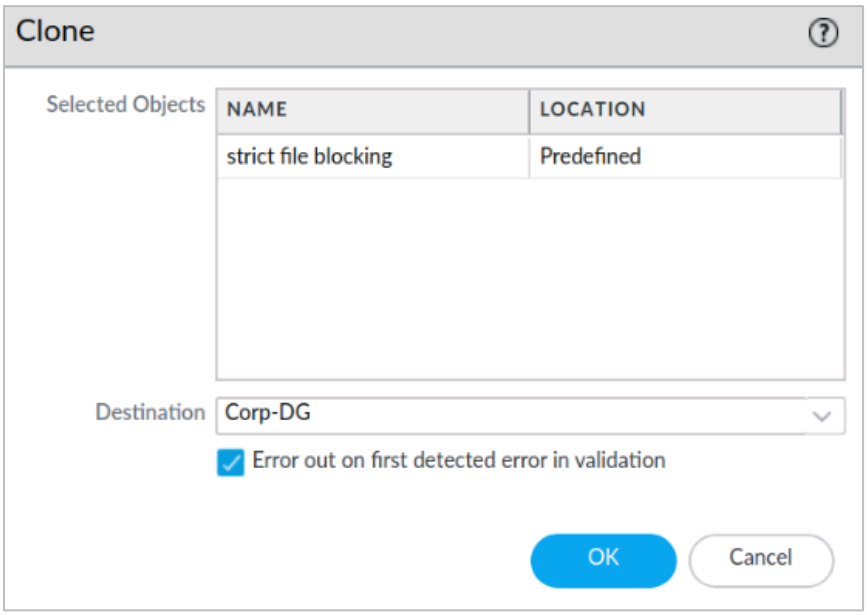
Create a File Blocking Security Profile

In this section, you will clone the predefined File Blocking Security Profile called **strict file blocking**. You then can make changes to your cloned copy.

78. Select **Objects > Security Profiles > File Blocking**.
79. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

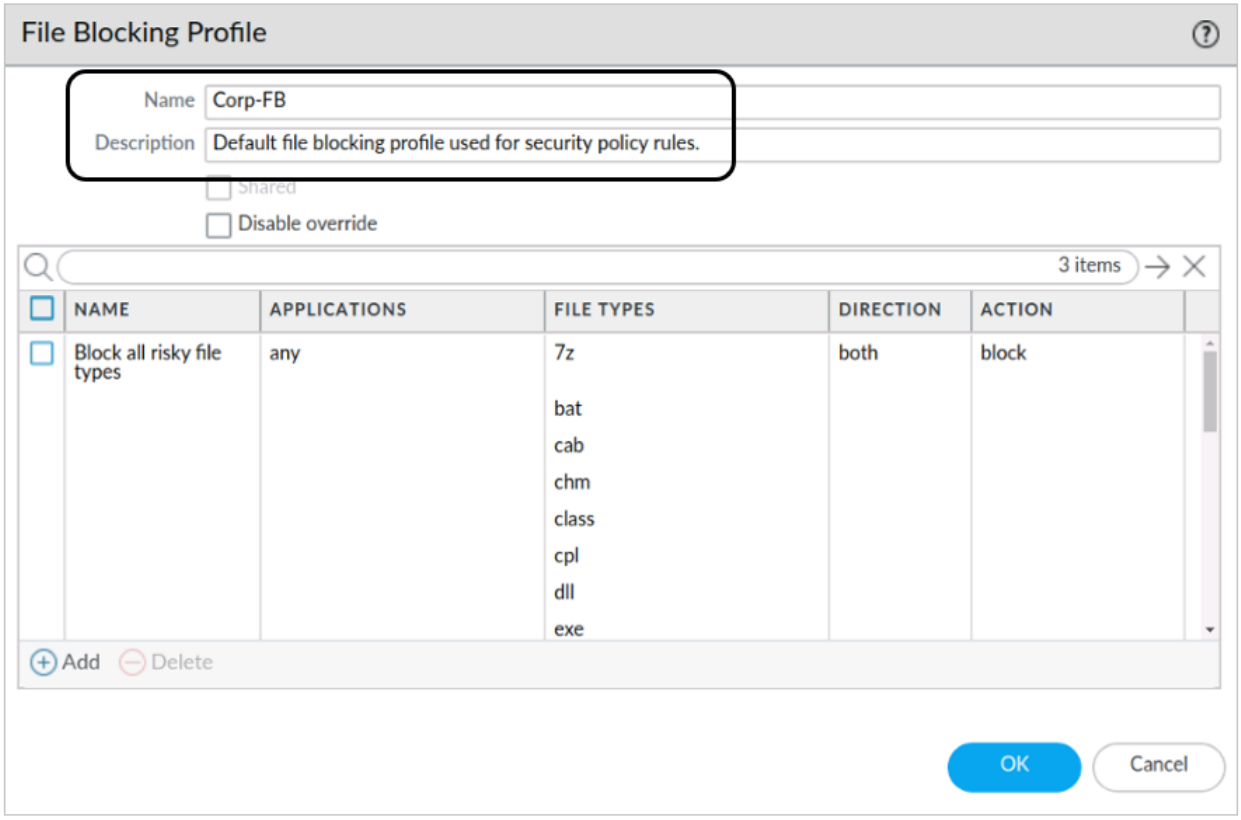


80. Highlight the entry for **strict file blocking**.
81. Click **Clone**.
82. In the **Clone** window, leave the settings unchanged:



83. Click **OK** to create a new profile called **strict file blocking-1**.
84. Edit the entry for **strict file blocking-1**.
85. Change the **Name** to **`Corp-FB`**.

86. For **Description**, enter **`Default file blocking profile used for security policy rules`**.
87. Leave the remaining settings unchanged:



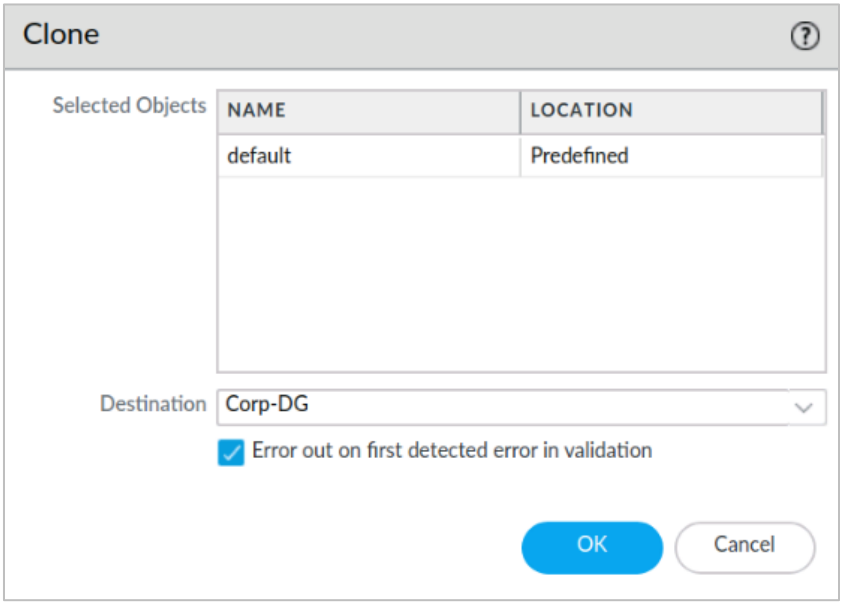
88. Click **OK**.

Create a WildFire Analysis Security Profile

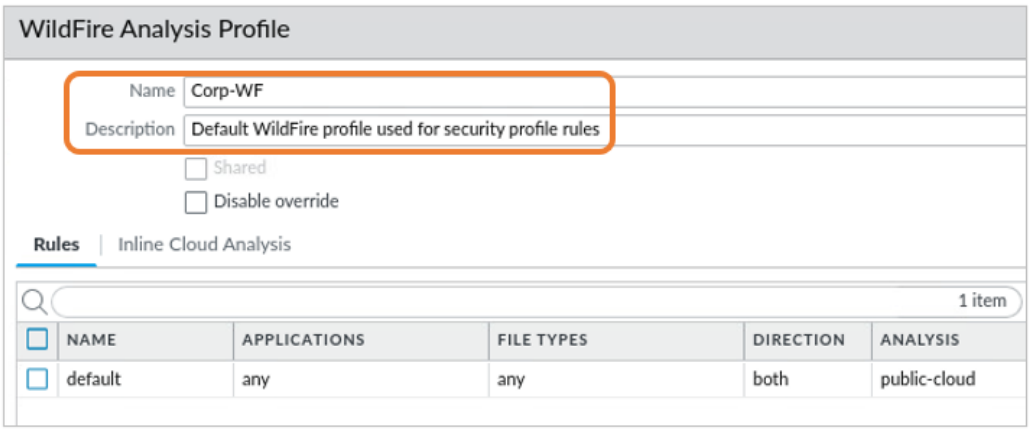
89. Select **Objects > Security Profiles > WildFire Analysis**.
90. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

91. Highlight the entry for **default**.
92. Click **Clone**.

93. In the **Clone** window, leave the settings unchanged:



94. Click **OK** to create a new profile called **default-1**.
95. Edit the entry for **default-1**.
96. Change the **Name** to **`Corp-WF`**.
97. For **Description**, enter **`Default WildFire profile used for security policy rules`**.
98. Leave the remaining settings unchanged:

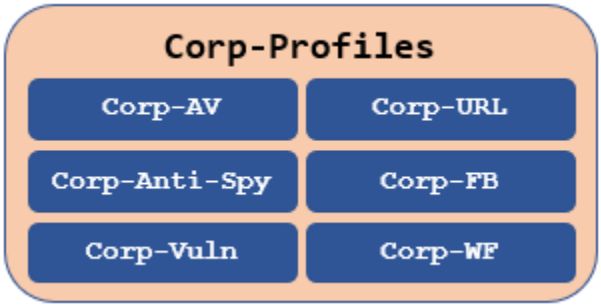


99. Click **OK**.

Create a Security Profile Group in the Corp-DG Device Group

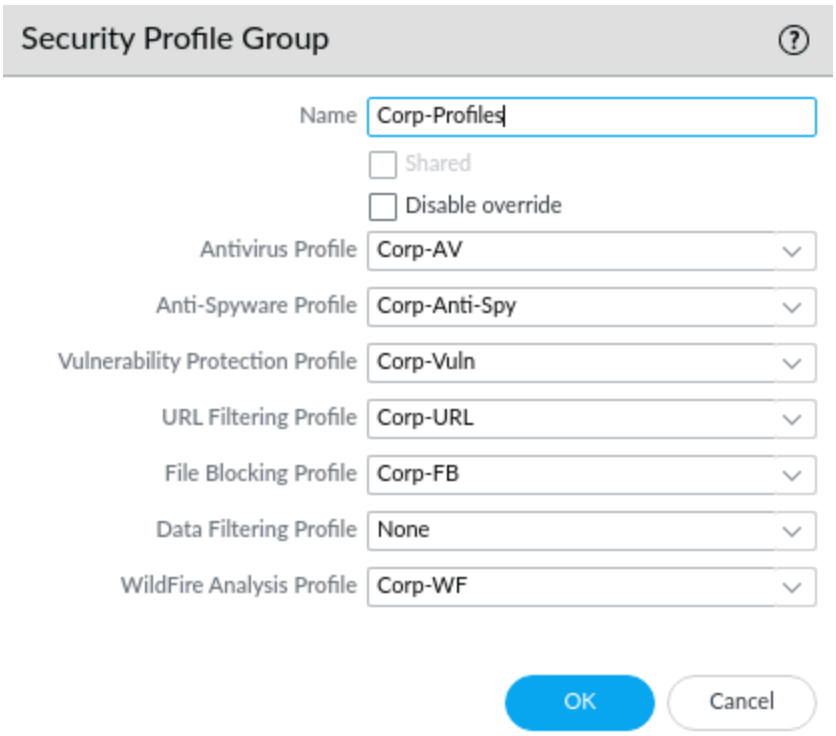
You have created corporate Security Profiles. You now can add each one to a single Security Profile Group. When you create a Security policy rule, you can select the single Security Profile Group instead of selecting each individual Security Profile.

In this section, you will create a Security Profile Group called Corp-Profiles and add each Security Profile to this Group:



100. Select **Objects > Security Profile Groups**.
101. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

102. Click **Add**.
103. For **Name**, enter **`Corp-Profiles`**.
104. For each of the categories, select the **Corp-** profile you created:
    - **Corp-AV**
    - **Corp-Anti-Spy**
    - **Corp-Vuln**
    - **Corp-URL**
    - **Corp-FB**
    - **Corp-WF**
105. Leave the **Data Filtering Profile** set to **None**.
106. Leave the remaining settings unchanged:

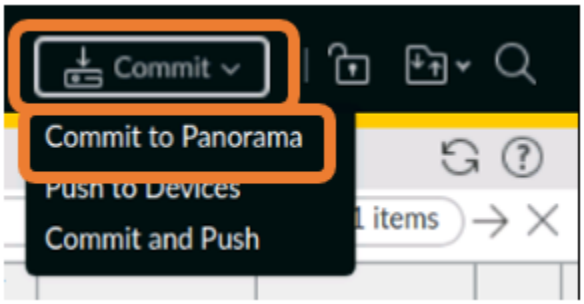


The name of the Security Profile Group and the individual profiles do not have to match, as they do in this example. However, using the same initial name for the Group and each individual profile can help you more easily match them in an environment where you may have many different Security Profiles and Security Profile Groups.

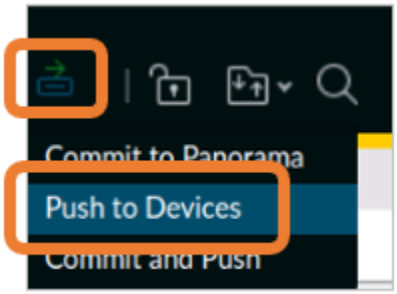
107. Click **OK**.

Commit the Configuration

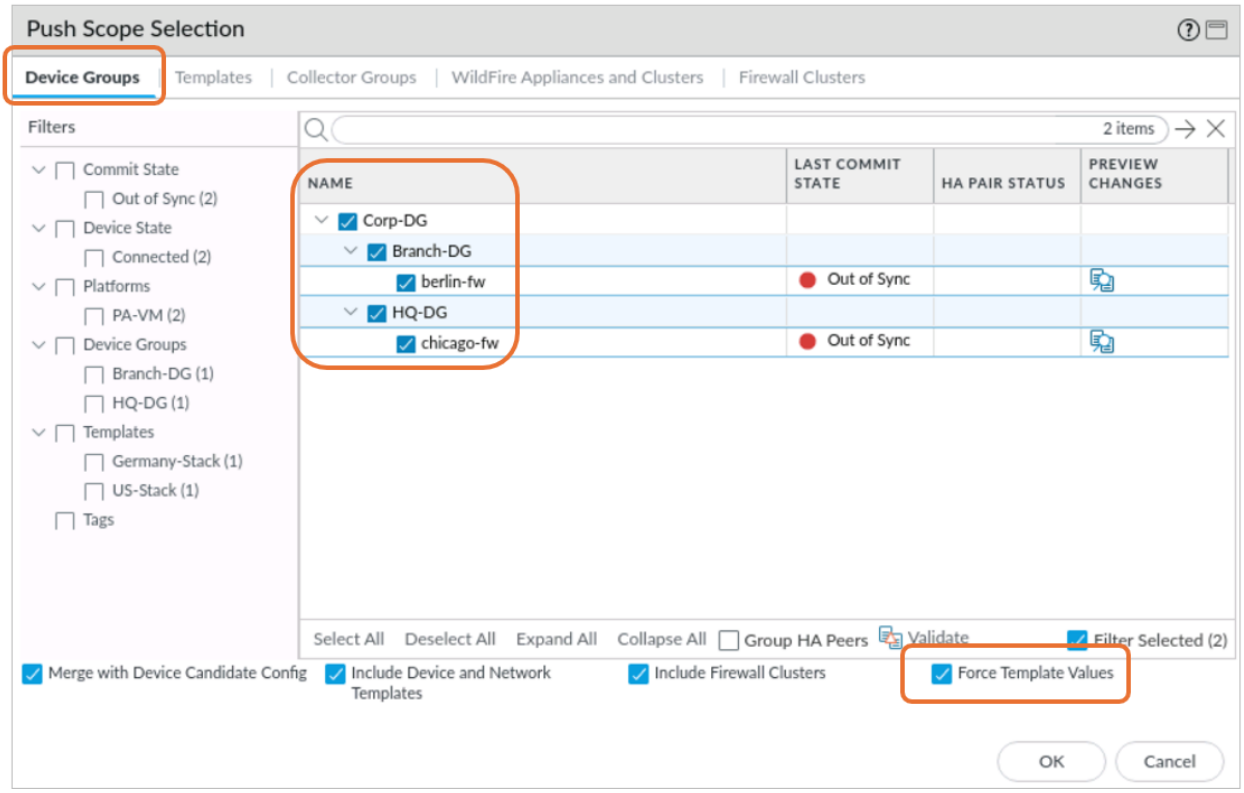
108. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



109. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
110. Monitor the status of the commit.
111. When the commit status is complete, click **Close**.
112. Select the Commit icon and choose **Push to Devices**:



113. Click **Edit Selections**.
114. Select the **Device Groups** tab, and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected:
115. Select the **Force Template Values** check box at the bottom.
116. Click **Yes** on the **Force Template Values** warning message:



Note – if you do not see a firewall listed, then uncheck the box for Filter Selected in the bottom right corner of the Push Scope Selection window.

117. On the **Templates** tab, check the boxes for the Chicago firewall and the Berlin firewall.
118. Click **OK**.
119. Click **Push** to start the process.
120. Wait until the **Commit All** jobs are complete.
121. Click **Close**.

Configure Security Policy Pre-Rules

You want to apply certain Security policy rules to all firewalls in your network. In this section, you will create a Security policy rule to block outbound traffic to known bad IP addresses from the Users_Net or Extranet zone.

Because this entry will be created as a Security policy pre-rule, it will appear at the beginning of the Security policy ruleset for all firewalls. Local firewall administrators will not be able to place any Security policy rules higher than the pre-rules that you define and push from Panorama.

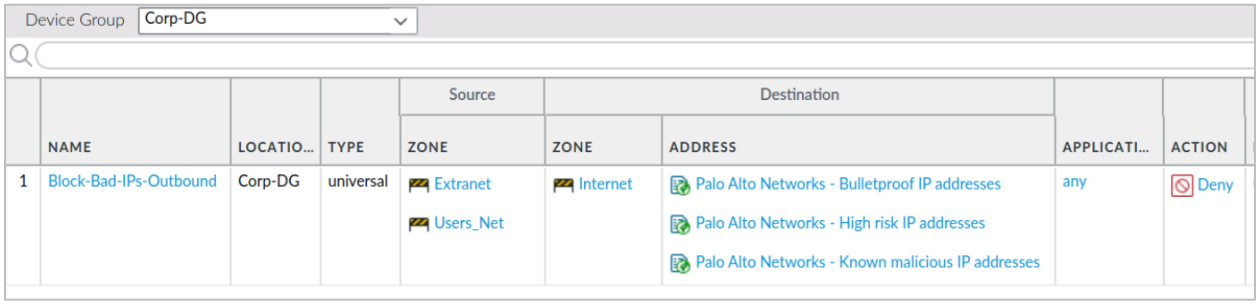
122. Select **Policies > Security > Pre Rules**.
123. From the drop-down list for **Device Group**, select **`Corp-DG`**.

124. Click **Add** and enter the following values:

Parameter	Value
General tab	
Name	`Block-Bad-IPs-Outbound`
Description	`Blocks traffic to bad IP addresses based on PANW lists.`
Source tab	
Source Zone	`Users_Net` `Extranet`
Destination tab	
Destination Zone	`Internet`
Destination Address	`Bulletproof IP addresses` `High Risk IP addresses`

Parameter	Value
	Known Malicious IP addresses
Application tab	
Application	Any
Service/URL Category tab	
Service	any
Actions tab	
Actions	Deny

125. Click **OK**.
126. Panorama creates an entry for your new rule in the Security policy:



Note that several columns have been hidden in the preceding image.

Configure Security Policy Post-Rules

In this section, you will create a Security policy post-rule to allow users to access the Internet. By placing this entry in the Security policy post-rules category, local administrators can create rules above the entry, which allows them to limit internet access for specific situations that would otherwise be granted by this Security policy rule.

127. Select **Policies** > **Security** > **Post Rules**.
128. Select **Corp-DG** from the **Device Group** drop-down list:

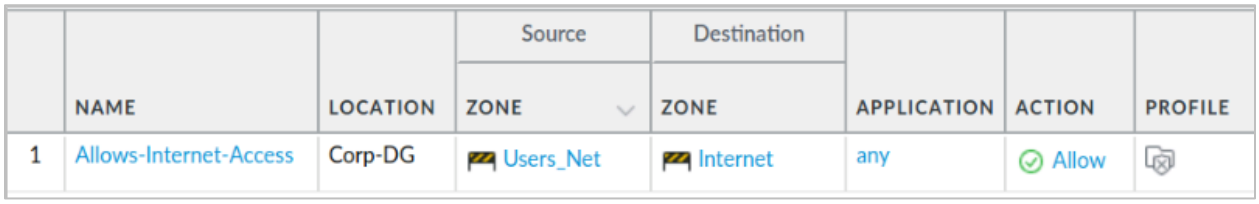
129. Click **Add** and enter the following values:

Parameter	Value
General tab	
Name	Allow-Internet-Access
Description	Allows hosts in the Users_Net zone access to the

Parameter	Value
	`Internet for all applications.`
Source tab	
Source Zone	`Users_Net`
Destination tab	
Destination Zone	`Internet`
Application tab	
Application	`Any`
Service/URL Category tab	
Service	`application-default`
Actions tab	
Actions	`Allow`
Profile Type	`Group`
Group Profile	`Corp-Profiles`

This security rule allows all applications and would not be appropriate for a production environment. You should always limit applications to only those that are necessary.

130. Click **OK**.
131. You should have a single Security policy rule entry in the post-rules table:

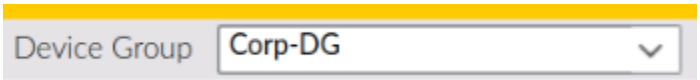


Note that several columns have been hidden in the preceding image.

Modify the intrazone-default Security Policy Rule

In this section, you will modify the intrazone-default Security policy rule and enable **Log at Session End**. You will apply the Corp-Profiles profile Group to this rule. The modified rule will be pushed down to all managed firewalls through the **Corp-DG** Device Group.

132. Select **Policies** > **Security** > **Default Rules**.
133. Select **Corp-DG** from the **Device Group** drop-down list:



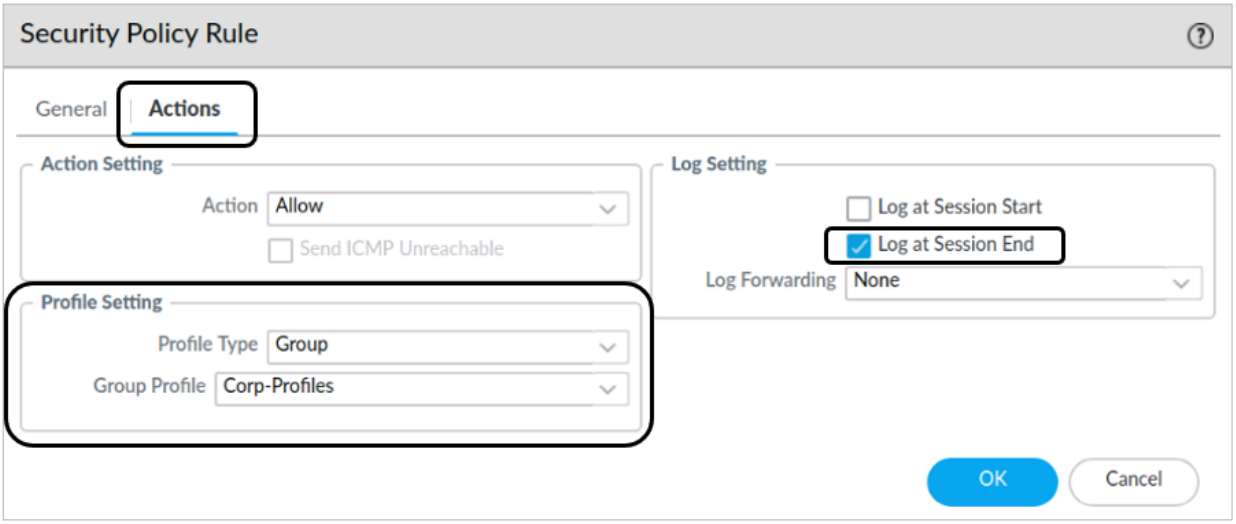
134. Highlight the entry for **intrazone-default** but do not open it.
135. Click **Override**.
136. Select the **Actions** tab.
137. Under the **Log Setting** section, place a **check mark** in the **box** for **Log at Session End**.

This setting instructs the firewall to create an entry in the Traffic log when an entry drops from the session table. By default, Palo Alto Networks firewalls do not write log entries for hits to intrazone traffic.

138. Under the **Profile Settings** section, set the **Profile Type** to **Group**.
139. For **Group Profile**, select **Corp-Profiles**.

These settings instruct the firewall to apply the Security Profiles contained in the Corporate-Security-Profiles Group that you created earlier. These profiles contain rules to examine traffic for viruses, spyware, vulnerabilities, and other malicious elements.

140. Leave the remaining settings unchanged:



141. Click **OK**.

Modify the interzone-default Security Policy Rule

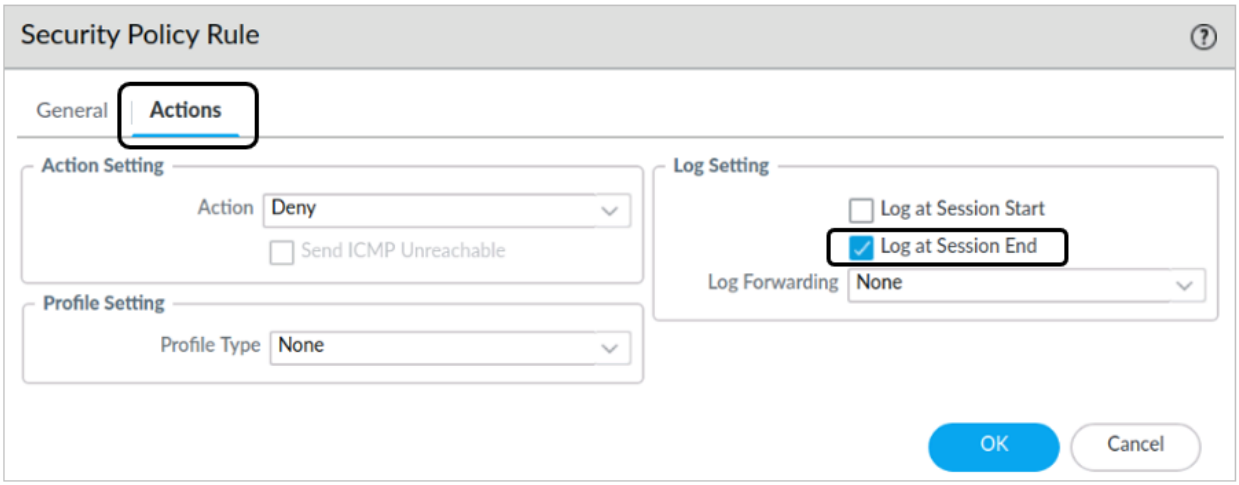
In this section, you will modify the interzone-default Security policy rule and enable **Log at Session End**. The modified rule will be pushed down to all managed firewalls through the **Corp-DG** Device Group.

142. Select **Policies** > **Security** > **Default Rules**.
143. Select **Corp-DG** from the **Device Group** drop-down list:

144. Highlight the entry for **interzone-default** but do not open it.
145. Click O**verride**.
146. Select the **Actions** tab.
147. Under the **Log Setting** section, place a **`check mark`** in the **box** for **Log at Session End**.

This setting instructs the firewall to create an entry in the Traffic log when an entry drops from the session table. By default, Palo Alto Networks firewalls do not write log entries for hits to interzone traffic.

148. Leave the remaining settings unchanged:



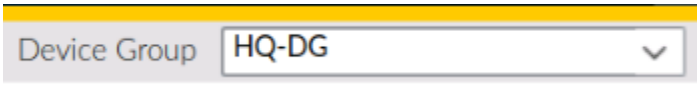
149. Click **OK**.

Create a Security Policy Post-Rule for Users to Extranet

Users in the Chicago office need access to hosts in the Extranet zone. In this section, you will create a Security policy rule to allow traffic from the **Users_Net** to the **Extranet** security zone. You will create this rule in the **HQ-DG** Device Group.

150. Select **Policies** > **Security** > **Post Rules**.

151. Select **HQ-DG** from the **Device Group** drop-down list:

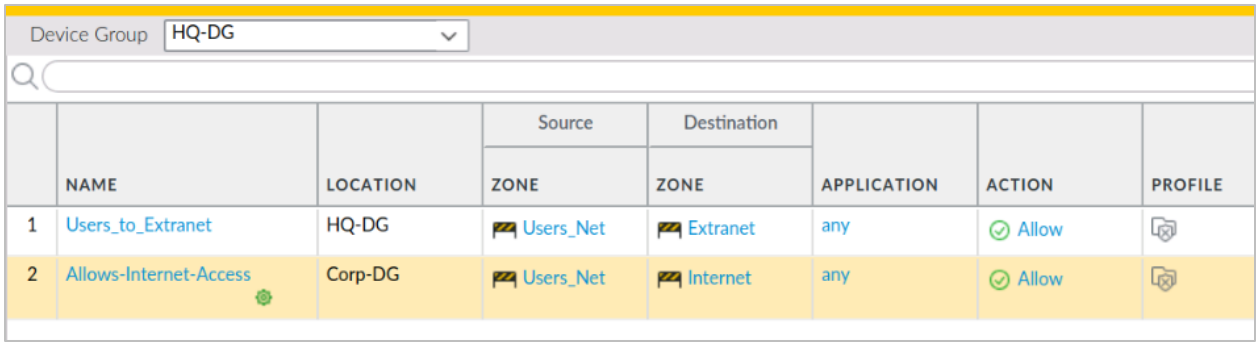


152. Click **Add** and enter the following values:

Parameter	Value
General tab	
Name	`Users_to_Extranet`
Description	`Allows Users_Net to Extranet.`
Source tab	
Source Zone	**Users_Net**
Destination tab	
Destination Zone	**Extranet**
Application tab	
Application	**Any**
Service/URL Category tab	
Service	**application-default**
Actions tab	
Actions	**Allow**
Profile Type	**Group**
Group Profile	**Corp-Profiles**

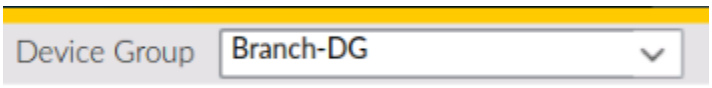
This security rule allows all applications and would not be appropriate for a production environment. You always should limit applications to only those that are necessary.

153. Click **OK**.
154. Note that you now have two Security policy rules listed in the **HQ-DG** Device Group:

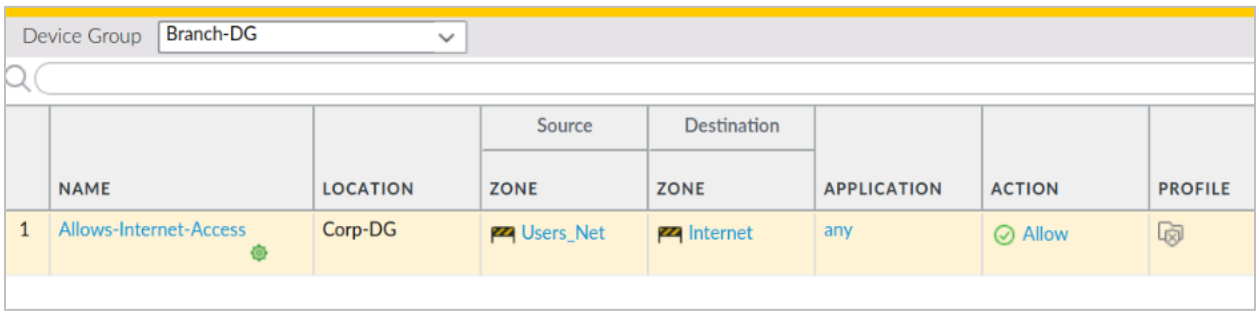


The Allow-Internet-Access rule was inherited from the Corp-DG Device Group.

155. Change the **Device Group** drop-down list to **`Branch-DG`**:



156. Note that you have only the **Allow-Internet-Access** rule that was inherited from the **Corp-DG** Device Group:



Create a Security Policy Rule for Extranet Traffic

The hosts in your Extranet security zone need access to the Internet. In this section, you will create a Security policy rule in the HQ-DG.

157. Select **Policies > Security > Post Rules**.
158. Select **HQ-DG** from the **Device Group** drop-down list:

159. Click **Add** and enter the following values:

Parameter	**Value**
General tab	
Name	**`Extranet_to_Internet`**
Description	**`Allows Extranet to Internet traffic.`**

Parameter	Value
Source tab	
Source Zone	**Extranet**
Destination tab	
Destination Zone	**Internet**
Application tab	
Application	**Any**
Service/URL Category tab	
Service	**application-default**
Actions tab	
Actions	**Allow**
Profile Type	**Group**
Group Profile	**Corp-Profiles**

This security rule allows all applications and would not be appropriate for a production environment. You always should limit applications to only those that are necessary.

160. Click **OK**.

Create a NAT Post-Rule for Users_Net Traffic

In this section, you will create a NAT rule that translates outbound traffic from the **Users_Net** zone to the **Internet** zone. The NAT rule will use the external interface address of the firewall as the translation source.

161. Select **Policies > NAT > Post Rules**.
162. Select **Corp-DG** from the **Device Group** drop-down list:

163. Click **Add** and enter the following values:

Parameter	Value
General tab	
Name	**NAT_Users_Net_to_Internet**

Parameter	Value
Description	`Translates traffic from Users_Net to Internet using e1/1 from firewall.`
NAT Type	**ipv4**
Original Packet tab	
Source Zone	**Users_Net**
Destination Zone	**Internet**
Translated Packet tab	
Source Address Translation Section	Set **Translation Type** to **Dynamic IP and Port**
Address Type	**Interface Address**
Interface	**ethernet1/1**
IP Type	**IP**
Field below IP Type	**$Internet-Interface**

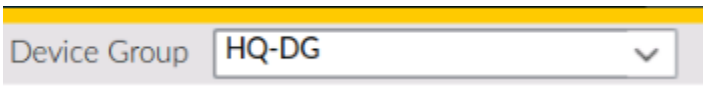
The variable $Internal-Interface will be resolved to 203.0.113.20/24 for the Chicago firewall and 203.0.113.25/24 for the Berlin firewall.

164. Click **OK**.

Create a NAT Post-Rule for Extranet Traffic

In this section, you will create a NAT rule that translates outbound traffic from the **Extranet** zone to the **Internet** zone. The NAT rule will use the external interface address of the firewall as the translation source. This rule is needed only in the **HQ-DG** Device Group.

165. Select **Policies** > **NAT** > **Post Rules**.
166. Select **HQ-DG** from the **Templates** drop-down list:



167. Click **Add** and enter the following values:

Parameter	Value
General tab	
Name	`NAT_Extranet_to_Internet`

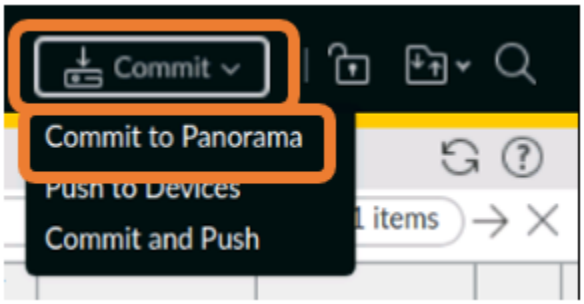
Parameter	Value
Description	`Translates traffic from Extranet to Internet using e1/1 from firewall.`
NAT Type	**ipv4**
Original Packet tab	
Source Zone	**Extranet**
Destination Zone	**Internet**
Translated Packet tab	
Source Address Translation Section	Set **Translation Type** to **Dynamic IP and Port**
Address Type	**Interface Address**
Interface	**ethernet1/1**
IP Type	**IP**
Field below IP Type	**$Internet-Interface**

The variable $Internet-Interface will be resolved to 203.0.113.20/24 for the Chicago firewall. This rule will not be pushed to the Berlin firewall, which is not in this Device Group.

168. Click **OK**.

Commit the Configuration to Panorama

169. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



170. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
171. Monitor the status of the commit.

172. When the commit status is complete, click **Close**.

Preview the Rules in Panorama

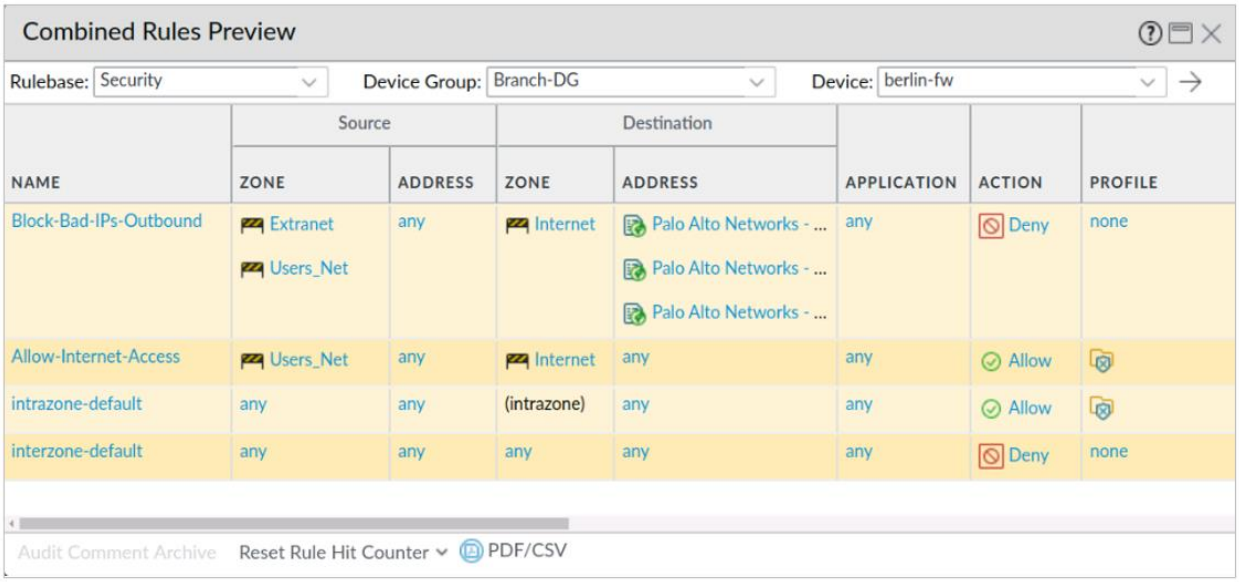
Panorama allows you to see what your rule sets will look like on managed firewalls before you push changes out through Device Groups. This feature lets you verify that the correct rules are in place and that the rules are in the correct order on a specific firewall.

In this section, you will examine the Security policy rules for both the berlin-fw and the chicago-fw before you push them down from Panorama.

173. In Panorama, select **Policies > Security > Pre Rules**.
174. At the bottom of the browser window, click **Preview Rules**:

175. In the **Combined Rules Preview** window, set the **Rulebase** drop-down list to **Security**.
176. Select **Branch-DG** from the **Device Group** drop-down list.
177. Select **berlin-fw** from the **Device** drop-down list.

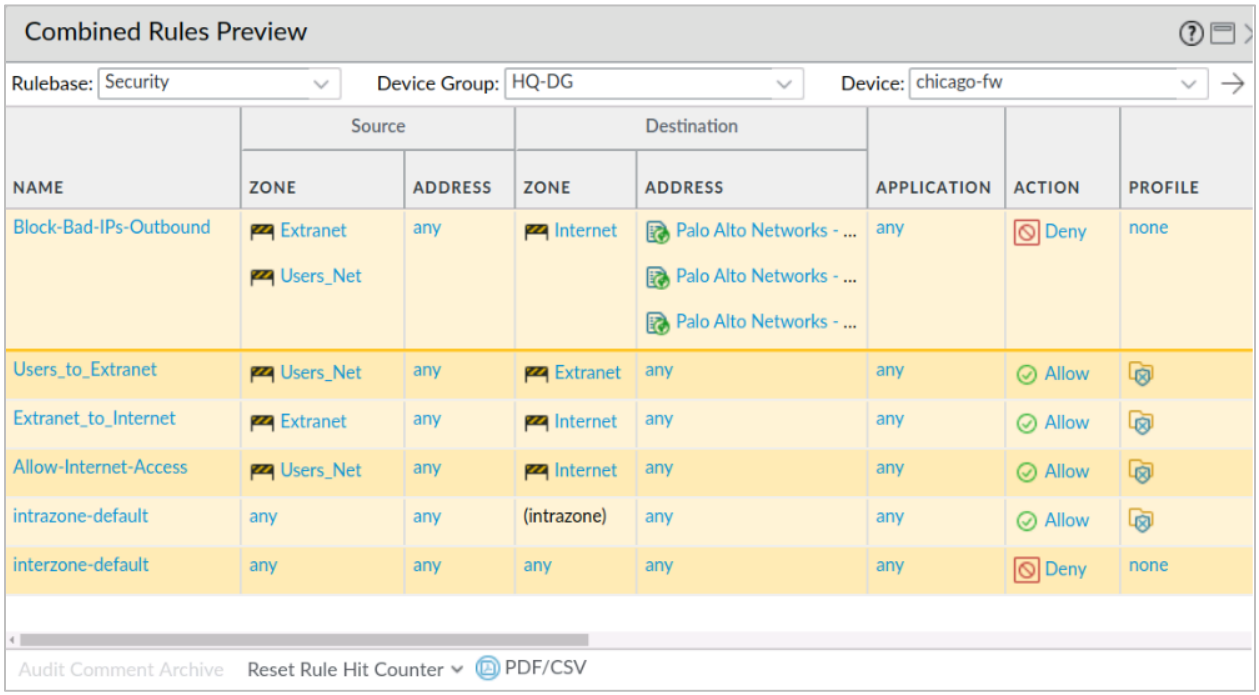
The berlin-fw value will be selected for you automatically because only one firewall is in the Branch-DG. If there are multiple firewalls in a Device Group, use the drop-down list for Device to select a specific one.



Some columns have been hidden in this example.

178. Note that this window shows you how the Security policy rules will appear on the berlin-fw after you have pushed them down from Panorama.

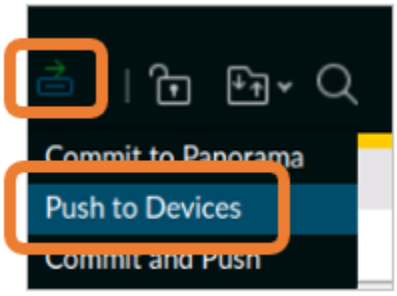
179. Change the **Device Group** to **HQ-DG**.
180. Select the **chicago-fw Device**:



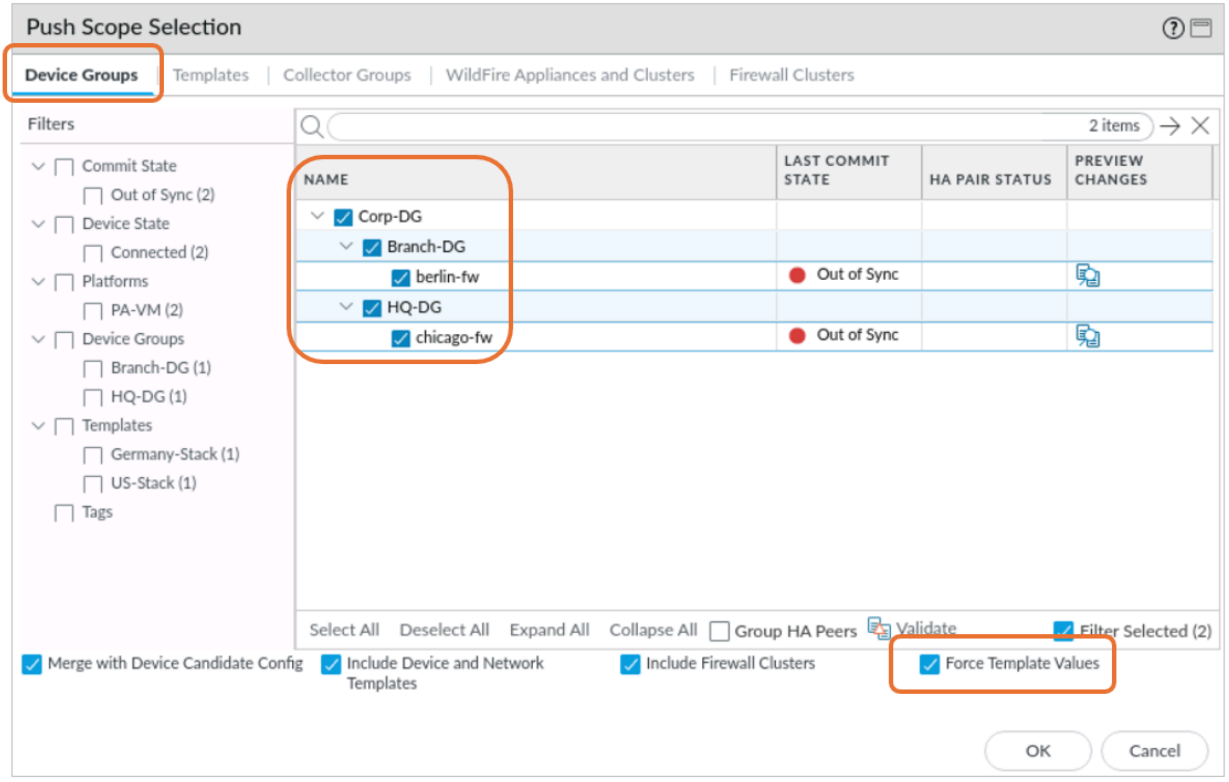
181. Close the **Combined Rules Preview** window.

Push the Configuration to the Firewalls

182. Select the **Commit** icon and choose **Push to Devices**:



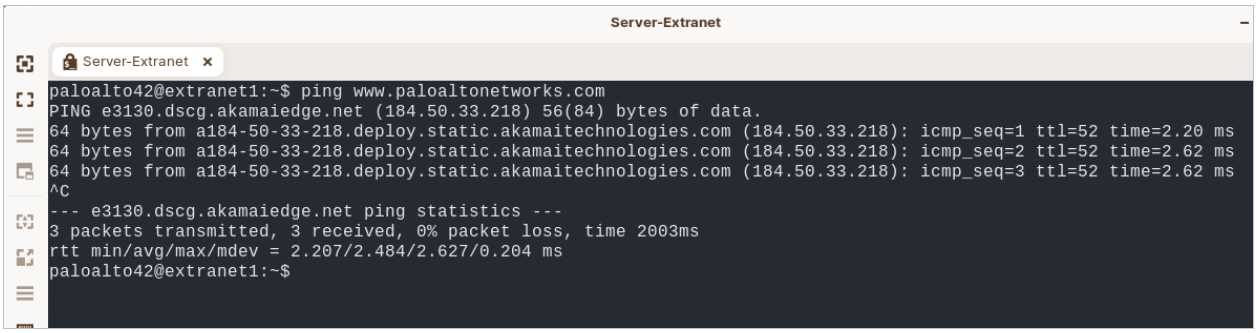
183. Click **Edit Selections**.
184. Select the **Device Groups** tab and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected.
185. Select the **Force Template Values** check box at the bottom.
186. Click **Yes** on the **Force Template Values** warning message:



187. On the **Templates** tab, check the boxes for the Chicago firewall and the Berlin firewall.
188. Click **OK**.
189. Click **Push** to start the process.
190. Wait until the **Commit All** jobs are complete.
191. Click **Close**.

Test Internet Access from User Hosts

192. From the client-A workstation, open the Testing web browser.
193. Browse to **`https://www.paloaltonetworks.com`** to verify that you have configured the chicago-fw correctly for access to the Internet security zone.
194. Open another tab in the Testing web browser and connect to **`http://www.panw.lab`** to verify that you have configured the chicago-fw correctly for access to hosts in the Extranet security zone.
195. Close the Testing browser on client-A.
196. On the client-A workstation, open Remmina using the icon on the Desktop.
197. Double-click the entry for **Server-Extranet** to connect to one of the servers using SSH in the Extranet zone.
198. From the command line on the server, ping **`www.paloaltonetworks.com`**:



The host www.paloaltonetworks.com may resolve to a different IP address than is shown in this example.

199. Press **Ctrl+C** to end the ping.
200. Type **`exit`** to close the Server-Extranet connection.
201. Use the Remmina Remote Desktop Client to log into the Berlin-Client workstation.
202. From the client-b workstation, ping **`www.paloaltonetworks.com`** to verify that you have configured the berlin-fw correctly for access to the Internet security zone.
203. Type **`exit`** to close the Remmina connection to the Berlin-Client.

    Note that the users in Berlin do not have direct access to hosts in the Extranet zone.

204. Close the Remmina Remote Desktop Client application window.

Confirm the Configurations on Each Firewall

From the client-A workstation, examine each firewall through its web interface using the Configuration browser.

205. In the Configuration browser, open a new tab and connect to the berlin-fw.
206. Open another new tab in the Configuration browser and connect to the chicago-fw.
207. In the web interface of each firewall, navigate to **Policies > Security**.

208. You will see the Security policy rules you created and pushed down from Panorama:

	NAME	Source ZONE	Destination ZONE	APPLICATION	ACTION	PROFILE
1	Block-Bad-IPs-Outbound	Extranet Users_Net	Internet	any	Deny	none
2	Users_to_Extranet	Users_Net	Extranet	any	Allow	
3	Extranet_to_Internet	Extranet	Internet	any	Allow	
4	Allow-Internet-Access	Users_Net	Internet	any	Allow	
5	intrazone-default	any	(intrazone)	any	Allow	
6	interzone-default	any	any	any	Deny	none

Chicago-FW Security Policy Rules

Note that some columns have been re-arranged and other columns have been hidden in the preceding example.

	NAME	Source ZONE	Destination ZONE	APPLICATION	ACTION	PROFILE
1	Block-Bad-IPs-Outbound	Extranet Users_Net	Internet	any	Deny	none
2	Allow-Internet-Access	Users_Net	Internet	any	Allow	
3	intrazone-default	any	(intrazone)	any	Allow	
4	interzone-default	any	any	any	Deny	none

Berlin-FW Security Policy Rules

Note that some columns have been rearranged and other columns have been hidden in the example above.

209. On each firewall, select **Policies > NAT**.

210. Both firewalls will have a NAT rule for **NAT_Users_Net_to_Internet**, but the Chicago firewall also will have a rule for **NAT_Extranet_To_Internet**:

	NAME	Original Packet		Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	NAT_Extranet_to_Internet	Extranet	Internet	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none
2	NAT_Users_Net_to_Internet	Users_Net	Internet	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none

211. **Chicago-FW NAT Policy Rule**

Note that some columns have been rearranged and other columns have been hidden in the example above.

	NAME	Original Packet		Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	NAT_Users_Net_to_Internet	Users_Net	Internet	dynamic-ip-and-port ethernet1/1 203.0.113.25/24	none

212. **Berlin-FW NAT Policy Rule**

Note that some columns have been rearranged and other columns have been hidden in the example above.

213. Close the Configuration browser tab for both firewalls but leave the tab open for Panorama.

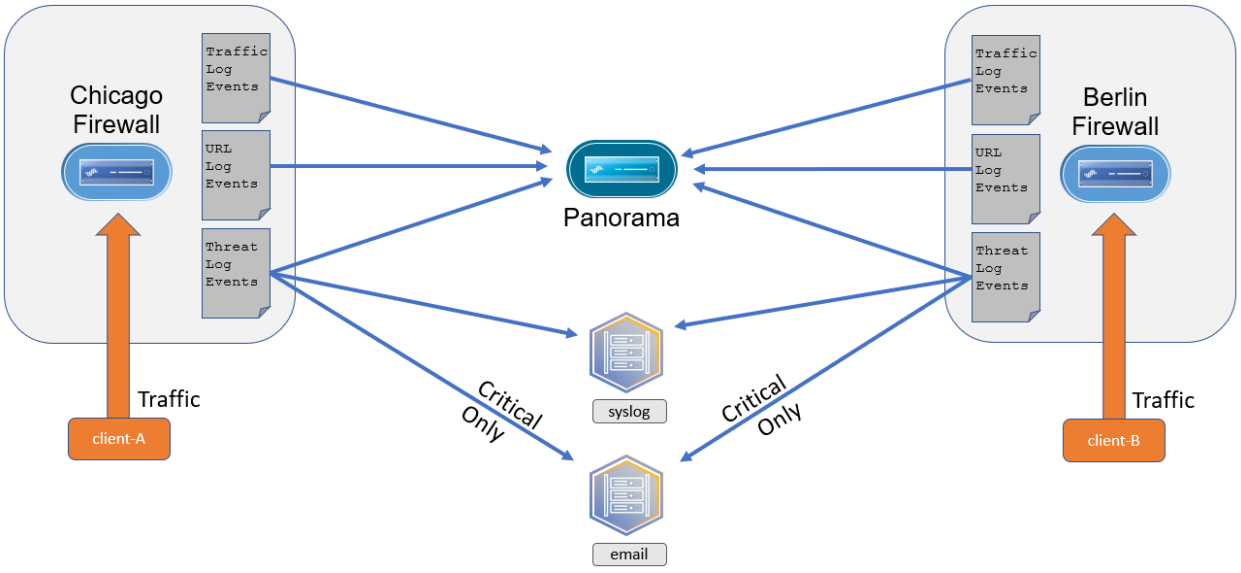
Stop. This is the end of the lab.

Lab 5 Scenario: Log Collection and Forwarding

In this section, you will use Panorama to configure both firewalls with **Log Forwarding profiles**.

You will configure both firewalls to send **Traffic**, **URL Filtering,** and **Threat** log events to Panorama so that you have an enterprise view of traffic in your organization.

Your organization uses a syslog server to collect important events from network hosts. You will configure both firewalls to send all **Threat** log events to your syslog server. You also want **email** notifications for **critical** Threat events sent from the firewalls to your administration team:



Lab Objectives

- Create a **`default`** Log Forwarding profile
- Modify security rules to use a **`default`** Log Forwarding profile
- Create a new Security policy rule to see effect of **`default`** Log Forwarding profile
- Create Panorama Server profiles
- Forward Panorama System and Config Log events
- Generate traffic and verify log forwarding

Note that the configuration you load in this lab has additional components, including a new zone and Security policy rules. These have been added for later tasks you will perform for logging and monitoring.

High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-5-Start.xml** configuration file on Panorama.

Push the Configuration to Firewalls

- Push the changes to the firewalls using **`Force Template Values`**

Create a Default Log Forwarding Profile

- Use the information below to create a Log Forwarding profile called **`default`** with five Profile Match List entries:

Parameter	Value
Log Forwarding Profile Name	`default`
Shared box	`Checked`
Description	`Standard Log Forwarding profile for all Security policy rules.`
Log Forwarding Profile Match List Entry 1	`Traffic-to-Panorama`
Description	`Sends all Traffic log file entries to Panorama`
Log Type	`Traffic`
Filter	`All Logs`
Forward Method	`Panorama/Cortex Data Lake`
Log Forwarding Profile Match List Entry 2	`URL-to-Panorama`
Description	`Sends all URL log entries to Panorama`
Log Type	`url`
Filter	`All Logs`
Forward Method	`Panorama/Cortex Data Lake`
Log Forwarding Profile Match List Entry 3	`Threat-to-Panorama-and-Syslog`
Description	`Sends all Threat log entries to both Panorama`

Parameter	Value
	and syslog.
Log Type	threat
Filter	All Logs
Forward Method	Panorama/Cortex Data Lake Syslog_Servers
Log Forwarding Profile Match List Entry 4	Wildfire-to-Panorama
Description	Sends all Wildfire log entries to Panorama
Log Type	wildfire
Filter	All Logs
Forward Method	Panorama/Cortex Data Lake
Log Forwarding Profile Match List Entry 5	Threat-critical-and-high-to-mail
Description	Sends email to paloalto42 for critical and high threat events
Log Type	threat
Filter	(severity eq critical) or (severity eq high)
Forward Method	Email_Servers

Modify Security Rules to Use the Default Log Forwarding Profile

- Modify the following Security Policy rules to use the **default** Log Forwarding Profile:
  - **Allow-Internet-Access**
  - **Users_to_Extranet**
  - **Extranet_to_Internet**
  - **Extranet_to_Users_Net**
  - **Danger_Traffic**

Create a New Security Policy Rule

- To see the effect of your default Log Forwarding Profile, create a new Security Policy Post Rule in the **Corp-DG** Device Group.
- Under the **Actions** tab, note that Panorama already applies the **default** Log Forwarding Profile for you when you create a new Security policy rule.

- Cancel the new rule.

Create Panorama Server Profiles

- Use the information below to create a Syslog Server Profile for Panorama:

Parameter	Value
Server Profile Name	`Panorama-Syslog`
Server Name	`US-Syslog-1`
Syslog Server	`192.168.50.55`

- Use the information below to create an Email Server Profile for Panorama:

Parameter	Value
Server Profile Name	`Panorama-Email`
Server Name	`US-Mail-1`
Email Display Name	`Panorama`
From	`panorama@panw.lab`
To	`paloalto42@panw.lab`
Email Gateway	`192.168.50.150`

Forward Panorama System Log Events to Syslog

- Use the information below to create an entry in the Configuration section of Panorama's Log Settings:

Parameter	Value
Name	`System-Logs-to-Syslog`
Filter	`All Logs`
Description	`Sends all system log events from Panorama to syslog`
Syslog Section	`Panorama-Syslog`

Forward Panorama Commit Log Events to Email

- Use the information below to create an entry in the Configuration section of Panorama's Log Settings:

Parameter	Value
Name	`Commit-to-Email`
Filter	`(cmd eq commit)`
Description	`Sends Panorama commit events to email`
Syslog Section	`Panorama-Email`

Commit the Configuration

- Commit the changes to Panorama and push the changes to the Devices.
    - You do not need to push any Template changes to the firewalls.

Verify Panorama Commit Email

- Modify the Panorama **Login Banner** to include the phrase **`Access attempts recorded.`**
- Commit the changes to Panorama.
- Log in to the **Lab Mail** account using the **`paloalto42/Pal0Alt0!`** Credentials.
- Verify that you have received an email about the Panorama Commit.

Generate Log Entries on Chicago Firewall

- Run the **`Log Testing`** script from the **/home/lab-user/Desktop/Class-Scripts/EDU-220/** folder on the client-A desktop.

Run the Traffic Script on the Berlin Firewall

- Use the Remmina application to connect to the Berlin-Client.
- Run the traffic generating script **`./b-logtesting.sh`** from the **/home/lab-user/Desktop/Lab-Files/EDU-220/**

Verify That Firewalls Forward Traffic Logs Events to Panorama

- Examine the Traffic log entries for the Corp-DG Group to verify that Panorama is receiving information from both the chicago-fw and the berlin-fw.
- Change the Traffic log to display entries from the HQ-DG Device Group and verify that you see only entries from the chicago-fw.
- Change the Traffic log to display entries from the Branch-DG Device Group and verify that you see only entries from the berlin-fw.

Verify That Firewalls Forward Threat Events to Panorama

- Examine the Threat log entries for the Corp-DG Group to verify that Panorama is receiving information from both the chicago-fw and the berlin-fw.
- Modify the Threat log columns to display only the following: Generate Time, Type, Threat ID/Name, From Zone, To Zone, Source Address, Source User, Destination Address, To Port, Application, Action, Severity, File Name, URL, and Device Name.
- Move the Device Name column to the far left side of the table.
- Move the Severity column next to the Device Name column.

Verify That Firewalls Forward URL Filtering Logs to Panorama

- Examine the URL Filtering log entries for the Corp-DG Group to verify that Panorama is receiving information from both the chicago-fw and the berlin-fw.
- Modify the Threat log columns to display only the following: Generate Time, URL Category List, URL, From Zone, To Zone, Source, Source User, Destination, Application, Action, Device Name.
- Move the Device Name column to the far left side of the table.
- Move the Action column next to the Device Name column.

Verify Threat Email from Firewalls

- Log in to the Lab Email server with the **`paloalto42/Pal0Alt0!`** credentials.
- Note emails from Chicago and Berlin firewalls about threats.
- Open any THREAT ALERT email to see details.

Detailed Lab Steps

Load the Lab Start Configuration File

1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-5-Start.xml**.
4. Leave the remaining settings unchanged.
5. Click **OK** to close the **Load Named Configuration** window.
6. Click **Close** on the **Loading Configuration** window.
7. Commit the changes to Panorama by selecting the **Commit** > **Commit to Panorama** in the upper-right corner of the window.
8. In the **Commit to Panorama** window, click **Commit**.
9. Allow the process to complete.
10. Click **Close** in the **Commit Status** window.

Push the Configuration to Firewalls

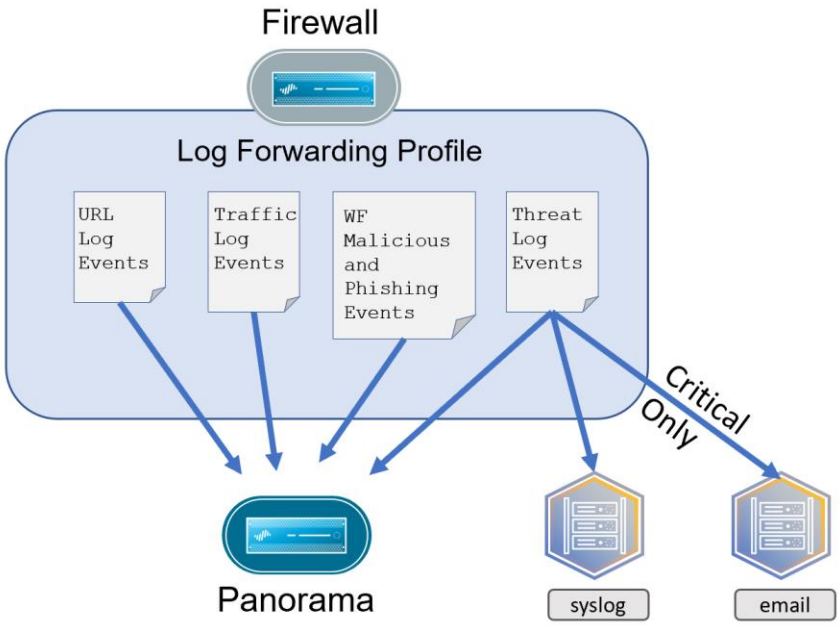
11. Select **Commit** > **Push to Devices**.
12. Click **Edit Selections**.
13. Select the **Device Groups** tab and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected.
14. Select the **Force Template Values** check box at the bottom.
15. Click **Yes** on the **Force Template Values** warning message.
16. On the **Templates** tab, verify that the check boxes for the Chicago firewall and the Berlin firewall are selected.
17. Click **OK**.
18. Click **Push** to start the process.
19. Wait until the **Commit All** jobs are complete.
20. Click **Close**.

Create a Default Log Forwarding Profile

You want all firewalls in your organization to send copies of their log file entries to Panorama. In this section, you will create a **Log Forwarding Profiles** called **`default`**. You will create the profile in the Shared Device Group so that it is available in all descendant Device Groups.

You will define rules in the Log Forwarding Profile to send log file entries from the firewalls to Panorama. You will include rules for Traffic, URL Filtering, Threat, and WildFire® log entries.

You also will define rules that send all Threat log events to your syslog server and only critical Threat log events to email:



You will use the name **default** for this Log Forwarding Profile so that Panorama automatically assigns this Log Forwarding Profile to any new Security policy rule you create.

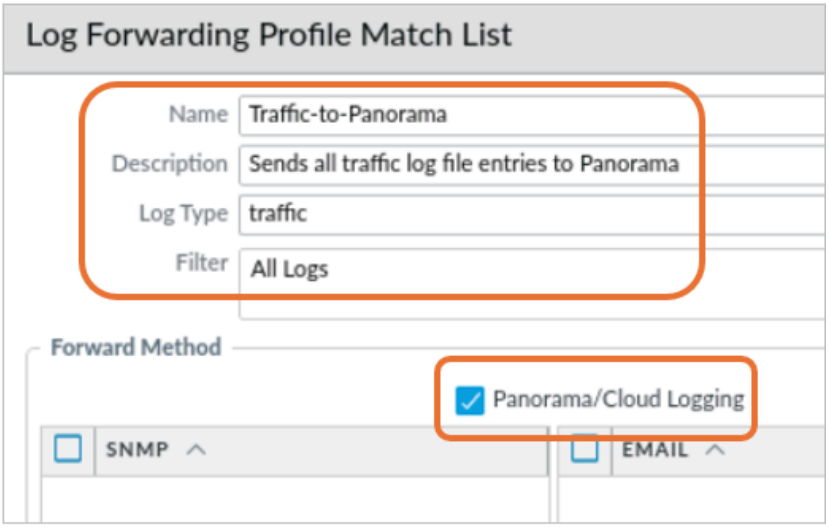
21. Select **Objects > Log Forwarding**.
22. Verify that you have the **Corp-DG** Device Group selected in the **Device Group** drop-down list near the top of the window:

23. Click **Add**.
24. For **Name**, enter **`default`**.

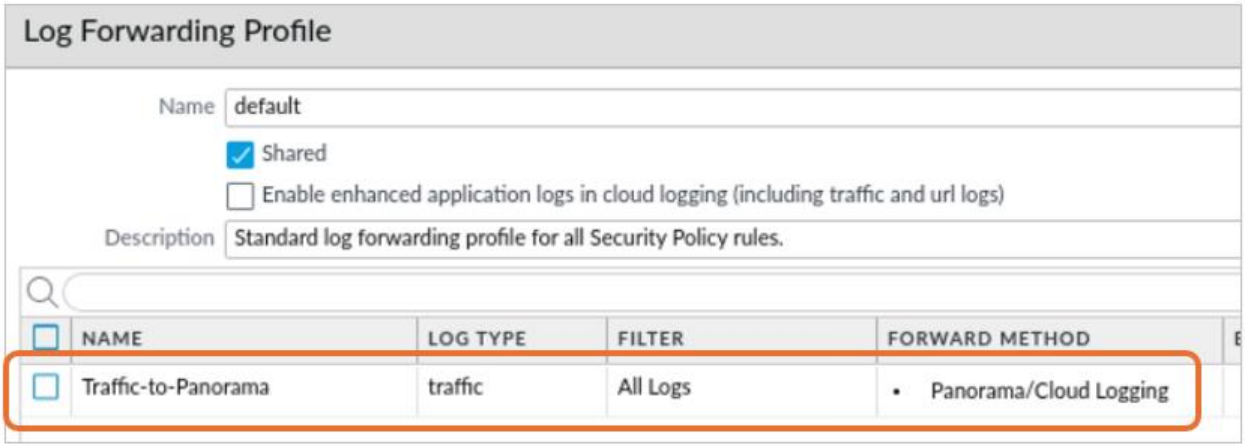
    Note that **default** should be in lowercase letters.
25. Place a **check mark** in the **box** for **Shared**.

    Remember that entries placed into the Shared Group will appear in all Device Groups.
26. For **Description**, enter **`Standard log forwarding profile for all Security Policy rules.`**
27. In the Log Forwarding Profile window, click **Add** in the bottom-left corner.
28. Panorama opens a new window titled **Log Forwarding Profile Match List**.
29. For **Name**, enter **`Traffic-to-Panorama`**.
30. For **Description**, enter **`Sends all traffic log file entries to Panorama`**.
31. Select **traffic** From the **Log Type** drop-down list.

32. Leave the **Filter** set to **All Logs**.
33. Place a **check mark** in the **box** for **Panorama/Cloud Logging**.
34. Leave the remaining settings unchanged:

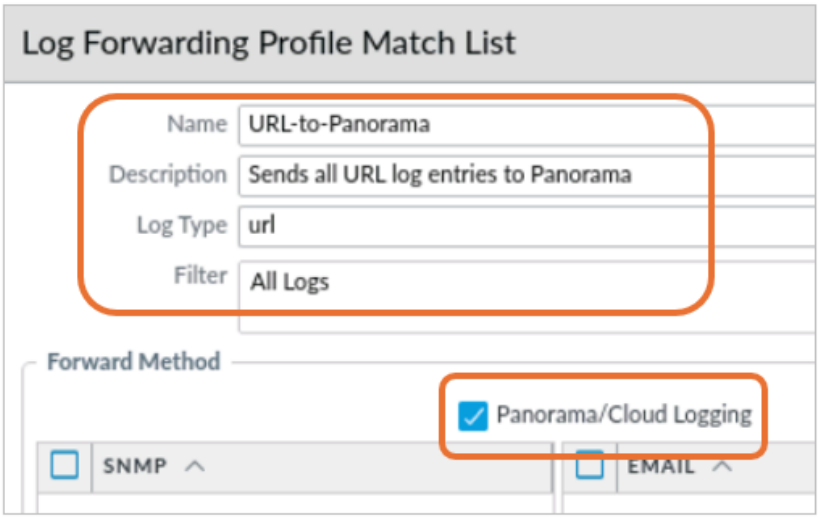


35. Click **OK** to return to the **Log Forwarding Profile** window.
36. Your **default** Log Forwarding Profile now has one entry called **Traffic-to-Panorama**:

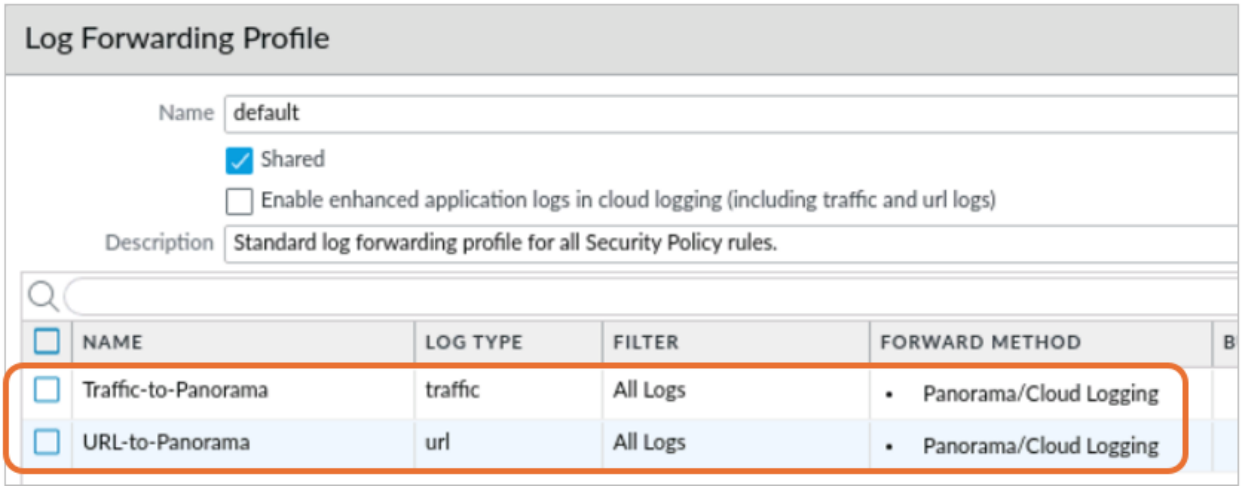


37. In the **Log Forwarding Profile** window, click **Add** again.
38. For **Name**, enter **`URL-to-Panorama`**.
39. For **Description**, enter **`Sends all URL log entries to Panorama`**.
40. For **Log Type**, select **url**.
41. Leave the **Filter** set to **All Logs**.
42. Place a check in the box for **Panorama/ Cloud Logging**.

43. Leave the remaining settings unchanged:

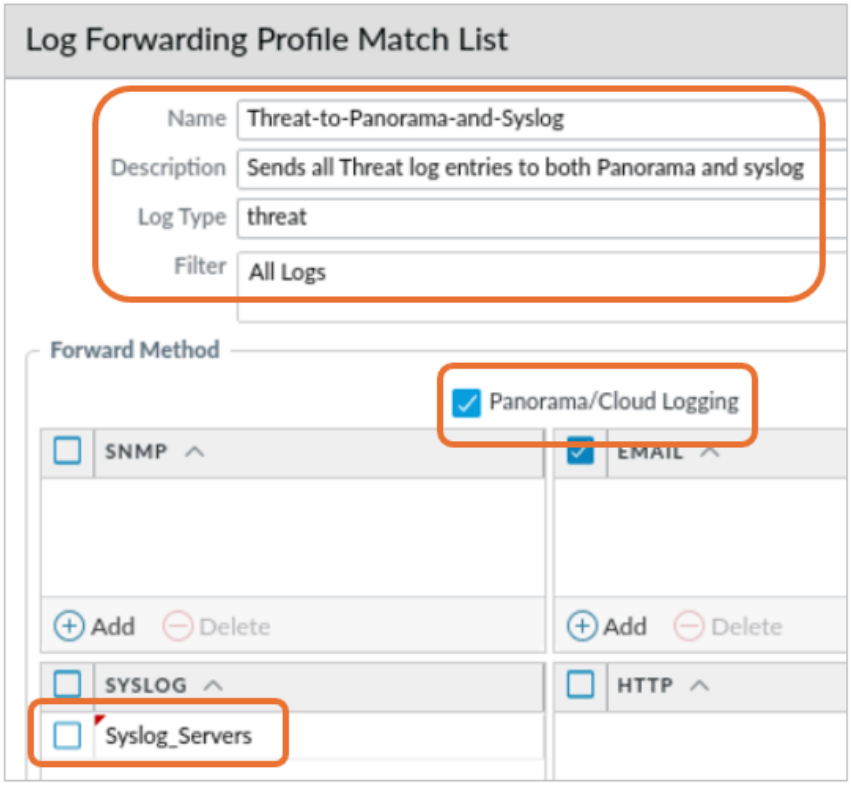


44. Click **OK** to return to the **Log Forwarding Profile** window.
45. Your **default** Log Forwarding Profile now has two entries:

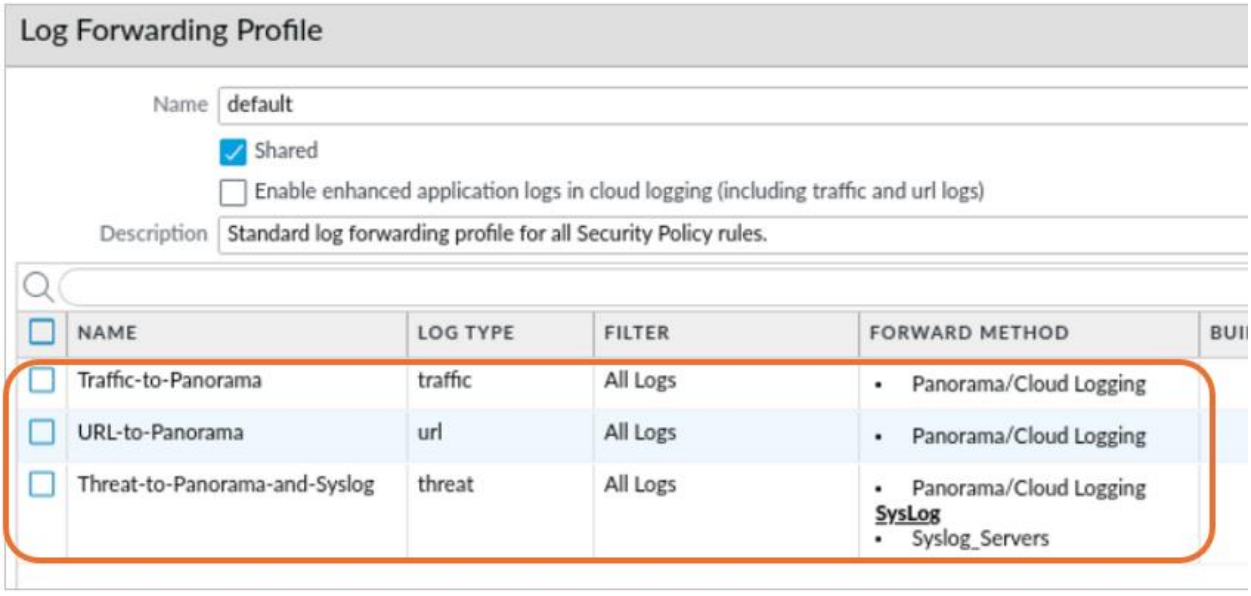


46. In the **Log Forwarding Profile** window, click **Add** again.
47. For **Name**, enter **`Threat-to-Panorama-and-Syslog`**.
48. For **Description**, enter **`Sends all Threat log entries to both Panorama and syslog`**.
49. For **Log Type**, select **threat**.
50. Leave the **Filter** set to **All Logs**.
51. Place a **check mark** in the **box** for **Panorama/Cloud Logging**
52. In the **Forward Method** area, beneath the **Syslog** section, click **Add**.
53. Select **Syslog_Servers**.

54. Leave the remaining settings unchanged:

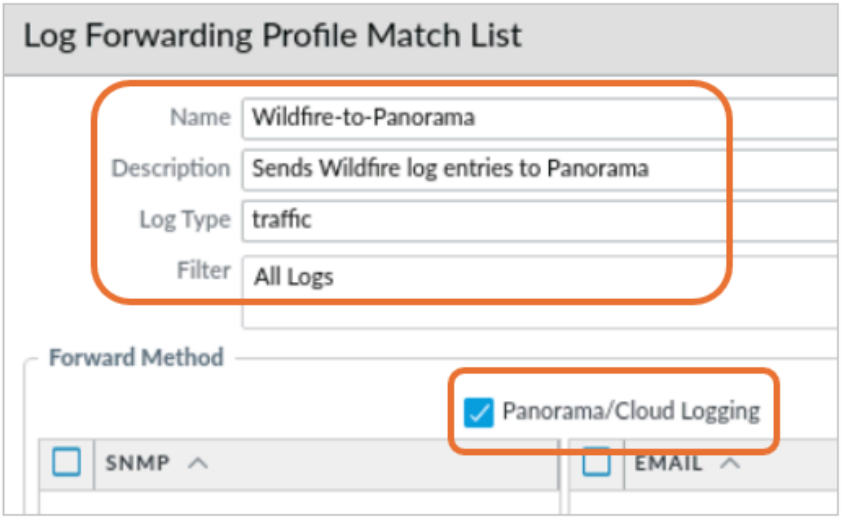


55. Click **OK** to return to the **Log Forwarding Profile** window.
56. Your **default** Log Forwarding Profile now has three entries:

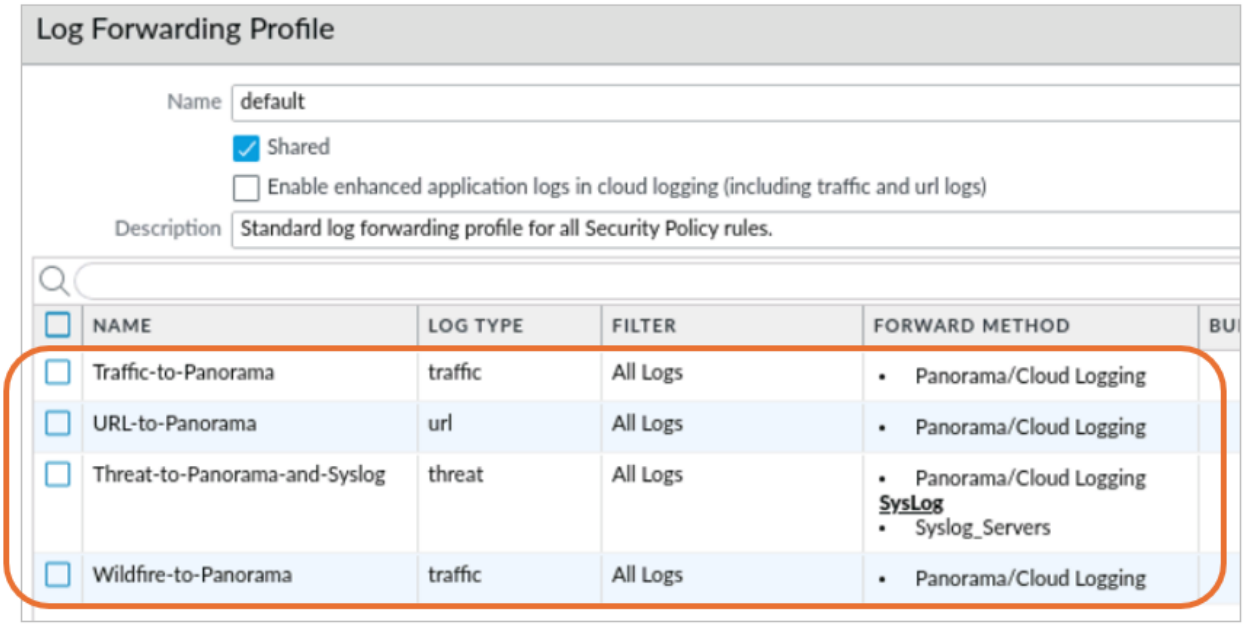


57. In the **Log Forwarding Profile** window, click **Add** again.
58. For **Name**, enter **`Wildfire-to-Panorama`**.

59. For **Description**, enter **`Sends Wildfire log entries to Panorama.`**
60. For **Log Type**, select **wildfire**.
61. Leave the **Filter** set to **All Logs**.
62. Place a **check mark** in the **box** for **Panorama/Cloud Logging**.
63. Leave the remaining settings unchanged:

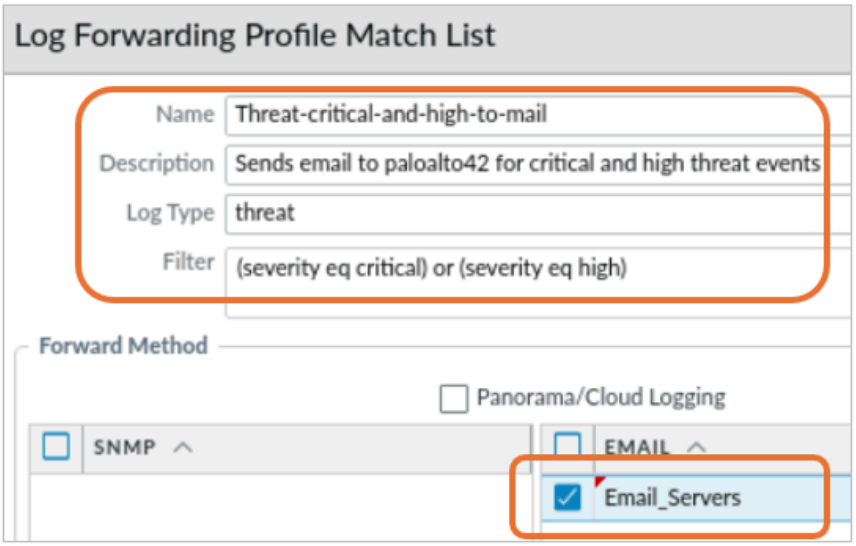


64. Click **OK** to return to the **Log Forwarding Profile** window.
65. You now have four entries in the **default** Log Forwarding Profile window:



Note that you may need to expand the size of the Log Forwarding Profile window to see all four entries.

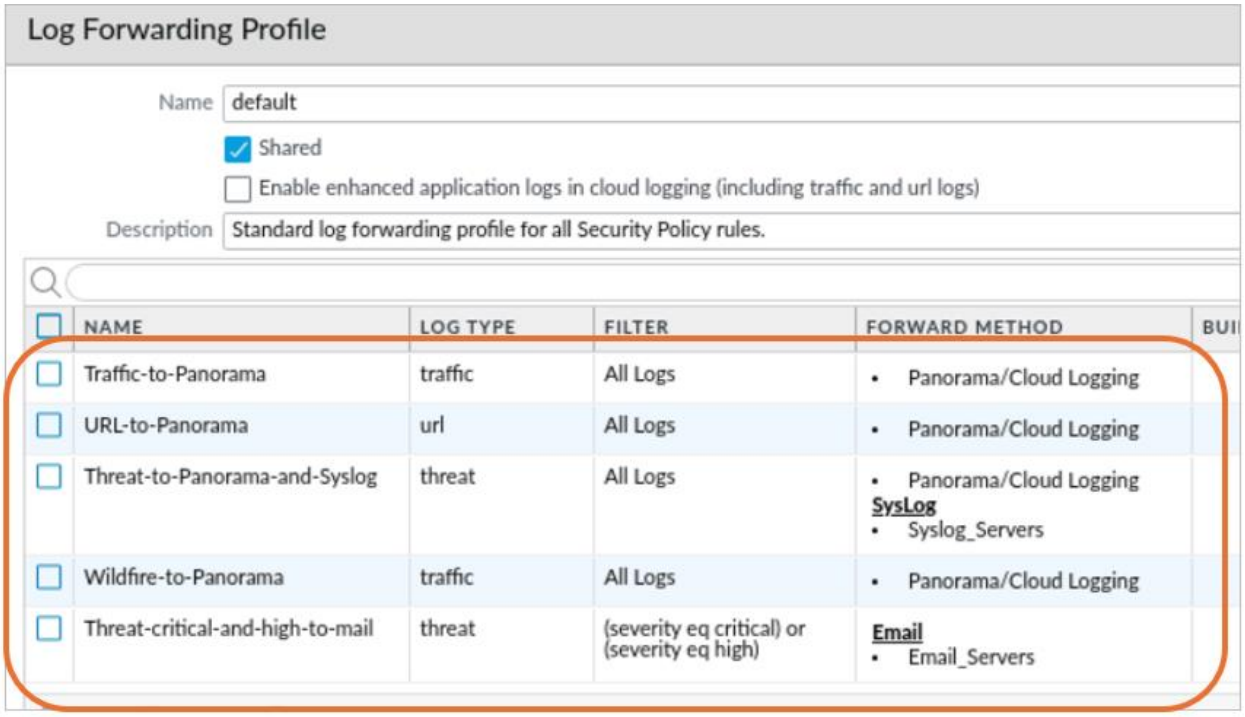
66. In the default **Log Forwarding Profile** window, click **Add**.
67. For **Name**, enter **`Threat-critical-and-high-to-mail`**.
68. For **Description**, enter **`Sends email to paloalto42 for critical and high threat events`**.
69. For **Log Type**, select **threat**.
70. For **Filter**, enter **`(severity eq critical) or (severity eq high)`**
71. In the **Forward Method** area, under the **Email** section, click **Add**.
72. Select **Email_Servers**:



Note: For this entry, you have not selected the box for Panorama/Cloud Logging. You already have an entry in this default Log Forwarding Profile that sends all Threat log events to Panorama. A check mark in the Panorama/ Cloud Logging box in this entry would be redundant.

73. Click **OK** to return to the **Log Forwarding Profile** window.

74. You now have five entries in the **default Log Forwarding Profile** window:



75. Take a moment to examine the entries in this default Log Forwarding Profile.

Each line is a rule that tells the firewall what to do for entries in specific log files. In this example, the profile tells the firewall to send copies of all Traffic, URL, Threat, and WildFire log entries to Panorama.

The profile also tells the firewall to send copies of the Threat log entries to your syslog servers.

The last entry in the list tells the firewall to send an email notification (with a copy of the log file entry) to an email address when the firewall encounters a Threat with a critical or high severity level.

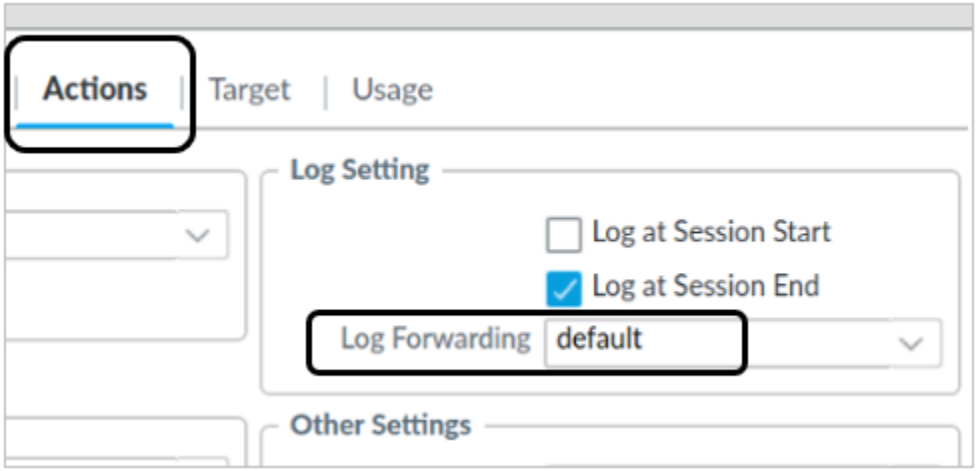
76. Click **OK** to close the **default Log Forwarding Profile**.

Modify Security Rules to Use the Default Log Forwarding Profile

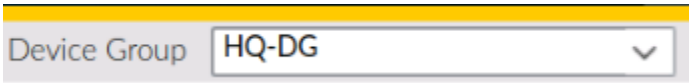
Whenever you create a new Security policy rule, Panorama automatically will apply the **default** Log Forwarding Profile. However, you need to modify existing Security policy rules to apply the **default** Log Forwarding Profile.

77. In Panorama, navigate to **Policies** > **Security** > **Post Rules**.
78. Select **Corp-DG** from the **Device Group** drop-down list:

79. Click the entry for **Allow-Internet-Access** to edit the rule.
80. Select the **Actions** tab.
81. Under the **Log Setting** section, change the drop-down list for **Log Forwarding** to **default**.
82. Leave the remaining settings unchanged:



83. Click **OK** to close the rule.
84. Select **HQ-DG** from the **Device Group** drop-down list:



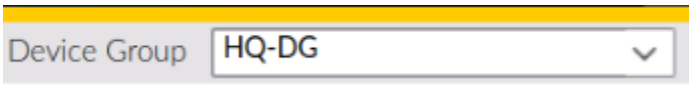
85. Edit the **Users_to_Extranet** rule and select the **Actions** tab.
86. Change the **Log Forwarding** drop-down list to **default**.
87. Leave the other settings unchanged.
88. Click **OK**.
89. Edit the **Extranet_to_Internet** rule and select the **Actions** tab.
90. Change the **Log Forwarding** drop-down list to **default**.
91. Leave the other settings unchanged.
92. Click **OK**.
93. Edit the **Extranet_to_Users_Net** rule and select the **Actions** tab.
94. Change the **Log Forwarding** drop-down list to **default**.
95. Leave the other settings unchanged:
96. Click **OK**.
97. Edit the **Danger_Traffic** rule and select the **Actions** tab.
98. Change the **Log Forwarding** drop-down list to **default**.

99. Leave the other settings unchanged.
100. Click **OK**.

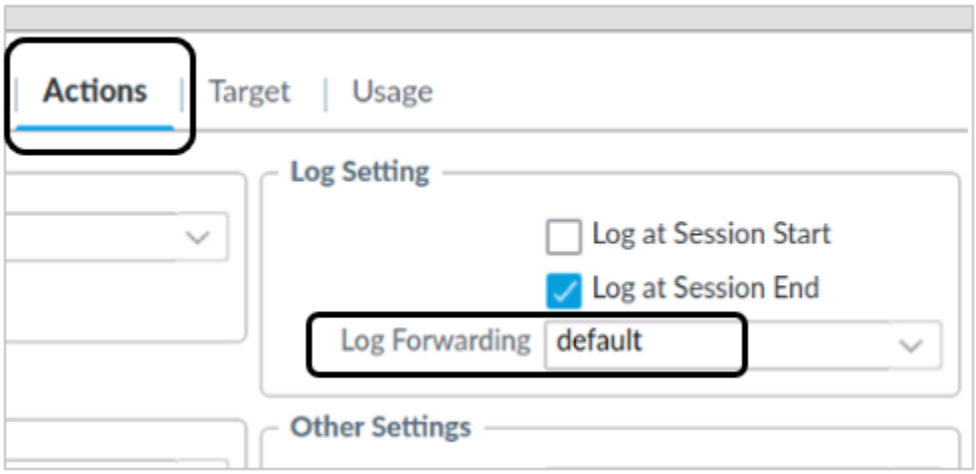
Create a New Security Policy Rule

To see the effect of your **`default`** Log Forwarding Profile, create a new Security policy rule.

101. Select **HQ-DG** from the **Device Group** drop-down list at the top:



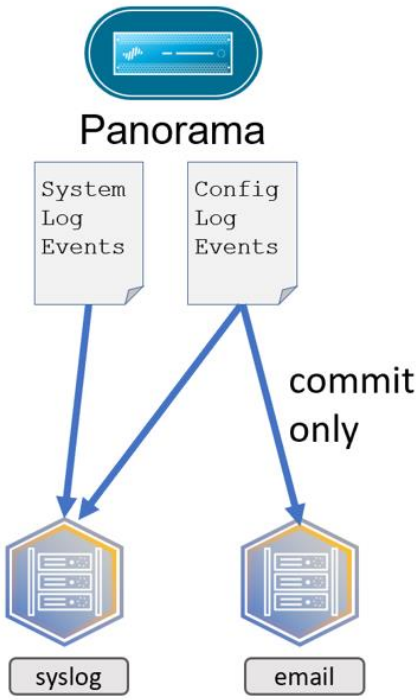
102. Select **Policies** > **Security** > **Post Rules**.
103. Click **Add**.
104. Select the **Actions** tab.
105. Note that Panorama has already applied the **default Log Forwarding Profile** for you when you create a new Security policy rule:



106. You do not need to complete the process of creating a new rule, so click **Cancel**.
107. Commit your changes to Panorama.

Create Panorama Server Profiles

To monitor Panorama itself, you want all Panorama system log events sent to your syslog server. You also want Panorama to send any configuration log events that include the **`commit`** command to your email address:

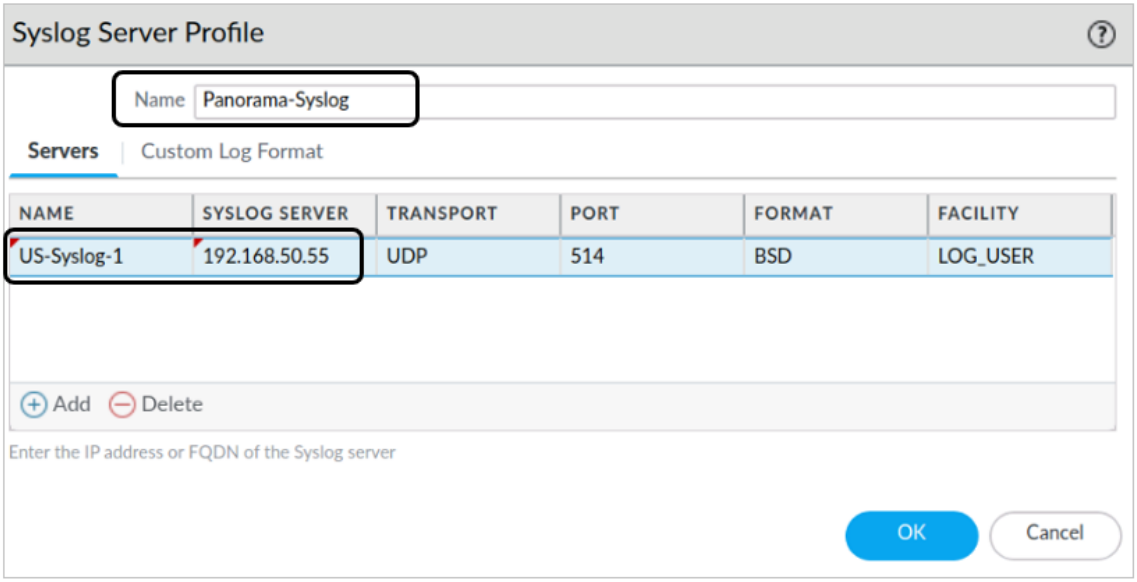


To accomplish this task, you must first define a Syslog Server Profile and an Email Server profile specifically for Panorama.

You might wonder why you cannot simply use the Syslog and Email Server Profiles that you defined for use in your Firewall Log Profiles. You can use the same server information, but Panorama needs its own separate set of server profiles for logging purposes.

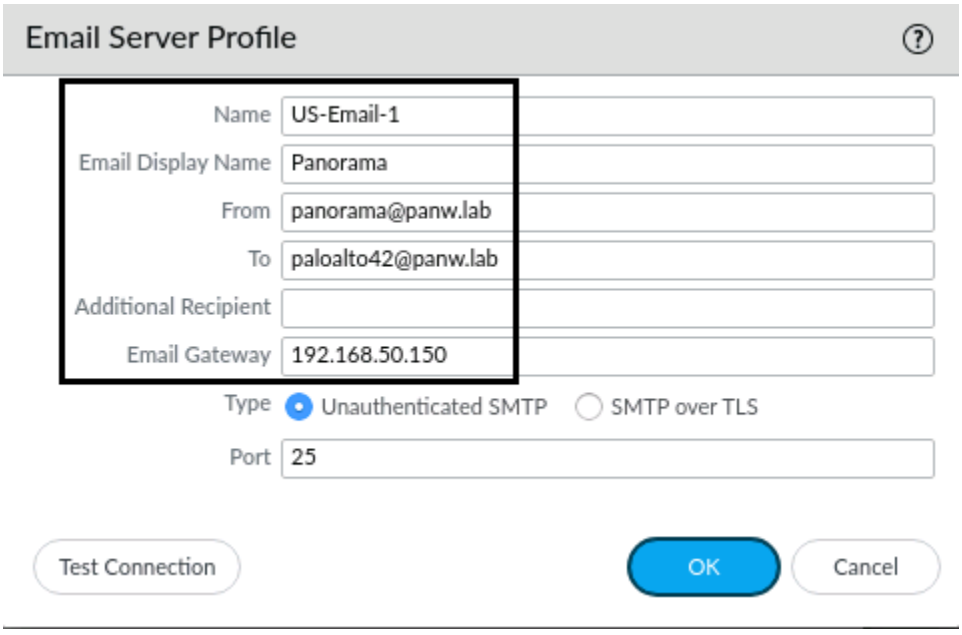
108. Create the Syslog Server Profile for Panorama to use by selecting **Panorama** > **Server Profiles** > **Syslog**.
109. Click **Add**.
110. For **Name**, enter **`Panorama-Syslog`**.
111. Under the **Servers** tab, click **Add**.
112. For **Name**, enter **`US-Syslog-1`**.
113. For **Syslog Server**, enter **`192.168.50.55`**.

114. Leave the remaining settings unchanged:

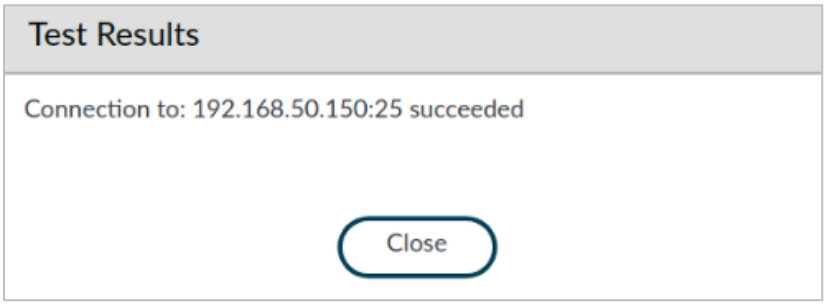


115. Click **OK**.
116. Create the Email Server Profile for Panorama to use by selecting **Panorama** > **Server Profiles** > **Email**.
117. Click **Add**.
118. For **Name**, enter **`Panorama-Email`**.
119. Leave the **Location** set to **Panorama**.
120. Under the **Servers** tab, click **Add**.
121. For **Name**, enter **`US-Email-1`**.
122. For **Email Display Name**, enter **`Panorama`**.
123. For **From**, enter **`panorama@panw.lab`**
124. For **To**, enter **`paloalto42@panw.lab`**
125. For **Email Gateway**, enter **`192.168.50.150`**

126. Leave the remaining settings unchanged:



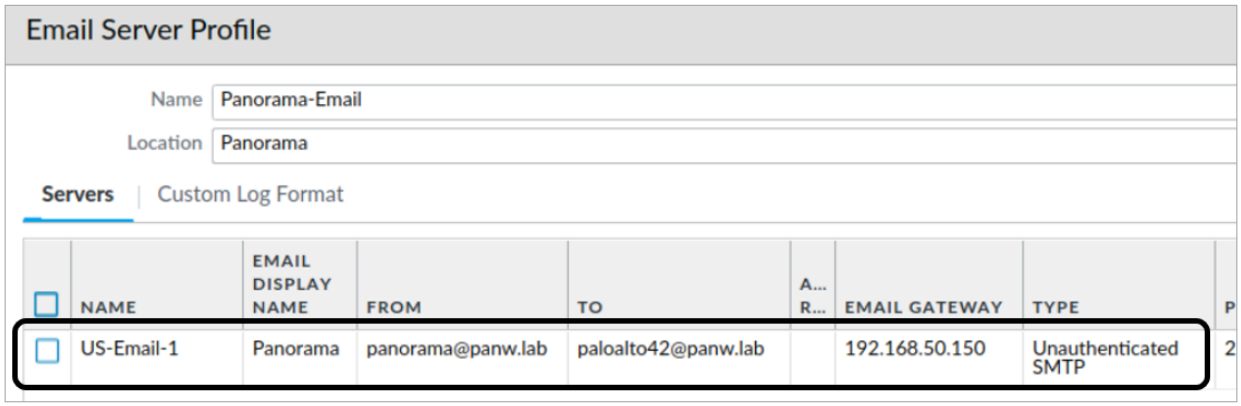
127. Click the **Test Connection** button.
128. You should receive a message indicating that the test has succeeded:



If the test does not succeed, verify the settings for your Email Server Profile and try again.

129. Click **Close** on the **Test Results** window.
130. Click **OK**.

131. Your **Email Server Profile** will have a new entry:

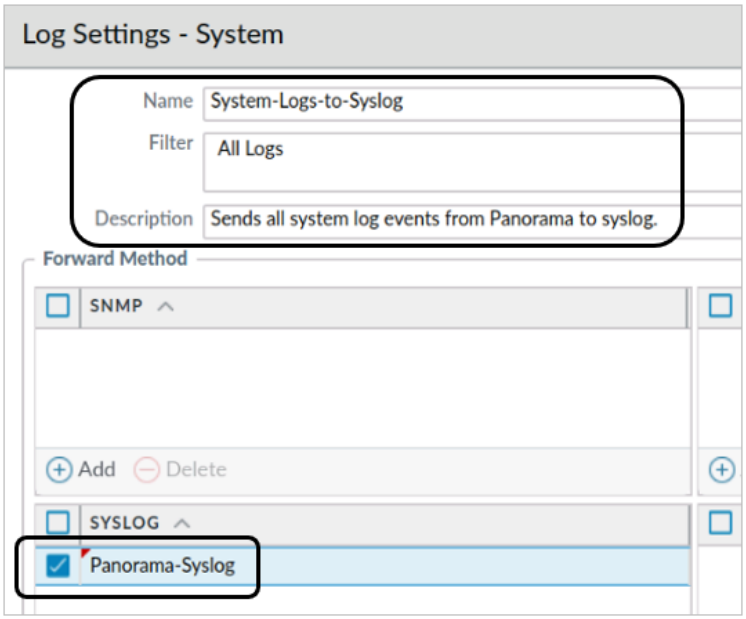


132. Click **OK** to close the **Email Server Profile** window.

Forward Panorama System Log Events to Syslog

You now will configure Panorama to send all System log events to your syslog server.

133. Navigate to **Panorama > Log Settings**.
134. Under the **System** section, click **Add**.
135. For **Name**, enter **`System-Logs-to-Syslog`**.
136. Leave the **Filter** set to **All Logs**.
137. For **Description**, enter **`Sends all system log events from Panorama to syslog`**.
138. Under the **Syslog** section, click **Add** and select **Panorama-Syslog**.
139. Leave the remaining settings unchanged:

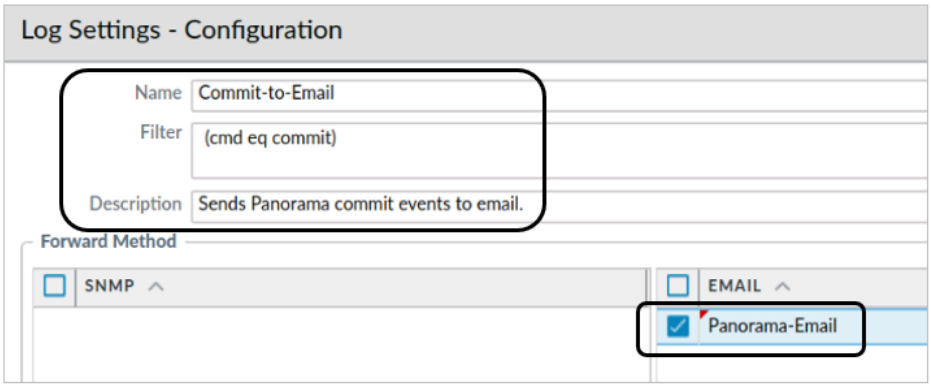


140. Click **OK**.

Forward Panorama Commit Log Events to Email

With your Email Server Profile in place, you can configure Panorama to send **commit** events from the Configuration log to your email.

141. Under **Panorama** > **Log Settings**, locate the **Configuration** section.
142. Click **Add**.
143. For **Name**, enter **`Commit-to-Email`**.
144. Enter **`(cmd eq commit)`** in the **Filter** field.
145. For **Description**, enter **`Sends Panorama commit events to email`**.
146. Under the **Email** section, click **Add** and select **Panorama-Email**.
147. Leave the remaining settings unchanged:



The Filter instructs Panorama to send only Configuration log file events that contain the command **commit**. You can use the Filter Builder to construct more complex filters. We will examine the Filter Builder later in the labs.

148. Click **OK**.

Commit the Configuration

149. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
150. When the **Commit to Panorama** window appears, leave the settings unchanged and click **Commit**.
151. Monitor the status of the commit.
152. When the commit status is complete, click **Close**.
153. Select the **commit** icon and choose **Push to Devices**.
154. Click **Edit Selections**.

155. Select the **Device Groups** tab and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected.
156.

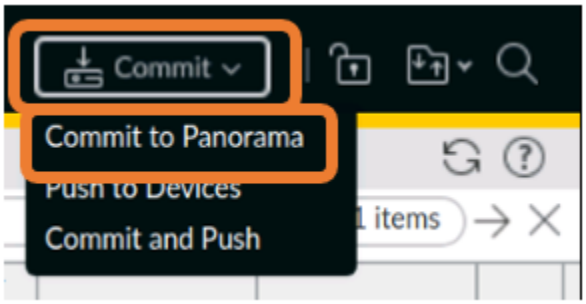
For this exercise, you do not need to use the Force Template Values or to select either firewall from the Templates tab. We have only made changes to the Device Groups.

157. Click **OK**.
158. Click **Push** to start the process.
159. Wait until the **Commit All** jobs are complete.
160. Click **Close**.

Verify Panorama Commit Email

In this section, you will make a minor change to the Panorama configuration and commit the change. This action will trigger an email from Panorama to the mail server.

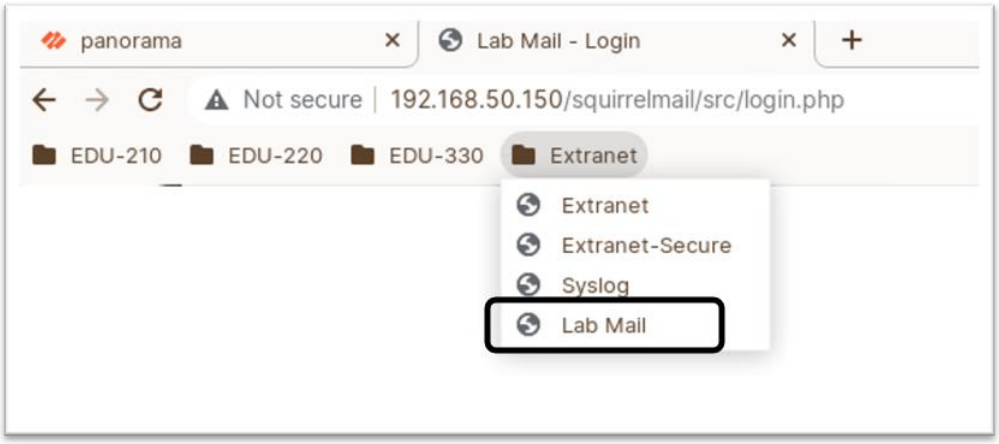
161. In Panorama, navigate to **Panorama** > **Setup** > **Management** and edit the **General Settings** section.
162. Add the following line to the **Login Banner**:
     `Access attempts recorded.`
163. Leave the remaining settings unchanged.
164. Click **OK**.
165. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



166. Click **Commit**.
167. Monitor the status of the commit.
168. When the commit status is complete, click **Close**.

Note that we are sending only changes to Panorama, so we do not need to push any changes to the managed firewalls.

169. Open a new browser tab in the Configuration browser.
170. From the Bookmark bar, select **Extranet > Lab Mail**:

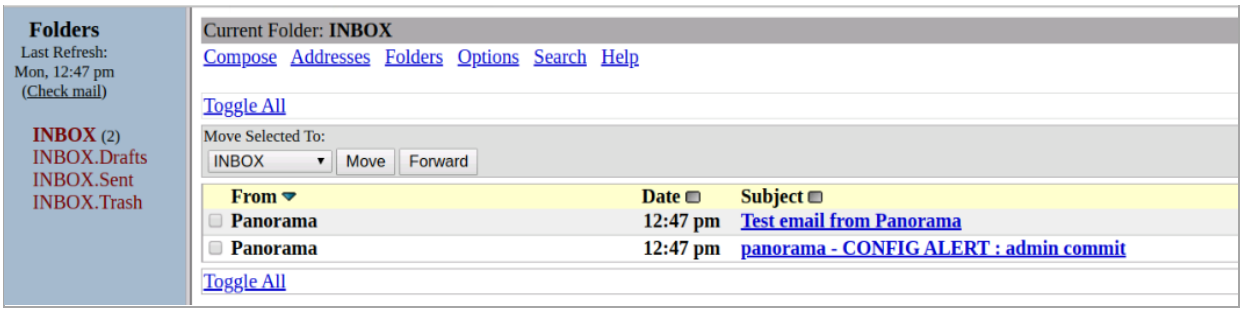


171. Use **`paloalto42`** for **Name.**
172. Enter **`Pal0Alt0!`** for **Password**.
173. Click **Login**:

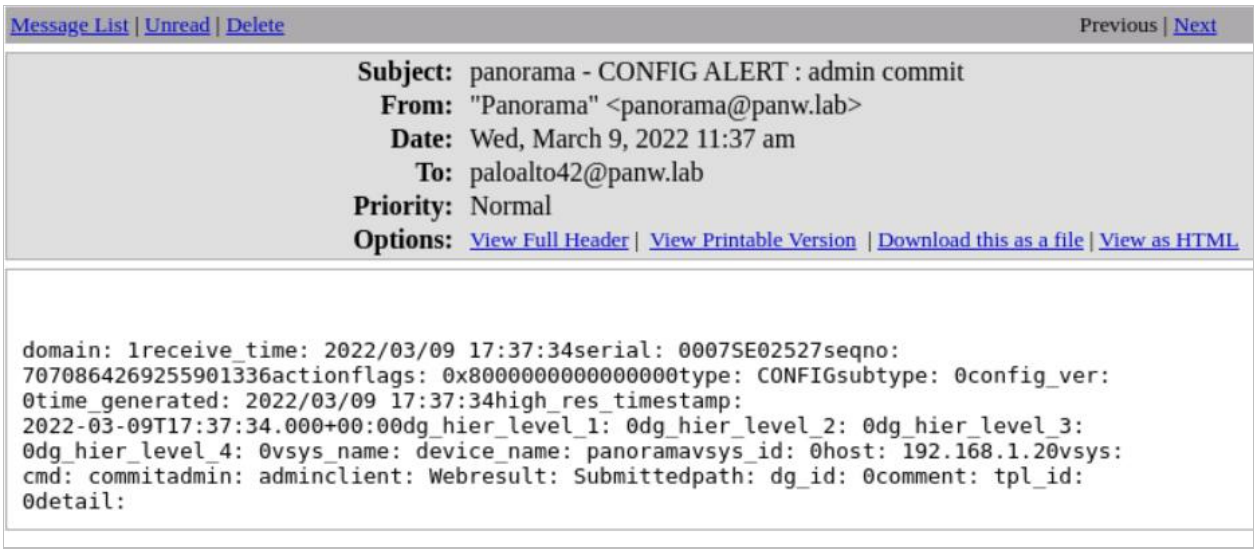
174. You should have at least two emails from Panorama in the **Inbox**.

One email was the test you sent from Panorama to verify mail connectivity. The other email is a notification about a Commit.

175. Click the **Inbox** link on the left:



176. Open the **panorama-CONFIG ALERT** email to see details about the event:



> Note that the date and time stamps for the message you see will differ from the example shown here.

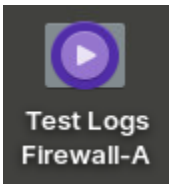
177. Click **Sign Out** in the upper-right corner of the email web interface.
178. Close the **Lab Mail** browser tab.

This exercise is simply an example of how to configure Panorama to send you email notifications for event types.

Generate Log Entries on Chicago Firewall

With your Log Forwarding Profiles in place, you now will run several scripts to generate traffic through the Chicago firewall. This process will allow you to verify that the firewalls and Panorama are forwarding log file entries correctly.

179. On the client-A workstation, double-click the icon for **Test Logs Firewall-A** to launch the script in a Terminal window:



180. Wait until you see that the script has completed before proceeding:

```
################################

Log entry generation complete.

################################
```

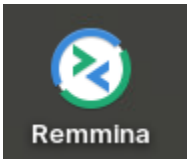
181. Press the **Enter** key to terminate the script and to close the terminal window.

This script generates traffic through the chicago-fw to create entries in the Traffic, URL Filtering, and Threat logs.

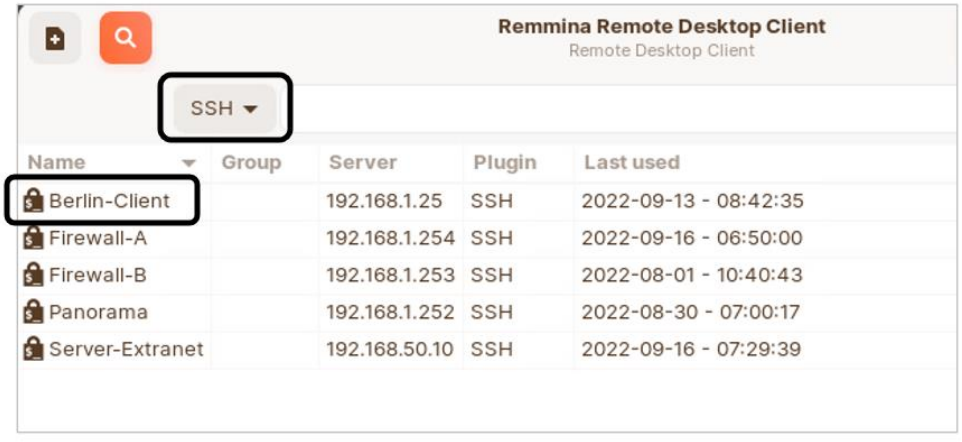
Run the Traffic Script on the Berlin Workstation

In this section, you will connect to the client behind the Berlin firewall and generate traffic.

182. On client-A, open the Remmina application:



183. Double-click the entry for **Berlin-Client**:



184. Remmina will connect to the Berlin client.

185. Run the following command:

```
./b-logtesting.sh <ENTER>
```

186. What until you see that the script has completed before proceeding:

```
################################

Log entry generation complete.

################################
```

187. Type **`exit`** and press **Enter** to close the SSH connection to the Berlin-Client.

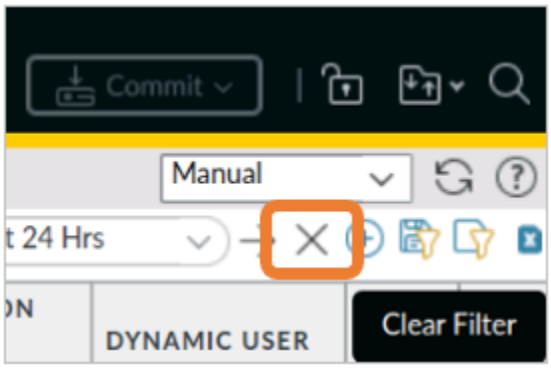
The script generates traffic from the Berlin client through the Berlin firewall to create entries in the Traffic, URL Filtering, and Threat logs.

188. Close the Remmina Remote Desktop Client application window.

Verify That Firewalls Forward Traffic Logs Events to Panorama

189. In Panorama, navigate to **Monitor** > **Traffic**.
190. Select **Corp-DG** from the **Device Group** drop-down list:

191. Clear any filters you may have in place by clicking the **Clear Filter** button in the upper-right corner of the window:

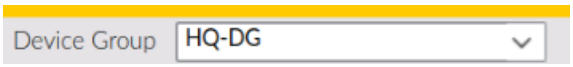


192. Scroll through the table and note that you have entries from the chicago-fw and berlin-fw Devices:

DEVICE NAME	GENERATE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION	RULE
berlin-fw	07/14 17:53:29	Users_Net	Internet	192.168.1.25	4.2.2.2	dns	allow	Allow-Internet-Access
berlin-fw	07/14 17:53:19	Users_Net	Internet	192.168.1.25	184.51.19.205	ssl	allow	Allow-Internet-Access
berlin-fw	07/14 17:53:14	Users_Net	Internet	192.168.1.25	184.51.19.205	ping	allow	Allow-Internet-Access
chicago-fw	07/14 17:53:34	Users_Net	Extranet	192.168.1.25	192.168.50.80	web-browsing	allow	Users_to_Extranet
chicago-fw	07/14 17:53:32	Users_Net	Internet	192.168.1.254	35.190.82.33	paloalto-updates	allow	Allow-Internet-Access
chicago-fw	07/14 17:53:24	Users_Net	Extranet	192.168.1.25	192.168.50.150	ping	allow	Users_to_Extranet

Remember that you can customize the columns to view and the order of those columns in any Panorama table. In the preceding example, the Device Name column has been moved to the far left side of the table. Other columns have been hidden.

193. Select **HQ-DG** from the **Device Group** drop-down list:



194. Scroll through the table and note that you have entries only from the chicago-fw Device:

DEVICE NAME	GENERATE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION	RULE
chicago-fw	07/14 17:57:27	Users_Net	Extranet	192.168.1.252	192.168.50.53	dns	allow	Users_to_Extranet
chicago-fw	07/14 17:57:27	Users_Net	Internet	192.168.1.252	8.8.8.8	dns	allow	Allow-Internet-Access
chicago-fw	07/14 17:57:27	Users_Net	Extranet	192.168.1.252	192.168.50.53	dns	allow	Users_to_Extranet
chicago-fw	07/14 17:57:07	Users_Net	Extranet	192.168.1.252	192.168.50.53	dns	allow	Users_to_Extranet
chicago-fw	07/14 17:57:07	Users_Net	Internet	192.168.1.252	8.8.8.8	dns	allow	Allow-Internet-Access
chicago-fw	07/14 17:57:07	Users_Net	Extranet	192.168.1.252	192.168.50.53	dns	allow	Users_to_Extranet

195. Change the **Device Group** drop-down list to **Branch-DG**:

DEVICE NAME	GENERATE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION	RULE
berlin-fw	07/14 17:54:35	Users_Net	Internet	192.168.1.25	184.51.19.205	web-browsing	allow	Allow-Internet-Access
berlin-fw	07/14 17:54:35	Users_Net	Internet	192.168.1.25	184.51.19.205	web-browsing	allow	Allow-Internet-Access
berlin-fw	07/14 17:54:35	Users_Net	Internet	192.168.1.25	184.51.19.205	web-browsing	allow	Allow-Internet-Access
berlin-fw	07/14 17:54:34	Users_Net	Internet	192.168.1.25	184.51.19.205	web-browsing	allow	Allow-Internet-Access
berlin-fw	07/14 17:53:35	Users_Net	Internet	192.168.1.25	4.2.2.2	dns	allow	Allow-Internet-Access

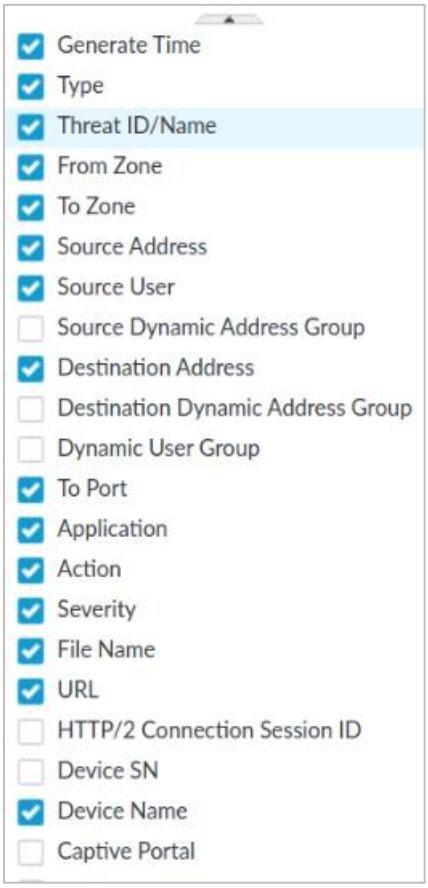
Both firewalls are forwarding Traffic log events to Panorama.

Verify That Firewalls Forward Threat Events to Panorama

The Log Forwarding Profile you defined instructs firewalls to forward Threat log events to Panorama. In this section, you will verify that entries from both firewalls appear in the Panorama Threat log.

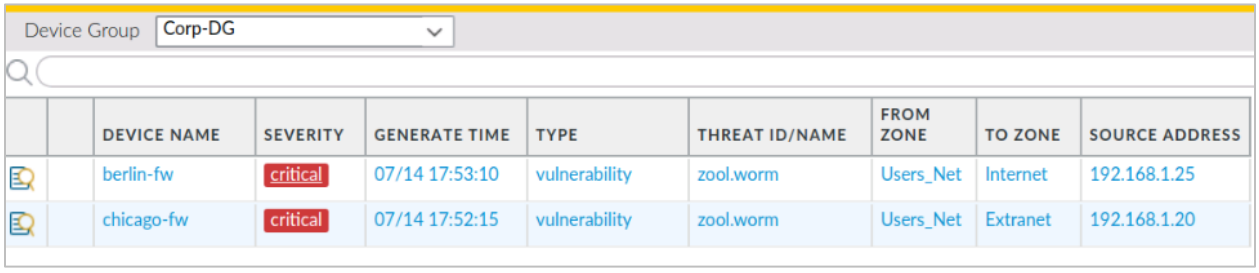
196. In Panorama, navigate to **Monitor** > **Threat**.
197. Select **Corp-DG** from the **Device Group** drop-down list:

198. Modify the columns to display only the following items:



199. Move the **Device Name** column to the left-most position:
200. Move the **Severity** column next to the **Device Name**.

201. Note vulnerability entries:



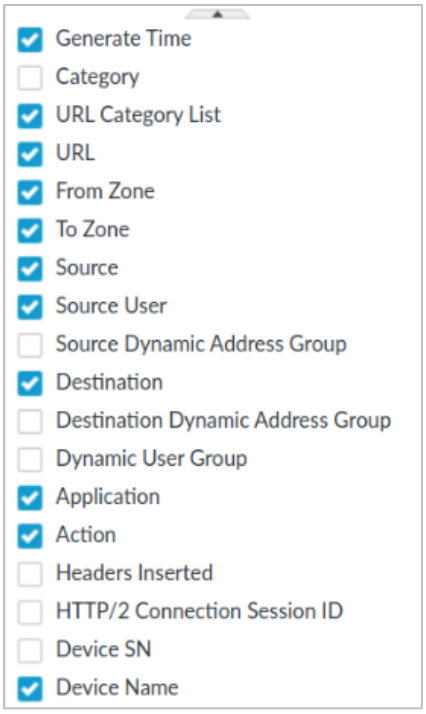
Both firewalls are forwarding Threat log events to Panorama. Remember that you can customize the columns to view and the order of those columns in any Panorama table.

Verify That Firewalls Forward URL Filtering Logs to Panorama

The Log Forwarding Profile you defined instructs firewalls to forward URL Filtering log events to Panorama. In this section, you will verify that entries from both firewalls appear in the Panorama URL Filtering log.

202. In the Panorama web interface, navigate to **Panorama > Monitor > URL Filtering**.
203. Select **Corp-DG** from the **Device Group** drop-down list:

204. Modify the table to display only the following columns:



205. Move the **Device Name** and **Action** columns to the left side of the table.
206. Note entries from the **chicago-fw** and **berlin-fw**:

	DEVICE NAME	ACTION	GENERATE TIME	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE
	berlin-fw	alert	07/14 17:53:10	computer-and-internet-info,low-risk	www.paloaltone...	Users_Net	Internet	192.168.1.25
	chicago-fw	alert	07/14 17:52:50	computer-and-internet-info,low-risk	ml-static.service....	Users_Net	Internet	192.168.1.253
	chicago-fw	alert	07/14 17:52:42	computer-and-internet-info,low-risk	ml.service.paloal...	Users_Net	Internet	192.168.1.253
	chicago-fw	alert	07/14 17:52:30	computer-and-internet-info,low-risk	updates.paloalto...	Users_Net	Internet	192.168.1.252

Both firewalls are forwarding URL Filtering log events to Panorama.

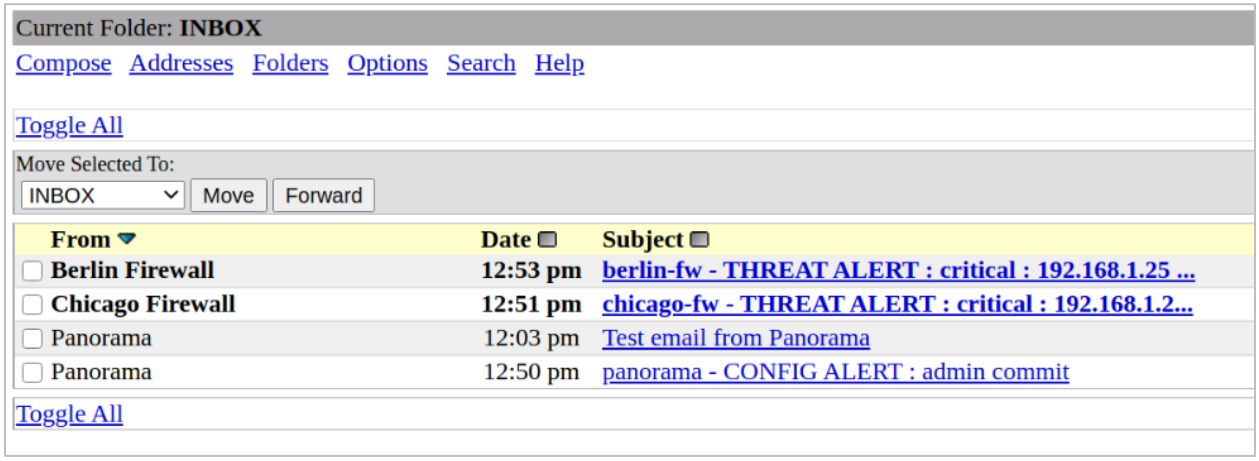
Verify Threat Email from Firewalls

The Log Forwarding Profile you defined instructs firewalls to send an email when they encounter a Threat with a critical or high severity level. In this section, you will check your lab email account.

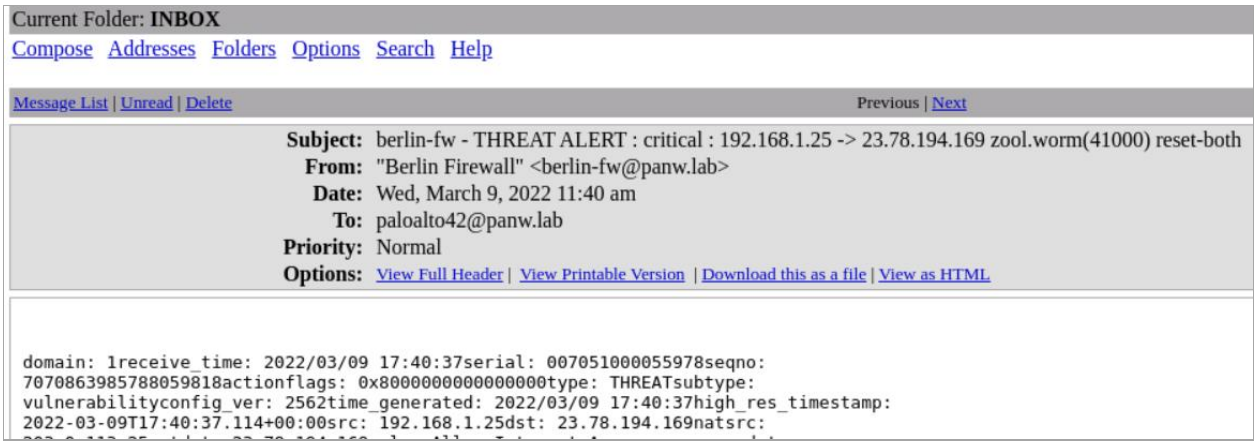
207. In the Configuration browser, open a new tab.
208. From the **Bookmark** toolbar, select **Extranet > Lab Mail**:

209. Log in with **`paloalto42`** and **`Pal0Alt0!`** as the credentials.

210. Note emails from Chicago and Berlin firewalls about threats:



211. Open any THREAT ALERT email to see details:



Note that the date and time stamps you see in the email will differ from the example shown here.

212. Note that the **Subject** line of the email gives you a synopsis of the message including the **severity**, **source and destination IP**, **threat name**, **threat ID number**, and **action**.
213. Close the Threat email message.
214. Sign out of web mail.
215. Close the **Mail** tab.

Stop. This is the end of the lab.

Lab 6 Scenario: Using Panorama Logs

With your Templates and Device Groups defined and deployed, you now can manage your firewalls through Panorama. You can define network and Device elements in Templates; and you can define policy and objects in Device Groups.

You also have successfully defined Log Forwarding Profiles that instruct firewalls in the HQ-DG Device Group and the Branch-DG Device Group to send copies of log events to Panorama. Panorama now provides you with a single management interface to examine application traffic, threats, URL requests, and other details across your network.

In this section, you will use Panorama to locate specific information from Traffic, URL Filtering, and Threat logs. You then will use this information to modify firewall configurations through Panorama to more effectively secure your network.

Lab Objectives

- Generate traffic from Chicago and Berlin clients
- Use information from traffic files to block certain applications
- Use information in the URL log to modify the URL Filtering Profile (Corp) to block certain sites
- Use information in the Threat log
- Use filters to locate specific hosts generating threat traffic
- Export filter results to a spreadsheet and open in **Calligra Sheets**

High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-6-Start.xml** configuration file on Panorama.

Push the Configuration to Firewalls

- Push the Device Group and Template changes to the firewalls using **`Force Template Values`**

Generate Traffic Through Both Firewalls

- On the Chicago workstation (client-a), run the **URL Traffic Generator** from with the **Class-Scripts/EDU-220** folder.
    - Allow this script to run throughout the entire lab.
- Use Remmina to connect to the Berlin-Client:
    - Change to the appropriate directory:

      `cd /home/lab-user/Desktop/Lab-Files/EDU-220/ <ENTER>`
    - Launch the b-url-traffic.sh script:

      `./b-url-traffic.sh <ENTER>`
    - Allow the script to run uninterrupted.
- Use Remmina to connect to the Server-Extranet host
    - Run the traffic generator using the following command:

      `./UsingLogs-V1.sh <ENTER>`
    - Leave the Remmina connections open because you will need them later in this lab

Identify Inappropriate Web Browsing

- Add the URL Category List to the URL Filtering log
- Create and apply a filter in the URL Filtering log to display entries that have visited gambling sites.

Use the Filter Builder

- Use the Filter Builder to create a filter that will display URL Filtering log entries for **gambling** and **weapons**.

Save This Filter

- Save the filter you created for gambling and weapons.

- For **Name**, use **`URL is gambling or weapons`**
- Clear any filters you currently have in the URL Filtering log.
- Load and apply the **URL is gambling or weapons** filter you saved to test its accuracy.

Identify Unauthorized Online Storage Traffic

- Create and apply a filter in the Traffic log to identify the **dropbox-base** application.

Export the Filtered Traffic to CSV

- Export the filtered Traffic log to a CSV file and save the file to the **Downloads** folder on the client-A host.
- Open the CSV file with **Calligra Sheets**.
- Note the columns and information exported to CSV.
- Close **Calligra Sheets**.

Modify Security Policy Rules to Block Dropbox

- Use the information below to create a **Security Pre-Rule** in the **HQ-DG** Device Group to block the **dropbox-base** application:

Parameter	**Value**
General tab	
Name	**`Block_Unauthorized_File_Storage_Apps`**
Description	**`Blocks non-corporate file storage applications.`**
Source tab	
Source Zone	**Users_Net**
Destination tab	
Destination Zone	**Internet**
Application tab	
Application	**dropbox**
Service/URL Category tab	
Service	**any**
Actions tab	
Actions	**Deny**
Log Forwarding	**default**

Modify the URL Filtering Profile to Block Categories

- Modify the **Corp-URL** Filtering Profile to block access to the following categories:
    - **`Adult`**
    - **`Command and control`**
    - **`Copyright infringement`**
    - **`Extremism`**
    - **`Gambling`**
    - **`Hacking`**
    - **`High-risk`**
    - **`Malware`**
    - **`Phishing`**
    - **`Proxy-avoidance-and-anonymizers`**
    - **`Shareware-and-freeware`**
    - **`Unknown`**
    - **`Weapons`**

Commit the Changes

- Commit the changes to Panorama before proceeding.

Push the Configuration to Firewalls

- Push the Device Group and Template changes to the firewalls using **`Force Template Values`**

Generate Traffic

- In the Remmina connection to the Server-Extranet host, run the traffic generator script again:

    `./UsingLogs-V1.sh <ENTER>`

    - Allow the script to complete (5-10 minutes).

Examine the Traffic Log

- Display entries in the Traffic log for all Device Groups that have been blocked by the new Security Policy Pre-Rule for dropbox-base
- Use a filter in the Traffic log to display all entries that have an action OTHER THAN **`allow`** or a filter that displays entries with dropbox-base as the application.

Examine the URL Filtering Log

- Create a filter to display entries in the URL Filtering log for URLs that have been blocked by the Corp-URL filtering profile you updated.

Create a Combined Filter

- Use the Filter Builder to create and apply a filter that displays traffic that has not been allowed for the past 15 minutes within All Device Groups.

Lab Cleanup

- Stop the script on the Berlin-Client and close the Remmina connection to the Berlin-Client.
- Close the Remmina connection to the Server-Extranet host.
- Stop the script on client-A and close the Terminal window.

Detailed Lab Steps

Load the Lab Start Configuration File

1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-6-Start.xml**.
4. Leave the remaining settings unchanged
5. Click **OK** to close the **Load Named Configuration** window.
6. Click **Close** on the **Loading Configuration** window.

Push the Configuration to Firewalls

7. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
8. When the **Commit to Panorama** window appears, click **Commit**.
9. Monitor the status of the commit.
10. When the commit status is complete, click **Close**.
11. Select the commit icon and choose **Push to Devices**.
12. Click **Edit Selections**.
13. Select the **Device Groups** tab and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected.
14. Select the **Force Template Values** check box at the bottom.
15. Click **Yes** on the **Force Template Values** warning message.
16. On the **Templates** tab, select the check boxes for the Chicago firewall and the Berlin firewall.
17. Click **OK**.
18. Click **Push** to start the process.
19. Wait until the **Commit All** jobs are complete.
20. Click **Close**.

Generate Traffic Through Both Firewalls

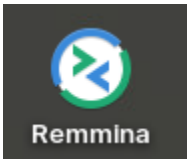
In this section, you will use scripts on the Berlin and Chicago clients to generate traffic. You also will generate traffic from the Extranet server. This automated process will result in numerous entries in the Traffic, Threat, URL Filtering, and User logs that you can examine in Panorama.

21. On client-A, double-click the icon for **URL Traffic Generator** to launch the script in a Terminal window:

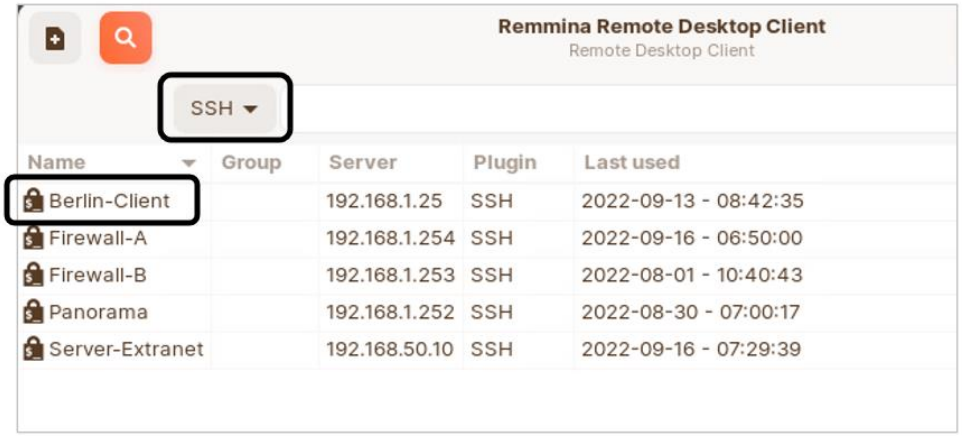
22. This script will loop continuously, and you should allow it to run uninterrupted until the end of this lab.

    This script clears the log files for the firewalls and Panorama. The script then generates various URL requests from users in Chicago to the Internet and to the Extranet security zones.

23. On client-A, open the Remmina application by double-clicking the icon on the Desktop:



24. Double-click the entry for **Berlin-Client**:



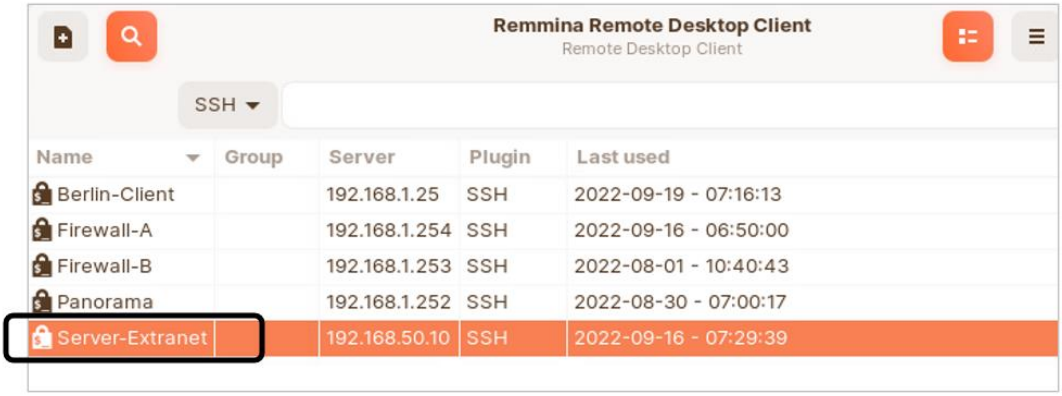
    This application will connect to the Berlin workstation through SSH.

25. Launch the b-url-traffic.sh script:

    `./b-url-traffic.sh <ENTER>`

    The script generates various URL requests from users in Berlin to the Internet and to the Extranet security zones.

26. This script will loop continuously, and you should allow it to run uninterrupted until the end of this lab.
27. In the Remmina Remote Desktop Client window, double-click the entry for **Server-Extranet**:



This application will connect to the Extranet server through SSH.

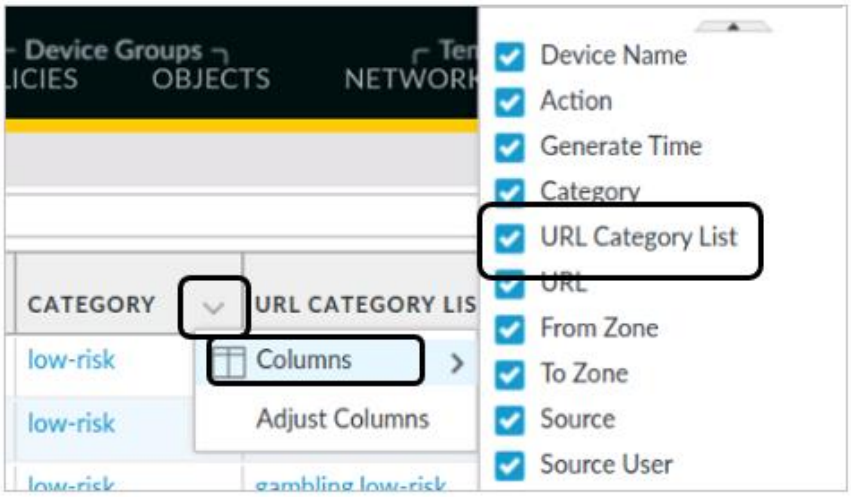
28. Remmina will create a connection to the Extranet server:
29. Run the traffic generator using the following command:
    `./UsingLogs-V1.sh <ENTER>`
30. The script presents a confirmation window – press **`<ENTER>`** to start the process.
    This script runs simulated application traffic through the Chicago firewall, and will take about 10 minutes to complete.
31. Leave the Remmina connections open because you will need them later in this lab.

Identify Inappropriate Web Browsing

32. Upper management in your organization is interested in applying a more strict policy about which websites employees may visit while at work.
33. However, before any restrictions are put into place, you have been asked to identify inappropriate categories that users are currently visiting so that management can make an informed decision about which types of sites to block.
34. In this section, you will use the URL Filtering log to determine whether employees are visiting the following URL categories:
    - Weapons
    - Gambling
35. In Panorama, navigate to **Monitor** > **URL Filtering**.
36. Select **Corp-DG** from the **Device Group** drop-down list:

This view will show you URL traffic from all firewalls in your organization.

37. Add the **URL Category List** column to the display (it may already be visible).
38. Click the small down **triangle** icon next to **Category**.
39. Choose **Columns**.
40. Place a **check mark** in the **box** for **URL Category List**:



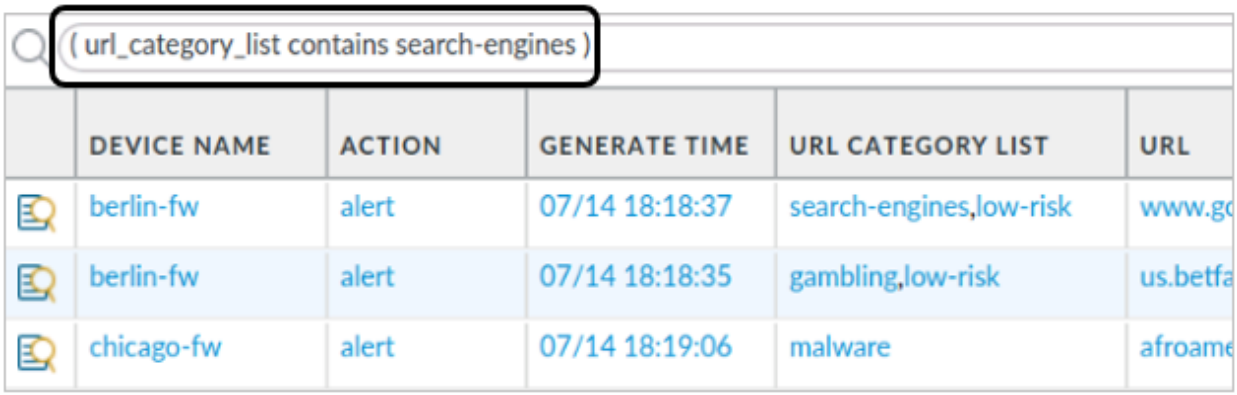
Panorama URL filtering service often assigns multiple categories to a single URL. The Category column shows the primary category for a specific URL. The URL Category List shows you all categories that a URL has been assigned.

41. Click the first item in the URL Category List for the first entry in the table. This example shows clicking of search-engines:

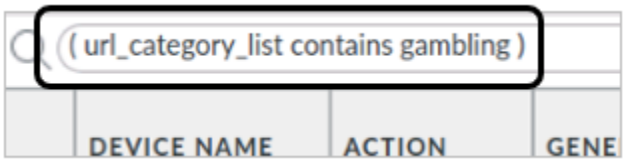
DEVICE NAME	ACTION	GENERATE TIME	URL CATEGORY LIST	URL
berlin-fw	alert	07/14 18:18:37	search-engines,low-risk	www.go
berlin-fw	alert	07/14 18:18:35	gambling,low-risk	us.betfai
chicago-fw	alert	07/14 18:19:06	malware	afroame

The link you click does not matter, as long as it resides in the URL Category List.

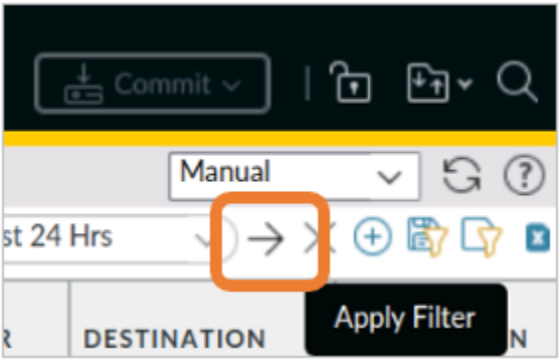
42. Clicking the link generates an entry in the filter field above the table:



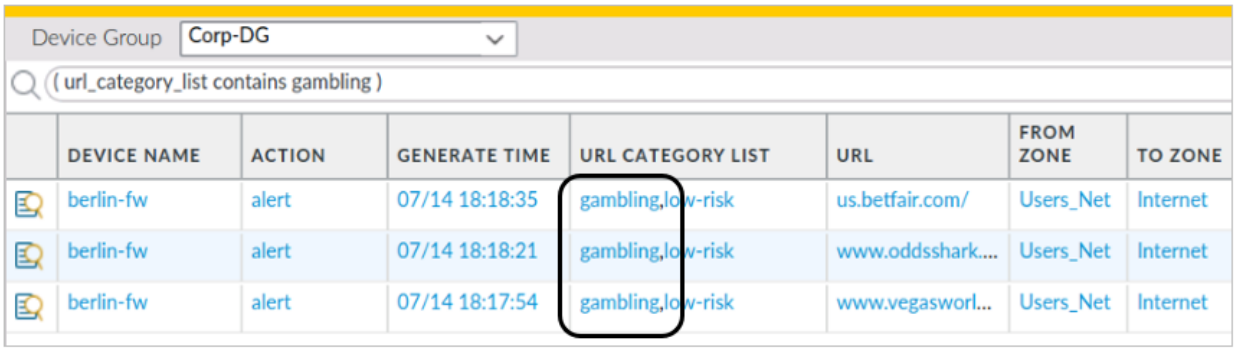
43. Change the category portion of the filter to **gambling**:



44. Click the **Apply Filter** button (small arrow in the upper-right section of the window):



45. Panorama will display only those entries for URLs that are in the **gambling** category:

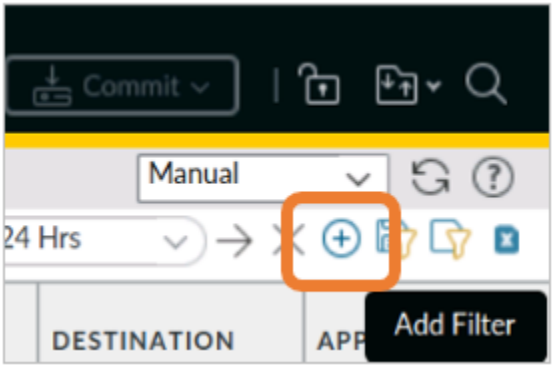


Note: Columns have been rearranged and hidden in the preceding image.

Use the Filter Builder

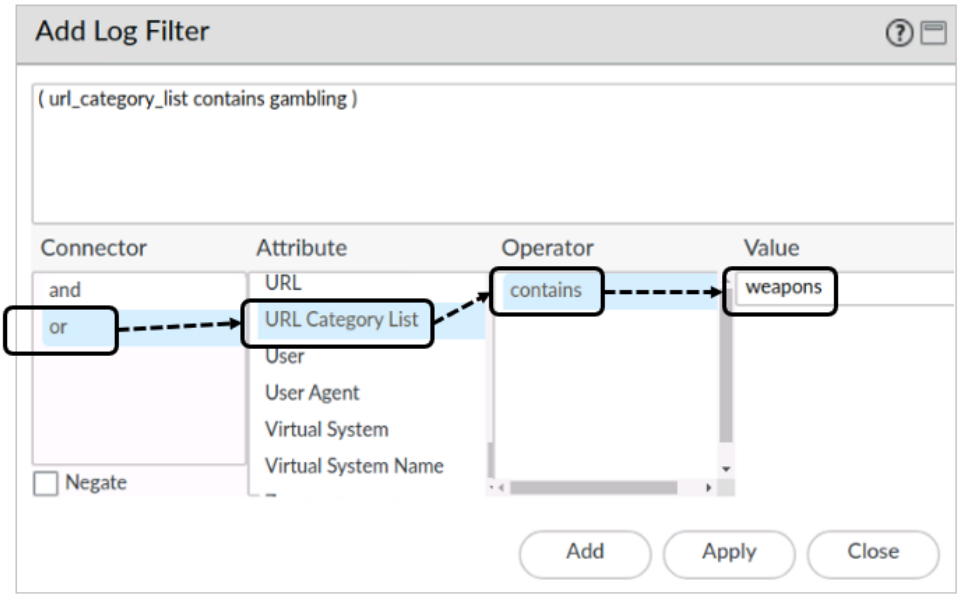
In the preceding section, you created a simple filter by clicking a single link in the URL filtering table and modifying the filter syntax. In this section, you will use the Filter Builder to create a combined filter. This combined filter will look for entries to either gambling or weapons websites.

46. Click the **Add Filter** button (small plus sign in the upper-right section of the window):



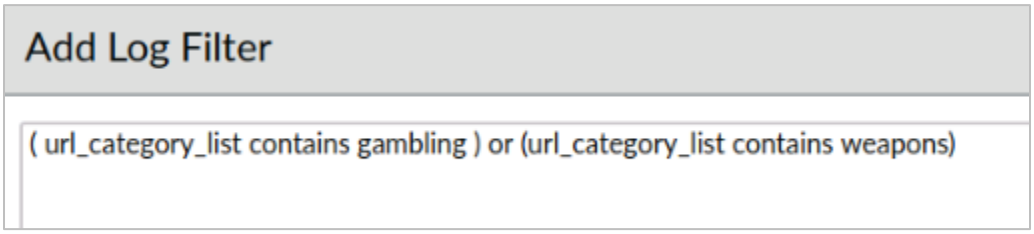
47. In the **Add Log Filter** window, note that the existing syntax for the gambling filter is still in place.
48. Under the **Connector** column, highlight **or**.
49. Under the **Attribute** column, scroll down and highlight **URL Category List**.
50. Leave the **Operator** set to **contains**.

51. In the **Value** field, enter **weapons**:

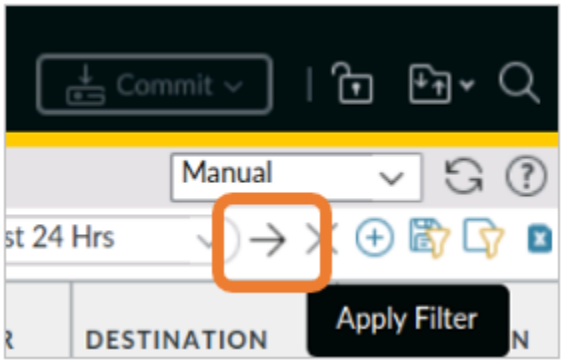


The **Value** is case-sensitive.

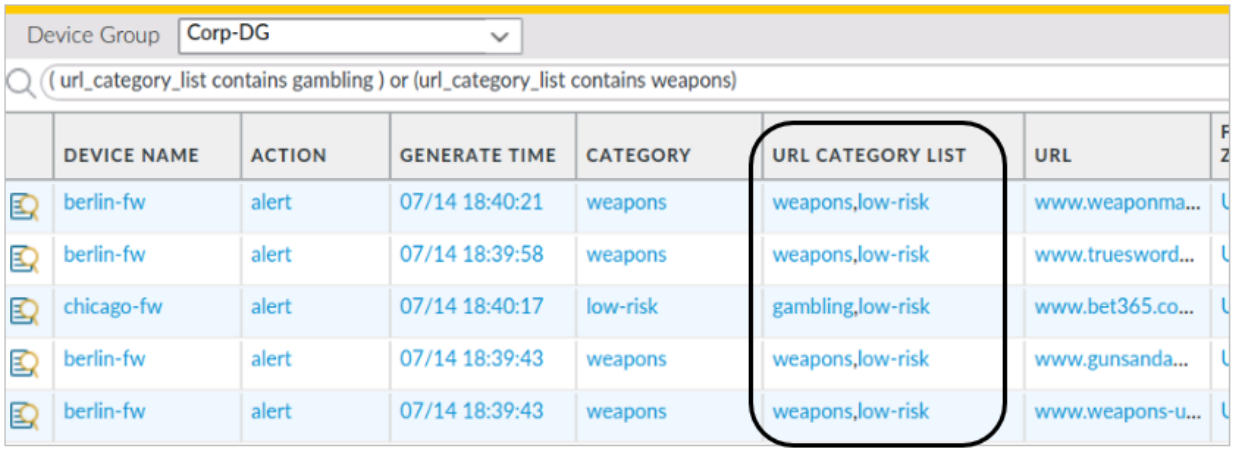
52. Click the **Add** button to append this filter to the existing entry for gambling:



53. Click the **Apply** button to add this new filter to the URL filtering table.
54. Click the **Apply Filter** button:

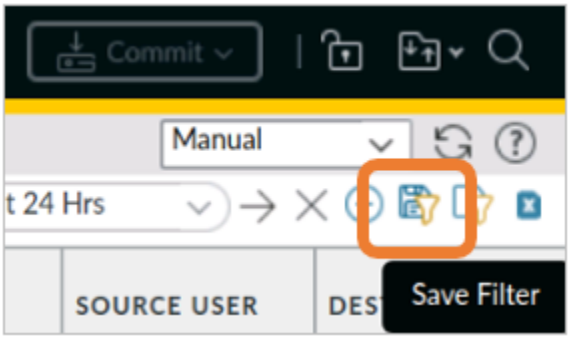


55. Panorama will display entries for traffic to either gambling or weapons websites:

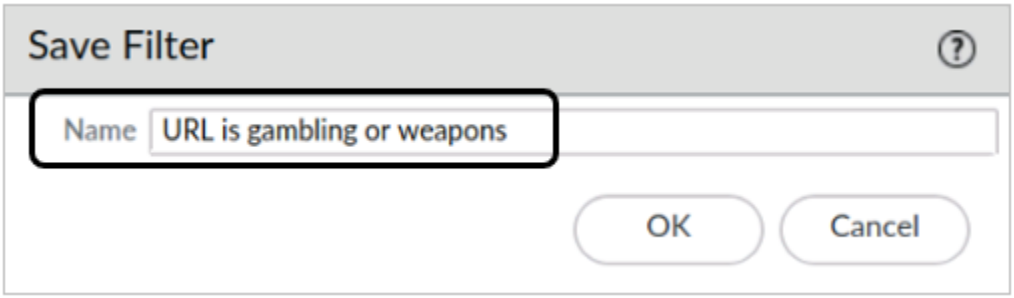


Save This Filter

56. You intend to use this filter frequently over the next few weeks. In this section, you will save the filter so that you can retrieve and apply it later.
57. Click the **Save Filter** button (small diskette in the upper-right section of the window):



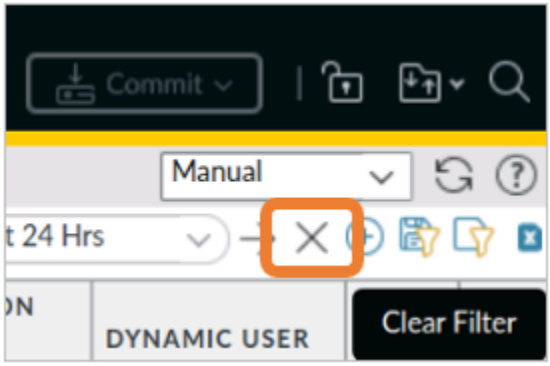
58. In the **Save Filter** window, enter **`URL is gambling or weapons`**:



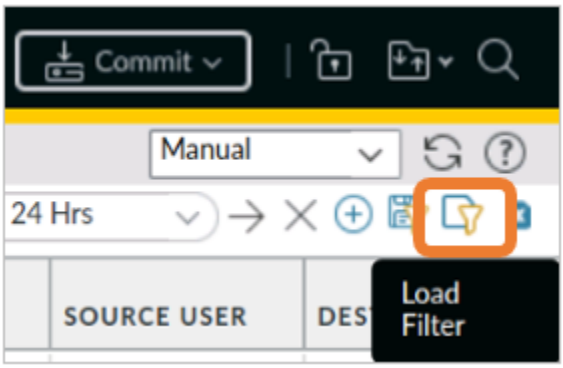
Note that the name you use should easily identify what the filter searches for.

59. Click **OK**.

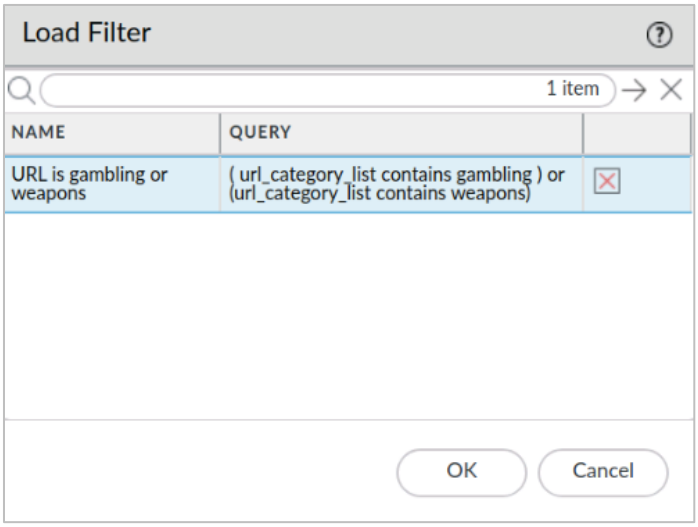
60. Clear the filter field (small X in the upper-right section of the window):



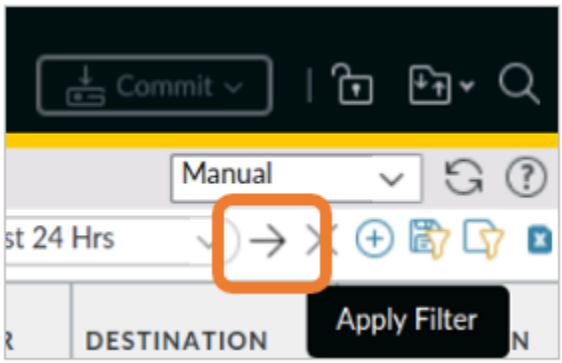
61. Load the filter you created by clicking the **Load Filter**:



62. In the **Load Filter** window, select the **URL is gambling or weapons** entry and click **OK**:



63. Click the **Apply Filter** button:



64. Panorama will display entries for traffic to either gambling or weapons websites based on the filter parameters.
65. Click the **Clear Filter** button to remove this filter.

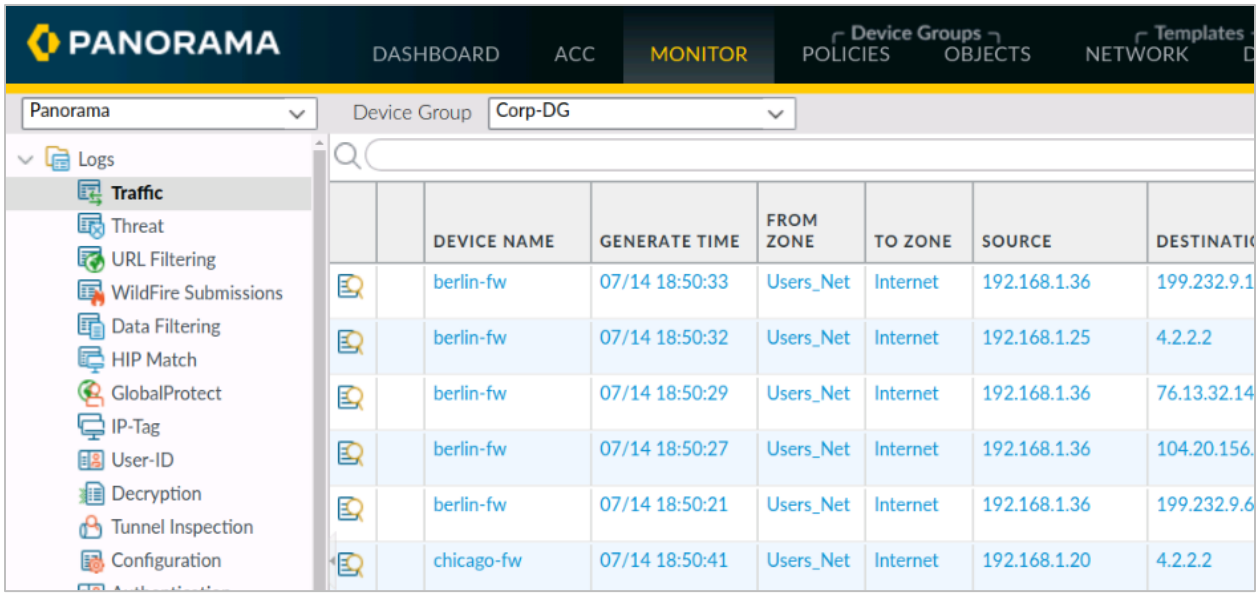
Identify Unauthorized Online Storage Traffic

Your organization recently consolidated all cloud-based storage for client workstations to a single application. However, some employees still are using unauthorized services to store work and personal files.

Your manager has instructed you to locate users who still are using Dropbox so that they can be notified to migrate any files to the official online storage application.

66. In Panorama, navigate to **Monitor** > **Traffic**.
67. Select **Corp-DG** from the **Device Group** drop-down list:

68. This view will show you traffic from all firewalls in your organization:

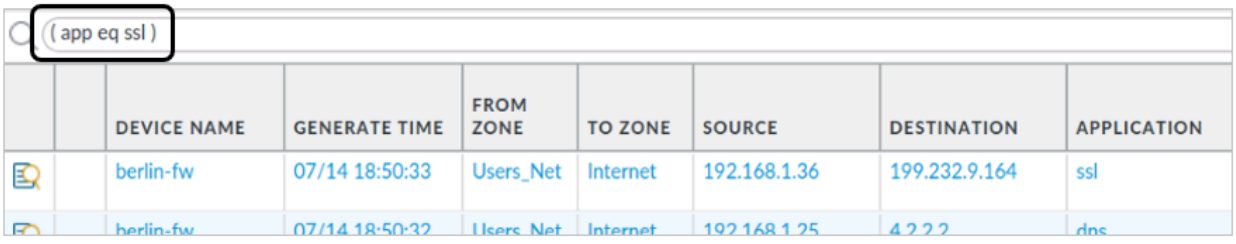


69. In the first entry in the list, click the link listed in the **Application** column. The following example shows clicking of the entry for ssl:

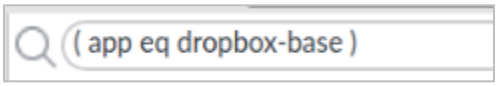
DEVICE NAME	GENERATE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION
berlin-fw	07/14 18:50:33	Users_Net	Internet	192.168.1.36	199.232.9.164	ssl
berlin-fw	07/14 18:50:32	Users_Net	Internet	192.168.1.25	4.2.2.2	dns
berlin-fw	07/14 18:50:29	Users_Net	Internet	192.168.1.36	76.13.32.141	ssl

The application you choose does not matter. You will modify the actual syntax.

70. Clicking the link will generate the correct syntax in the **Filter** field to search for entries that contain **ssl** in the **Application** column:

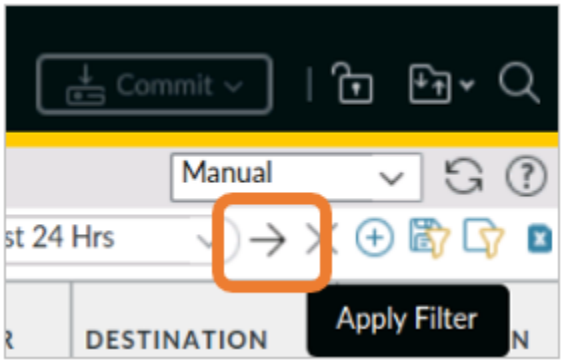


71. Manually change the listed application in the filter to **`dropbox-base`**:

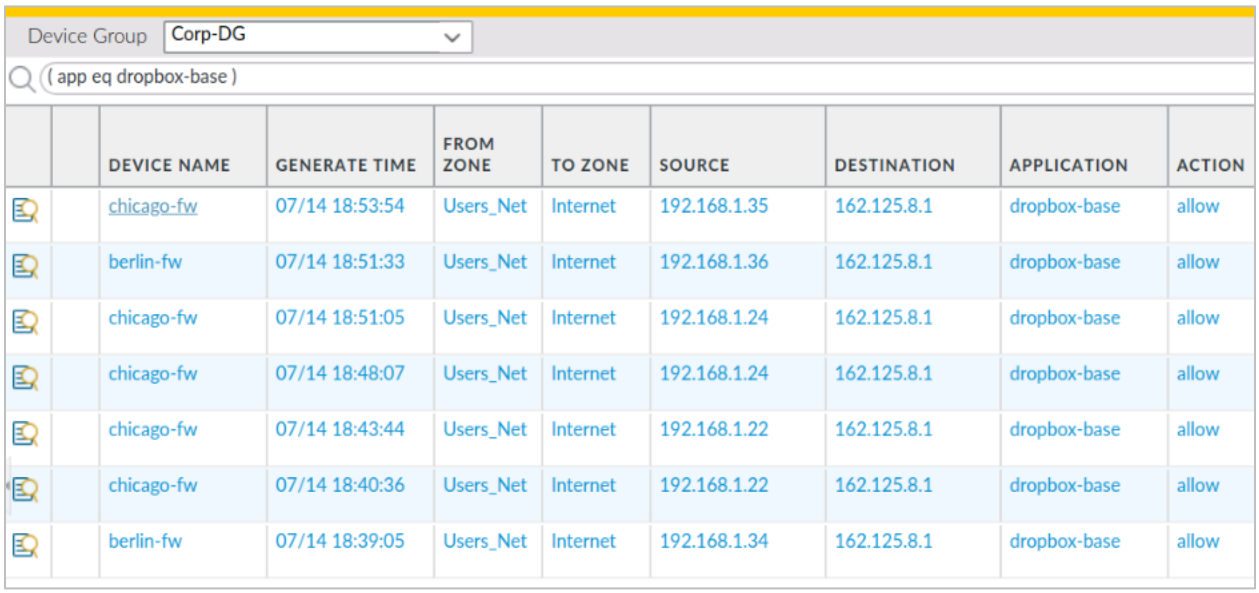


Remember that entries are case-sensitive.

72. Click the **Apply Filter** button:



73. Panorama will display only those entries the contain dropbox-base as the application:



		DEVICE NAME	GENERATE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
		chicago-fw	07/14 18:53:54	Users_Net	Internet	192.168.1.35	162.125.8.1	dropbox-base	allow
		berlin-fw	07/14 18:51:33	Users_Net	Internet	192.168.1.36	162.125.8.1	dropbox-base	allow
		chicago-fw	07/14 18:51:05	Users_Net	Internet	192.168.1.24	162.125.8.1	dropbox-base	allow
		chicago-fw	07/14 18:48:07	Users_Net	Internet	192.168.1.24	162.125.8.1	dropbox-base	allow
		chicago-fw	07/14 18:43:44	Users_Net	Internet	192.168.1.22	162.125.8.1	dropbox-base	allow
		chicago-fw	07/14 18:40:36	Users_Net	Internet	192.168.1.22	162.125.8.1	dropbox-base	allow
		berlin-fw	07/14 18:39:05	Users_Net	Internet	192.168.1.34	162.125.8.1	dropbox-base	allow

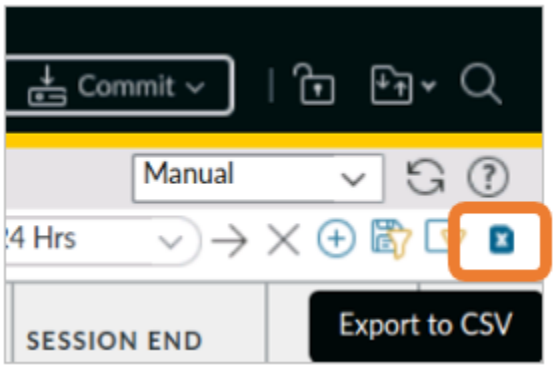
You can see from the filter results that users are still employing Dropbox.

Note that it may take a few minutes to generate dropbox traffic. If the table is empty, periodically use the refresh button to update the display.

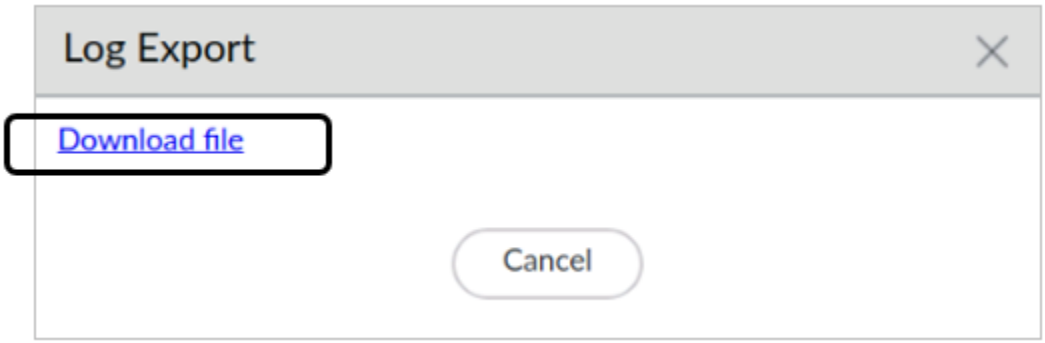
Export the Filtered Traffic to CSV

Management wants a list of employees who still are using Dropbox. In this section, you will export the filtered Traffic log to a CSV file.

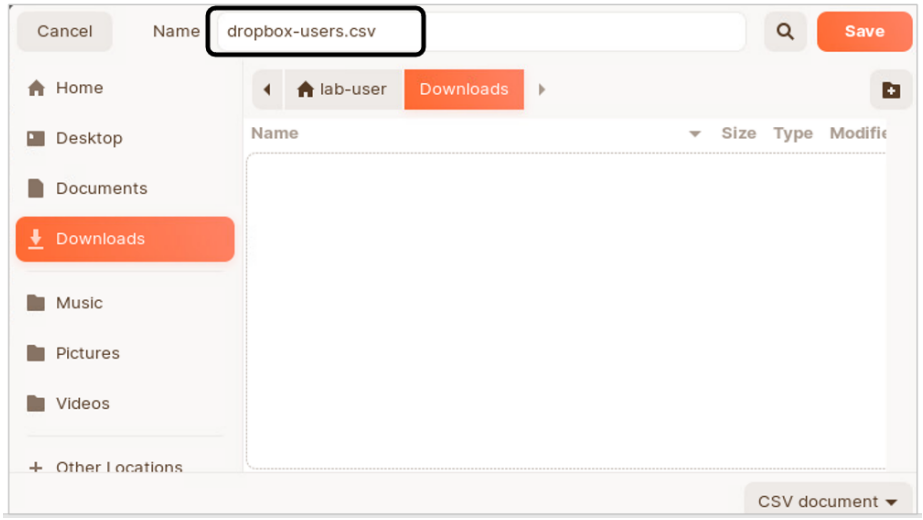
74. In the Traffic log, click the **Export to CSV** button (small page with X in the upper-right corner of the window):



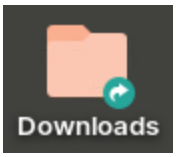
75. In the **Log Export** window, click **Download file**:



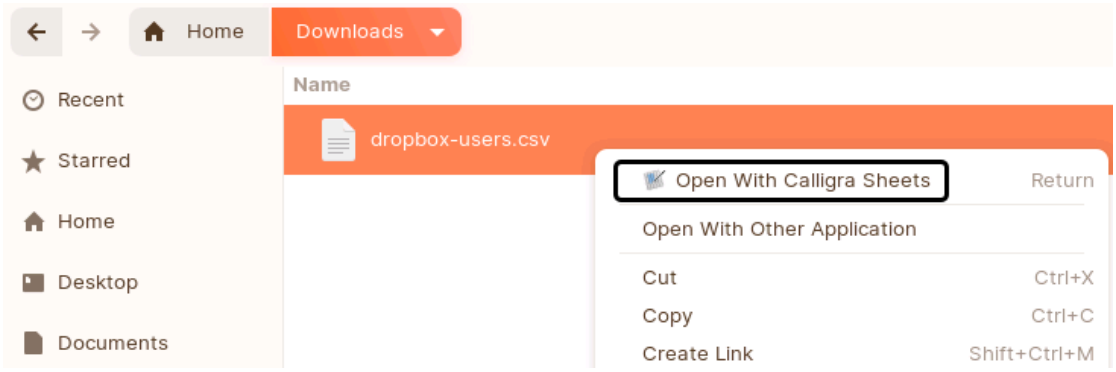
76. Save the file as **`dropbox-users.csv`** in the Downloads folder:



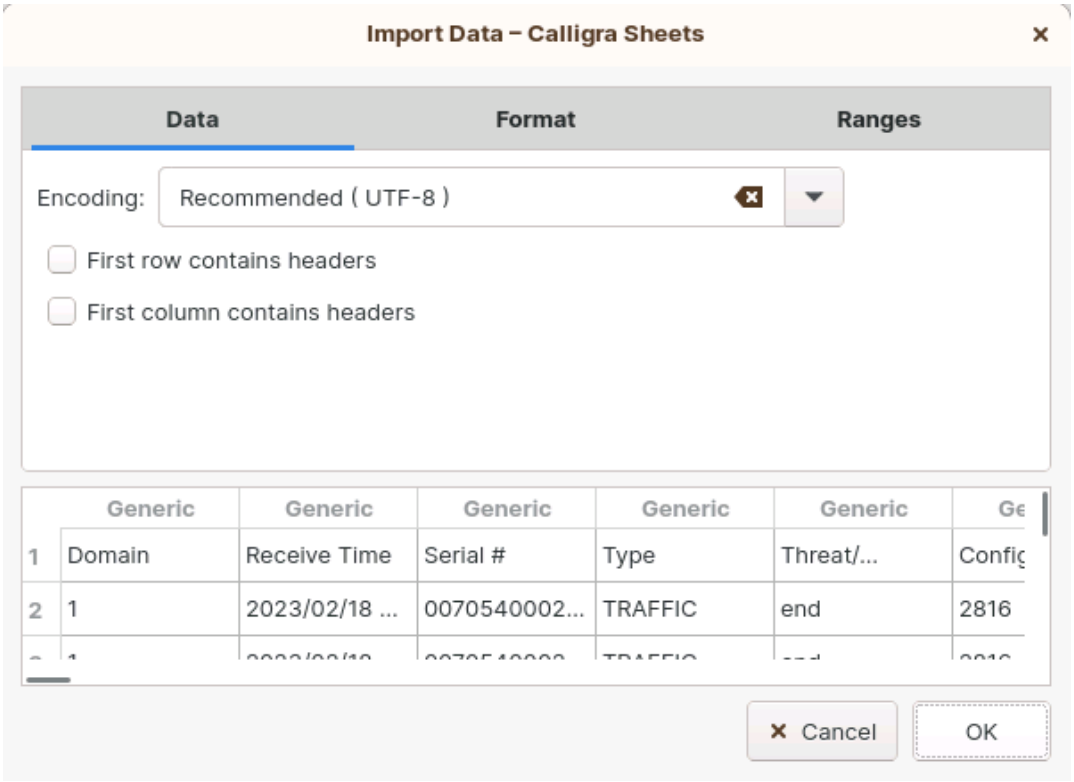
77. On the **Desktop**, double-click the **Downloads** icon:



78. Right-click the entry for **log.csv** and choose **Open With "Calligra Sheets"**:



79. In the **Text Import** window, leave the settings unchanged and click **OK**:



80. The log file opens in the spreadsheet application.

81. You can see that the exported log file includes the **Source User** column.

Note that when you export the contents of any log file to a CSV file, Panorama will include all columns for that log file type, regardless of the columns you have displayed or hidden in the Panorama web interface.

By default, the maximum number of entries for the export from all log files is capped at 1000. You can change the number of rows that Panorama exports for all tables.

For more information on this topic, log in to live.paloaltonetworks.com and search for "How to Increase the Maximum Number of Rows in a CSV Export" to locate the most recent article.

82. Close the **Calligra Sheets** window.
83. Close the **Downloads** folder window.
84. In the Configuration browser tab for Panorama, click **Cancel** on the **Log Export** window.

Modify Security Policy Rules to Block Dropbox

You have used the Traffic log in Panorama to verify some users are still employing unauthorized applications for file storage. Currently, you only need to employ this rule on firewalls in the HQ-DG. In this section, you will modify your Security policy rules to prevent users in the HQ offices from accessing Dropbox.

85. From the Panorama web interface, navigate to **Policies** > **Security** > **Pre Rules**.

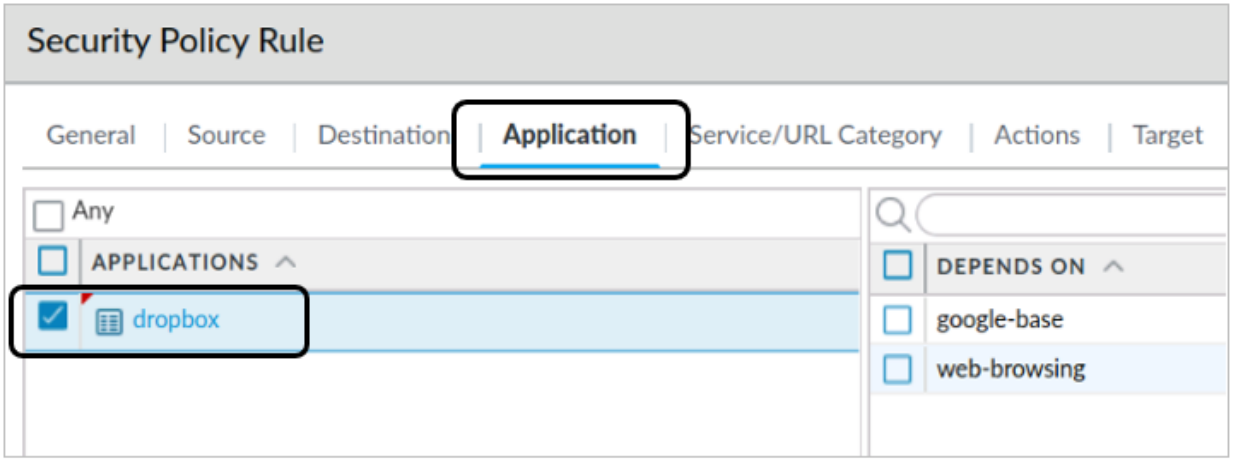
You will create a Pre Rule for firewalls so that local administrators cannot place an exception rule higher in the ruleset.

86. Select **HQ-DG** from the **Device Group** drop-down list:

87. Click **Add**.
88. Enter or select the following values to create a Security policy rule:

Parameter	Value
General tab	
Name	`Block_Unauthorized_File_Storage_Apps`
Description	`Blocks non-corporate file storage applications.`

Parameter	Value
Source tab	
Source Zone	**Users_Net**
Destination tab	
Destination Zone	**Internet**
Application tab	
Application	**dropbox**
Service/URL Category tab	
Service	**any**
Actions tab	
Actions	**Deny**
Log Forwarding	**default**



89. Click **OK** to create the new rule to block dropbox.

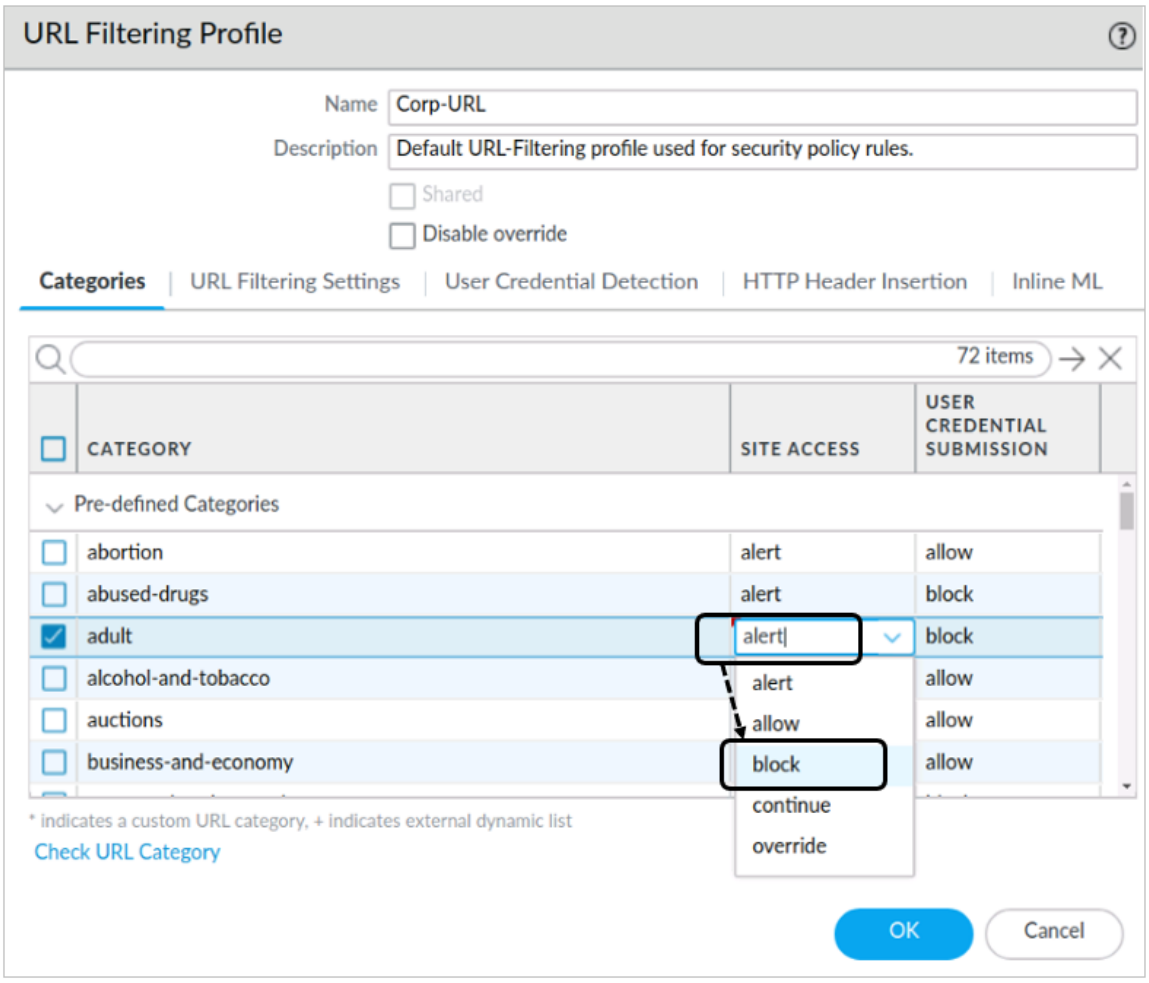
Modify the URL Filtering Profile to Block Categories

You provided a list of web categories to your organization's leadership team, and they have decided that employees should not visit certain types of websites while at work. You also have determined that you should block URL categories that pose a security risk to your organization.

In this section, you will modify the **Corp-URL** Filtering Profile to block dangerous or inappropriate categories.

90. In Panorama, navigate to **Objects > Security Profiles > URL Filtering**.
91. Select **Corp-DG** from the **Device Group** drop-down list:

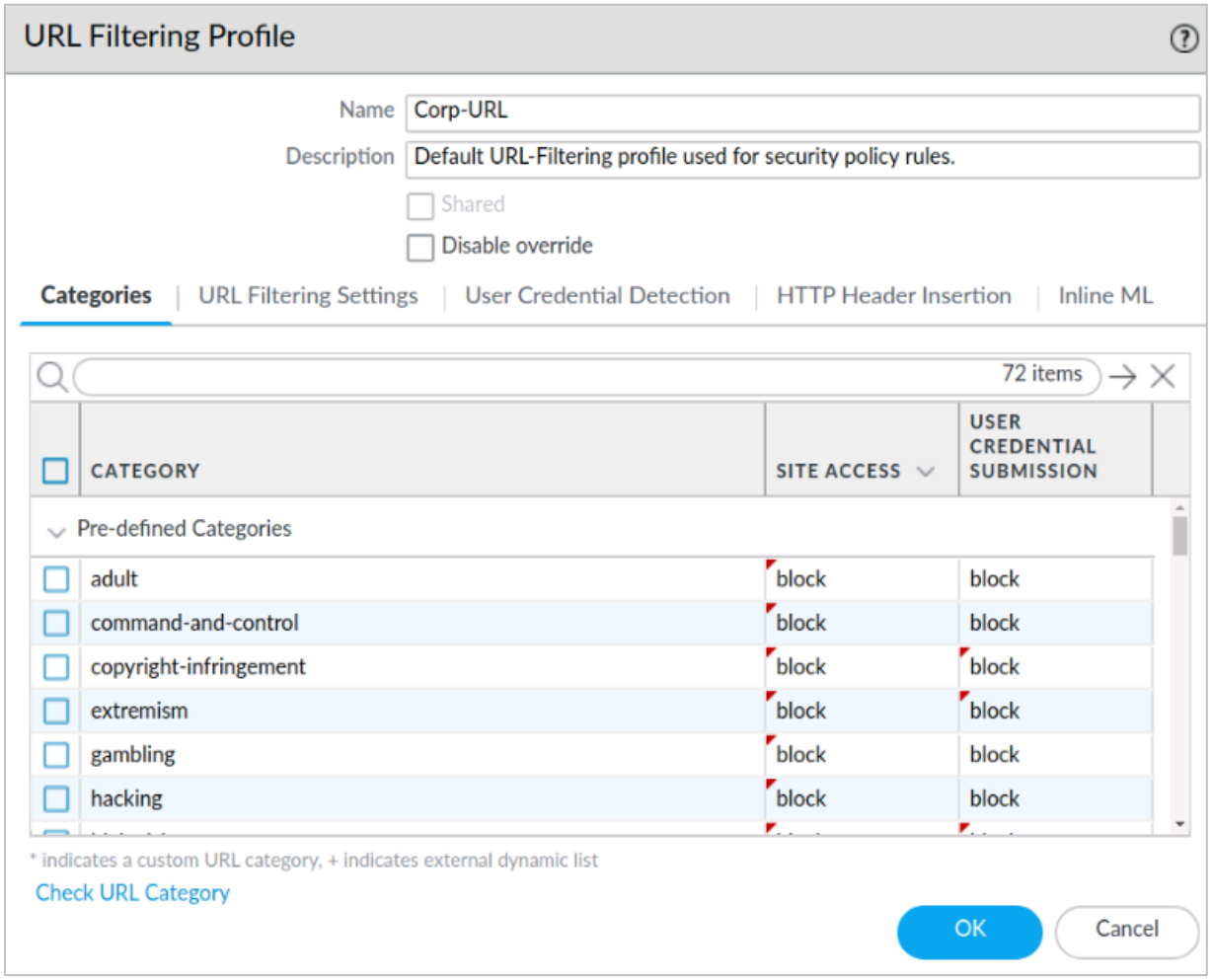
92. Click the link for **Corp-URL** to edit the entry.
93. In the list of **Predefined Categories**, scroll down and locate **adult**.
94. In the **Site Access** column, change the **Site Access** from **alert** to **block**:



95. Repeat this step for each of the following categories to set them to **block**:
    - Adult
    - Command and control
    - Copyright infringement
    - Extremism
    - Gambling
    - Hacking
    - High-risk
    - Malware

- Phishing
- Proxy-avoidance-and-anonymizers
- Shareware-and-freeware
- Unknown
- Weapons

96. Leave the remaining settings unchanged:

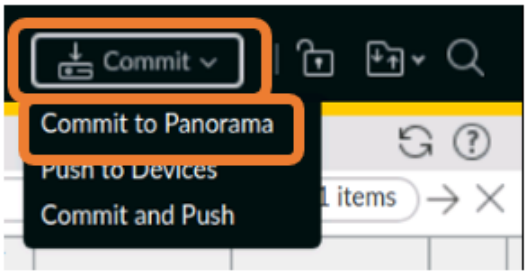


You can click the **Site Access** column header to sort entries. The example shows the entries sorted in reverse order starting with block. This arrangement makes all the entries that have been set to block easier to see.

97. Click **OK**.

Commit the Changes

98. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



99. Click **Commit**.
100. Monitor the status of the commit.
101. When the commit status is complete, click **Close**.

Push the Configuration to the Firewalls

102. Select **Commit > Push to Devices**.
103. Click **Edit Selections**.
104. Select the **Device Groups** tab, and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected
105. Select the **Force Template Values** check box at the bottom.
106. Click **Yes** on the **Force Template Values** warning message.
107. On the **Templates** tab, verify that the check boxes for the **chicago-fw** and the **berlin-fw** are selected.
108. Click **OK**.
109. Click **Push** to start the process.
110. Wait until the **Commit All** jobs are complete.
111. Click **Close**.

Generate Traffic

With the new Security policy rule in place and with updates to the Corp-URL profile, you need to verify that the managed firewalls are blocking traffic appropriately. You will run the traffic-generating scripts again.

112. In the Remmina Remote Desktop Client window, select the connection for **Server-Extranet**.
113. Run the traffic generator using the following command:
    `./UsingLogs-V1.sh <ENTER>`
    This script runs simulated application traffic through the Chicago firewall and can take from 5 to 10 minutes to complete.

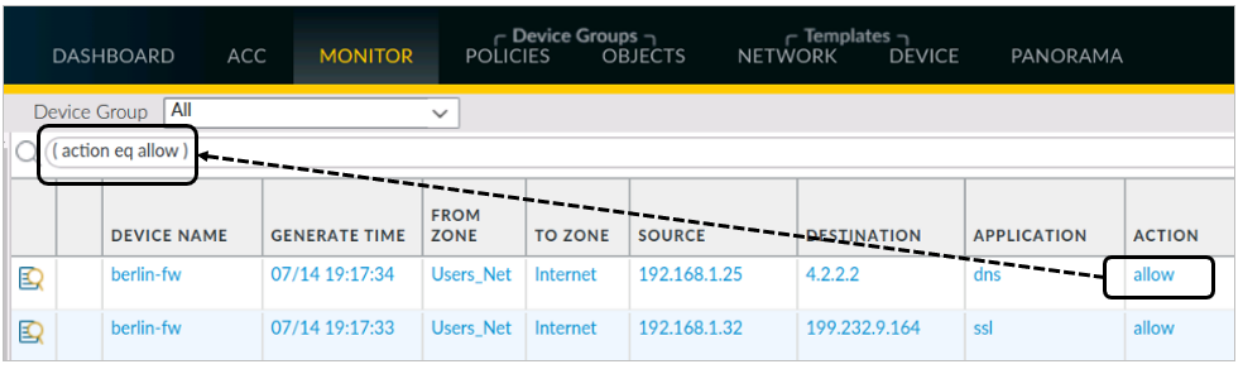
114. Allow this script to run until it completes.
115. Note that the URL scripts on client-A and client-b should still be running.

Examine the Traffic Log

Use a filter in the Traffic log on Panorama to verify that your firewalls are blocking dropbox.

116. In Panorama, navigate to **Monitor > Logs > Traffic**.
117. Select **All** from the **Device Group** drop-down list:

118. Clear any filters you may already have in place.
119. Click the link for **allow** under the **Action** column for the first entry in the table.
120. This action will create the syntax for a filter:

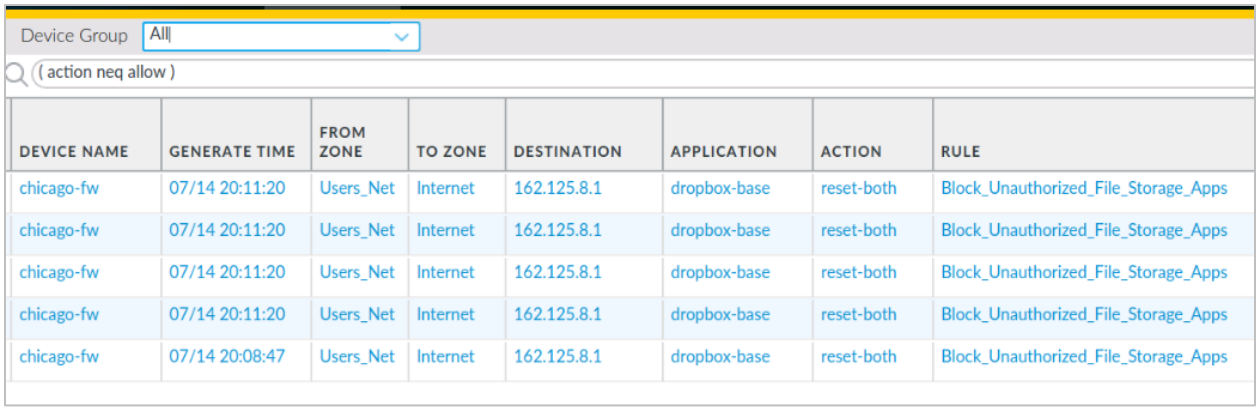


121. Modify the filter to look for entries in which the action is **not equal to allow**:

```
( action neq allow )
```

122. Click the **Apply** filter button:

123. Panorama displays a list of entries for sessions that have been blocked:



You also could filter the entries for dropbox-base as the application.

Examine the URL Filtering Log

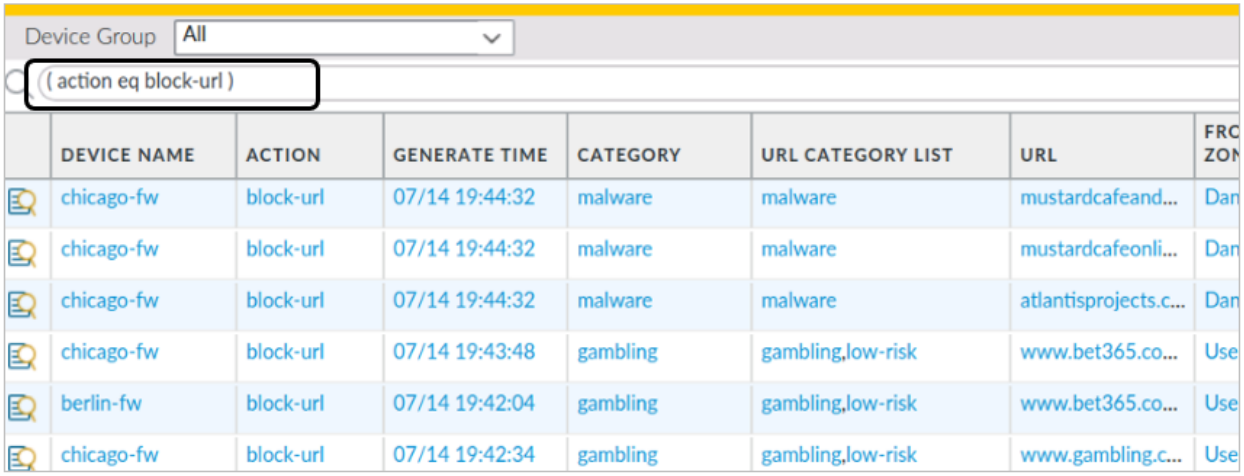
Use the URL Filtering log in Panorama to verify that your firewalls are blocking web browsing to inappropriate and dangerous website categories.

124. Navigate to **Monitor > Logs > URL Filtering**.
125. Drag and drop the **Action** column to the left side of the window between **Generate Time** and **Category**.
126. Set the **Device Group** drop-down list to **All**.
127. Clear any filters you have in place.
128. In the filter field, enter the following:

```
( action eq block-url )
```

As you use filters in log files, you will become more familiar with the syntax for creating and modifying filters. You always can save your filters or use the Filter Builder to create more advanced syntax based on your needs.

129. Click the **Apply Filter** button to see the results:



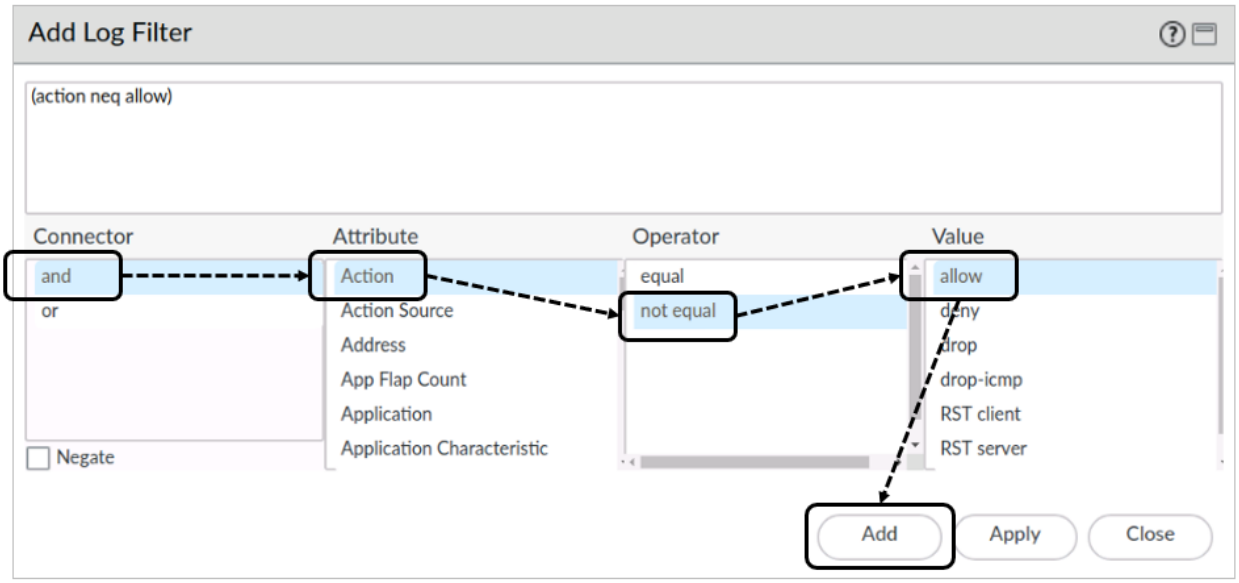
Create a Combined Filter

You can create filters that use a combination of fields. In this section, you will create a filter to view traffic that has not been allowed within the last 15 minutes.

130. In Panorama, select the **Dashboard** tab.
131. Under the **General** section at the bottom, note the current date and time:

132. Navigate to **Monitor > Logs > Traffic**.
133. Clear any filters you have in place.
134. Click the **Add Filter** icon in the upper-right corner of the window.
135. For **Connector**, select **and**.
136. For **Attribute**, select **Action**
137. For **Operator**, select **not equal**.
138. For **Value**, select **allow**.

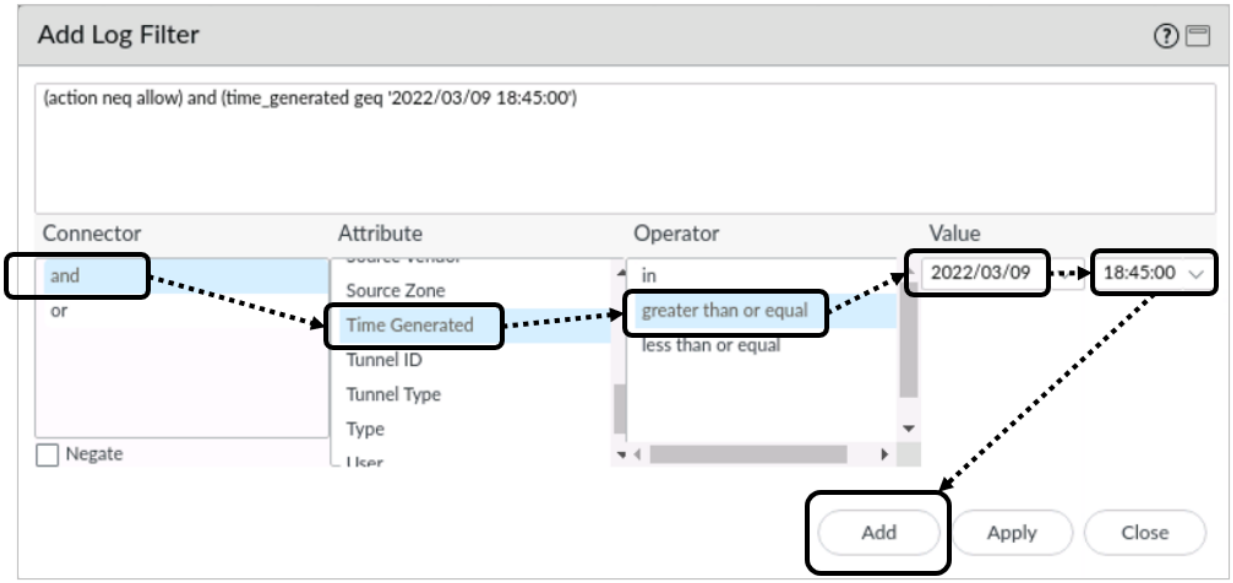
139. Click the **Add** button, but *do not* click **Apply** or **Close** yet:



140. In the same **Add Log Filter** window, click **and** in the **Connector** column.
141. For **Attribute**, scroll down and select **Time Generated**.
142. For **Operator**, select **greater than or equal**.
143. For **Value**, use the drop-down icon in the first section to select the current date (this example shows March 09, 2022).
144. Under the **Value**, use the drop-down icon in the second section to select a time about 15 minutes before your current time.
145. For example, if the current time in Panorama is 13:35, select the value of 13:15:

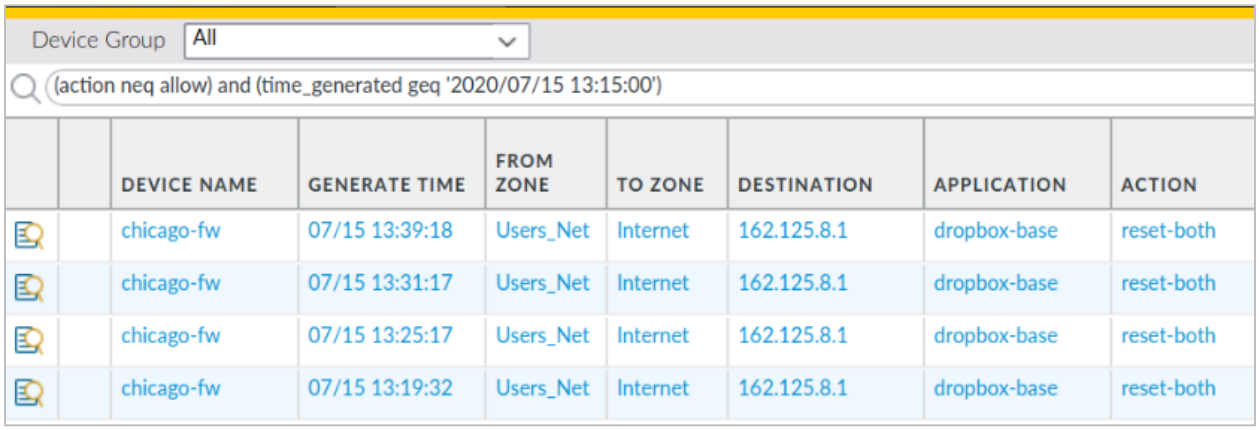
146. Click **Add**.

147. The Filter Build now displays the syntax for this combined filter:



148. Click **Apply**.

149. Click the **Apply Filter** button in the upper-right corner of the window:



		DEVICE NAME	GENERATE TIME	FROM ZONE	TO ZONE	DESTINATION	APPLICATION	ACTION
		chicago-fw	07/15 13:39:18	Users_Net	Internet	162.125.8.1	dropbox-base	reset-both
		chicago-fw	07/15 13:31:17	Users_Net	Internet	162.125.8.1	dropbox-base	reset-both
		chicago-fw	07/15 13:25:17	Users_Net	Internet	162.125.8.1	dropbox-base	reset-both
		chicago-fw	07/15 13:19:32	Users_Net	Internet	162.125.8.1	dropbox-base	reset-both

Lab Cleanup

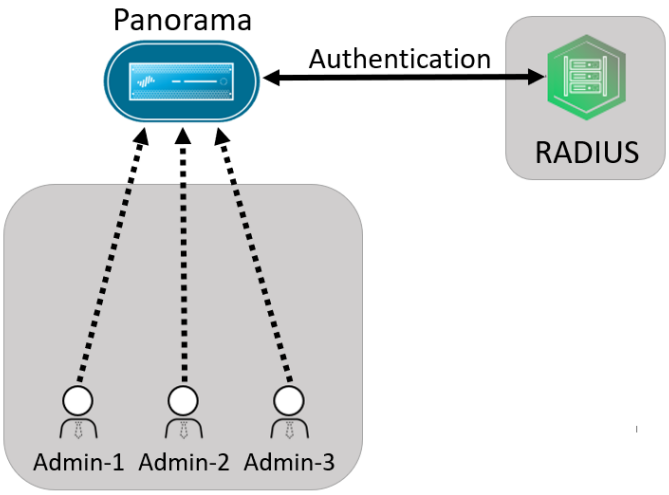
150. Select the Remmina connection for the **Berlin-Client**.
151. Use **Ctrl+C** to halt the script.
152. Type **`exit <ENTER>`** to close the SSH connection to the Berlin client host.
153. Select the Remmina connection for the **Server-Extranet** and type **`exit <ENTER>`** to close the SSH connection to the Extranet host.
154. On client-A, select the **Terminal Emulator** window.
155. Use **Ctrl+C** to halt the script.
156. The window should close, but if not, type **`exit <ENTER>`** to close the Terminal Emulator window.
157. Close any File Manager windows on the client-A host.
158. Close the Remmina Remote Desktop Client application window on client-A.

Stop. This is the end of the lab.

Lab 7 Scenario: Panorama Administration Accounts

In this lab, you will configure Panorama to authenticate administrators against a RADIUS server.

You will also examine and test Commit locks so that you can explain how to use them to other administrators who often will be working in Panorama simultaneously:



Lab Objectives

- Configure a RADIUS Server Profile and Authentication Profile
- Test the RADIUS Authentication Profile from the Panorama CLI
- Configure an Admin Role Profile
- Create an administrator account and assign the Admin Role Profile to it
- Configure and validate Administrator Accounts
- Use Commit Lock

High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-7-Start.xml** configuration file on Panorama.

Commit the Configuration

- Commit the configuration to Panorama.
- You do not need to push any configuration to the firewalls for this lab.

Configure a RADIUS Server Profile

Use the information below to create a Server profile for RADIUS that you will use later to authenticate accounts for access to Panorama and managed firewalls.

1. In the Panorama web interface, select **Panorama > Server Profiles > RADIUS**.
   The lab has a preconfigured RADIUS server running on 192.168.50.150.
2. Click **Add**, and then configure the RADIUS Server Profile using the following value:

Parameter	Value
Profile Name	`Panorama_RADIUS_Servers`
Server Settings Section	
Timeout	`3`
Retries	`3`
Authentication Protocol	**CHAP**
Server Section	
Name	`radius.panw.lab`
RADIUS Server	`192.168.50.150`
Secret	`Pal0Alt0!`

Create a RADIUS Authentication Profile

Use the information below to create a **RADIUS Authentication Profile**:

Parameter	Value
Authentication tab	
Name	**`RADIUS_Auth_Profile`**
Type	Select **RADIUS**
Server Profile	Select **Panorama_RADIUS_Servers**
Advanced tab	
Allow List	Click **Add** and then select **all**

Test the RADIUS Authentication Profile from Panorama CLI

- Connect to Panorama using the Remmina application.
- Use the following command to verify that Panorama can authenticate a network administrator using RADIUS:

```
test authentication authentication-profile RADIUS_Auth_Profile username adminHelga
password <ENTER>
```

- When prompted for **password**, enter **`Pal0Alt0!`**

Commit the Changes

- Commit the changes to Panorama.
    - You do not need to push any configuration changes to the managed firewalls.

Configure an Admin Role Profile

- Use the information below to create an **Admin Role Profile** called **`Intern`**:

Parameter	Value
Name	**`Intern`**
Role	**Panorama**
Description	**Access limited to Dashboard, ACC and Logs**
Web UI tab	In the **Web UI** column, set: • **Policies**: Mark all settings **disabled** (red) • **Objects**: Mark all settings **disabled** (red) • **Network**: Mark all settings **disabled** (red)

Parameter	Value
	• **Device**: Mark all settings **disabled** (red) • **Panorama**: Mark all settings **disabled** (red) • **Privacy**: Mark all settings **disabled** (red) • **Validate**: Mark all settings **disabled** (red) • **Save**: Mark all settings **disabled** (red) • **Commit**: Mark all settings **disabled** (red) • **Tasks**: Mark all settings **disabled** (red) • **Global**: Mark all settings **disabled** (red)
XML API tab	Verify that all objects are **disabled** (red)
Command Line tab	Verify that **None** is selected
REST API tab	Set all objects to **disabled** (red)
Plugins	Mark the setting **disabled** (red)

Configure an Administrator Account

- Create a new administrator account using the information below:

Parameter	Value
Name	**`internBob`**
Authentication Profile	**RADIUS_Auth_Profile**
Administrator Type	**Custom Panorama Admin**
Profile	Select **Intern**

Commit the Changes

- Commit the changes to Panorama.
    - You do not need to push any configuration changes to the managed firewalls.

Validate Administrator Access

- Log out of Panorama.
- Log back in using **`internBob/Pal0Alt0!`** as the credentials.
- Use the **System Log** in Panorama to examine events that show the **`internBob`** account being authenticated.
- Log out of Panorama.
- Log back into Panorama using the **`admin/Pal0Alt0!`** credentials.

Use Commit Lock

- Create two new administrator accounts using the information below:

Parameter	Value
Name	**admin-1**
Authentication Profile	**None**
Password	**Pal0Alt0!**
Confirm Password	**Pal0Alt0!**

Parameter	Value
Name	**admin-2**
Authentication Profile	**None**
Password	**Pal0Alt0!**
Confirm Password	**Pal0Alt0!**

- Commit the changes to Panorama only.
- Log out of Panorama.
- Log in with **admin-1/Pal0Alt0!**
- Take a **Configuration Lock**.
- Use the information below for the Configuration Lock.

Parameter	Value
Type	**Config**
Location	**All Configuration**
Comments	**<Your Initials> - Working on Sec Profiles. Will be done by noon PDT.**

- Log out of Panorama.
- Log in to Panorama with the **admin-2/Pal0Alt0!** Credentials.
- Attempt to create a new **Address Object** called **DNS** with a **Type** of **IP Netmask** and a value of **4.2.2.2**
- Note the message you receive when you attempt to create this entry.
- While logged in as admin-2, examine the **Lock** that admin-1 took.
- Log out of Panorama.
- Log back in as **admin-1**.

- Modify the **Login Banner** for Panorama to include **`Access attempts logged`**
- Commit your changes to Panorama.
    - Note that Panorama removes your lock automatically when you commit your changes.

Detailed Lab Steps

Load the Lab Start Configuration File

1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-7-Start.xml**.
4. Leave the remaining settings unchanged.
5. Click **OK**.

Commit the Configuration

6. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
7. When the **Commit to Panorama** window appears, click **Commit**.
8. Monitor the status of the commit.
9. When the commit status is complete, click **Close**.

Note that you do not need to push any configurations to the firewall. This lab describes administrative accounts and authentication for Panorama.

Configure a RADIUS Server Profile

In this section, you will define a Server Profile for RADIUS that you will use later to authenticate accounts for access to Panorama and managed firewalls.

10. In the Panorama web interface, select **Panorama** > **Server Profiles** > **RADIUS**.
    The lab has a preconfigured RADIUS server running on 192.168.50.150.
11. Click **Add**, and then configure the RADIUS Server Profile using the following value:

Parameter	Value
Profile Name	`Panorama_RADIUS_Servers`

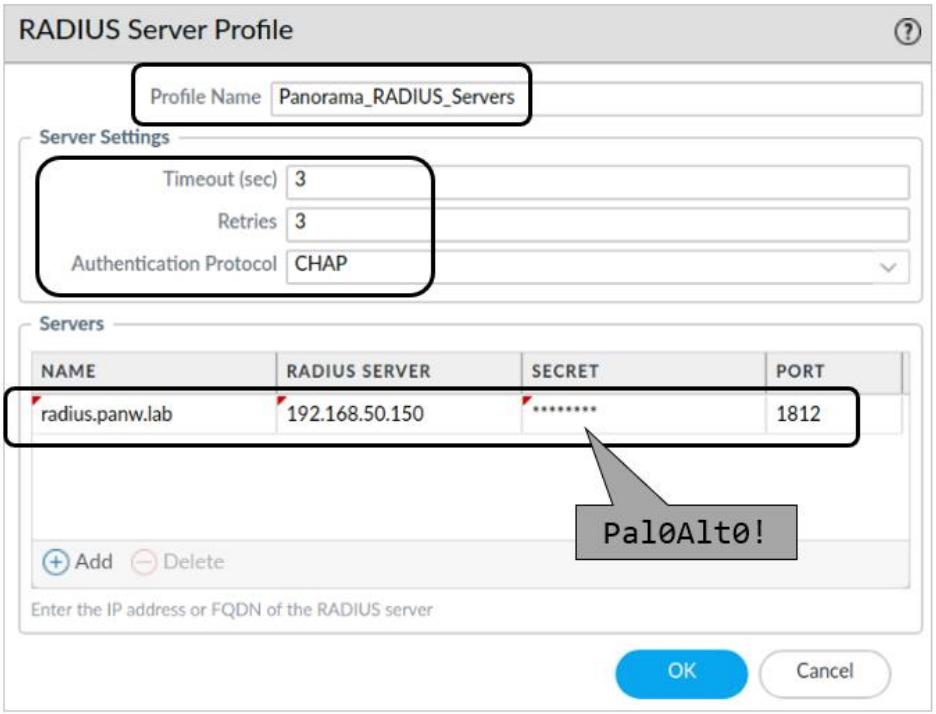
12. Under the **Server Settings**, configure the following:

Parameter	Value
Timeout	`3`
Retries	`3`
Authentication Protocol	**CHAP**

13. Under the **Servers** section, click **Add** and configure the following.

Parameter	Value
Name	`radius.panw.lab`
RADIUS Server	`192.168.50.150`
Secret	`Pal0Alt0!`

14. Leave the remaining settings unchanged:

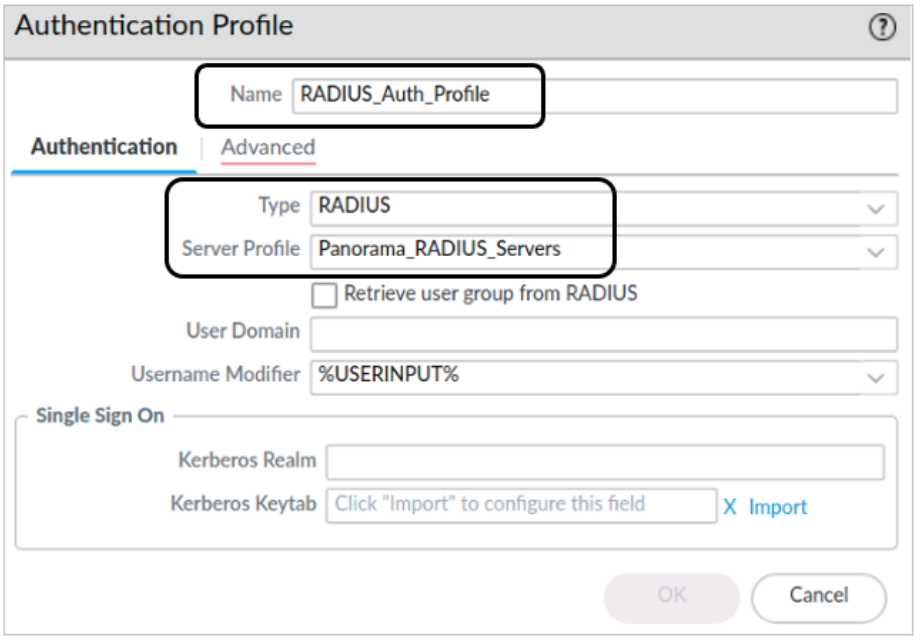


15. Click **OK**.

Create a RADIUS Authentication Profile

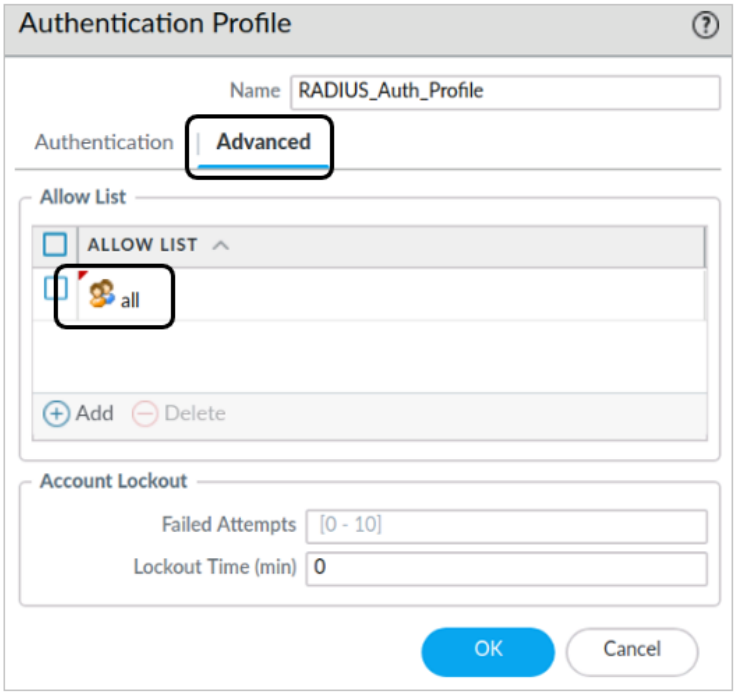
16. Under **Panorama > Authentication Profile**, click **Add**.
17. Create an **Authentication Profile** using the following values:

Parameter	Value
Authentication tab	
Name	`RADIUS_Auth_Profile`
Type	Select **RADIUS**
Server Profile	Select **Panorama_RADIUS_Servers**



18. Leave the remaining settings unchanged.
19. Select the **Advanced** tab.
20. Under the **Allow List**, click **Add**.
21. Select **All**.

22. Leave the remaining settings unchanged:



23. Click **OK**.

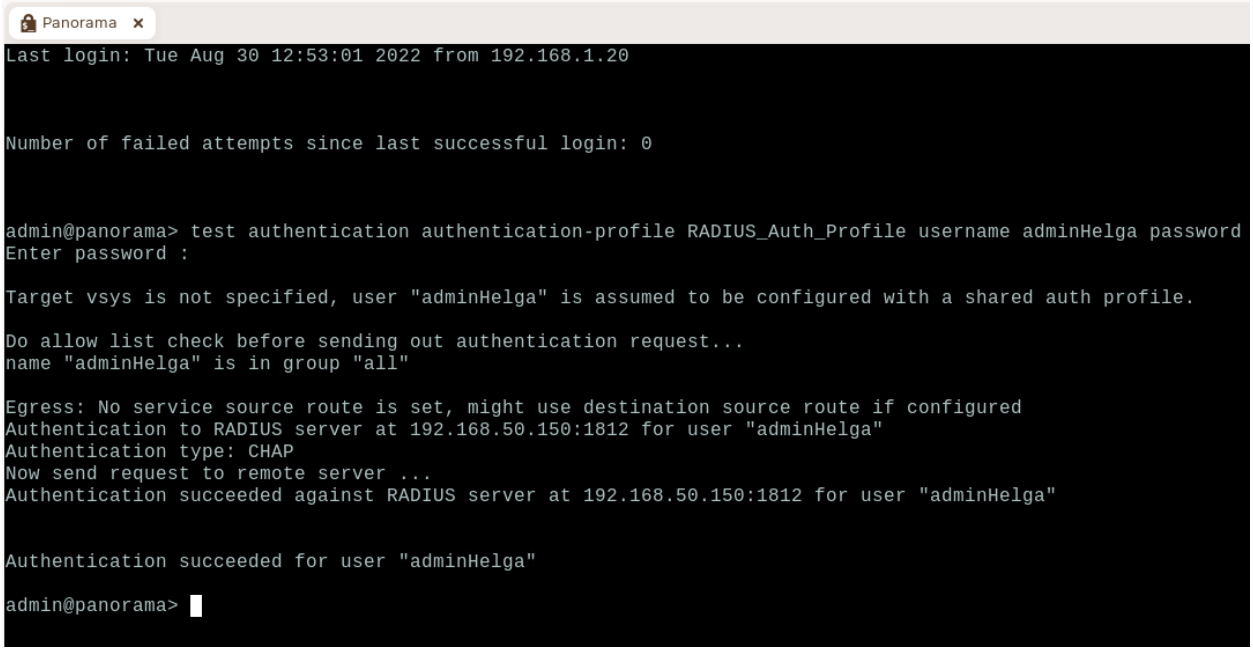
Test the RADIUS Authentication Profile from Panorama CLI

Before you commit the configuration to Panorama, you can use a test command from the CLI to verify the RADIUS authentication.

24. On the client-A Desktop, use the Remmina application to connect to the Panorama CLI.
25. Enter the following command to verify that Panorama can authenticate a network administrator using RADIUS:

```
test authentication authentication-profile RADIUS_Auth_Profile username adminHelga
password <ENTER>
```

26. Enter **`Pal0Alt0!`** when prompted for password.

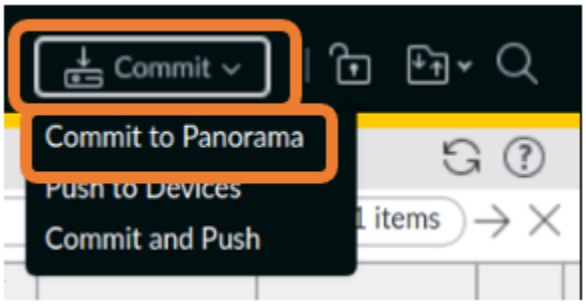


The adminHelga account was preconfigured in the lab RADIUS server.

27. Note the message **`Authentication succeeded for user “adminHelga”`**.
28. This message indicates that you have correctly configured the RADIUS Server Profile and RADIUS Authentication Profile.
29. Type **`exit <ENTER>`** to close the connection to Panorama.
30. Close the Remmina application window.

Commit the Changes

31. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



32. Click **Commit**.

33. Monitor the status of the commit.
34. When the commit status is complete, click **Close**.

You only made changes to Panorama in the previous section, so you do not need to push any configuration changes to the managed firewalls.

Configure an Admin Role Profile

As your company has grown, you have added more network administrators to your team. However, not all administrators are equally proficient. To avoid inadvertent resume-generating mistakes for you and other team members, you want to define sets of permissions that you can apply to administrators, based on their experience level and responsibilities.

In this section, you will define **Admin Role Profiles** that contain permissions for access to Panorama configuration options. With your Admin Role Profiles in place, you can assign individual administrator accounts to a specific Admin Role Profile so that an administrator will have the permissions applied through the Role Profile.

In this section, you will create an admin role profile called **Intern**. You will define this role so that any administrator account assigned to it will have limited access to the Panorama configuration but will be able to examine logs, the **Dashboard**, and the **ACC**.

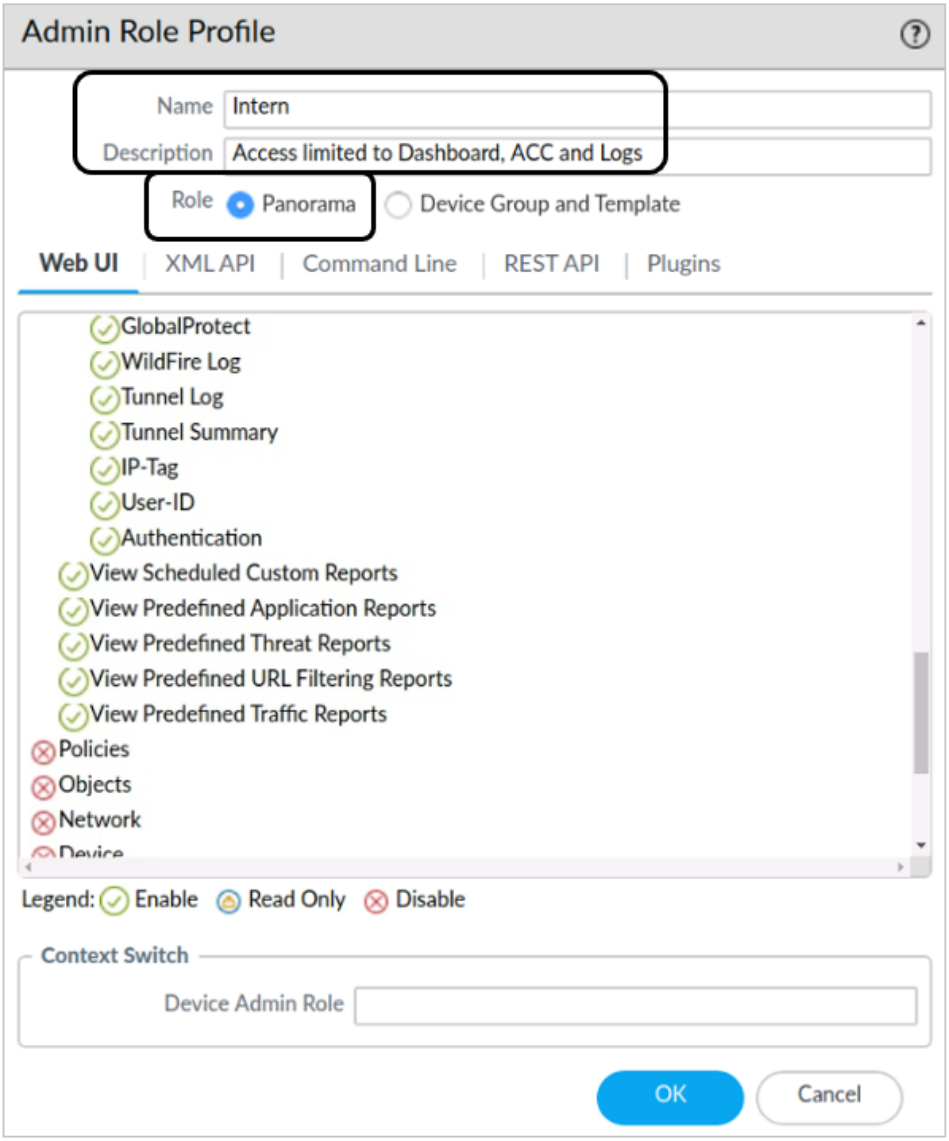
35. Select **Panorama** > **Admin Roles**.
36. Click **Add**, and then create an Admin Role Profile using the information in the following table.

Note that you can change the access level of an item by directly clicking the icon beside it.

Parameter	Value
Name	`Intern`
Description	**Access limited to Dashboard, ACC and Logs**
Role	**Panorama**
Web UI tab	In the **Web UI** column, set: • **Policies**: Mark all settings **disabled** (red) • **Objects**: Mark all settings **disabled** (red) • **Network**: Mark all settings **disabled** (red) • **Device**: Mark all settings **disabled** (red)

Parameter	Value
	• **Panorama**: Mark all settings **disabled** (red) • **Privacy**: Mark all settings **disabled** (red) • **Validate**: Mark all settings **disabled** (red) • **Save**: Mark all settings **disabled** (red) • **Push All Changes**: Mark all settings **disabled** (red) • **Commit**: Mark all settings **disabled** (red) • **Tasks**: Mark all settings **disabled** (red) • **Global**: Mark all settings **disabled** (red)
XML API tab	Verify that all objects are **disabled** (red)
Command Line tab	Verify that **None** is selected
REST API tab	Set all entries to **disabled** (red)
Plugins	Mark the setting **disabled** (red)

37. Verify your settings as shown in the following screenshot:



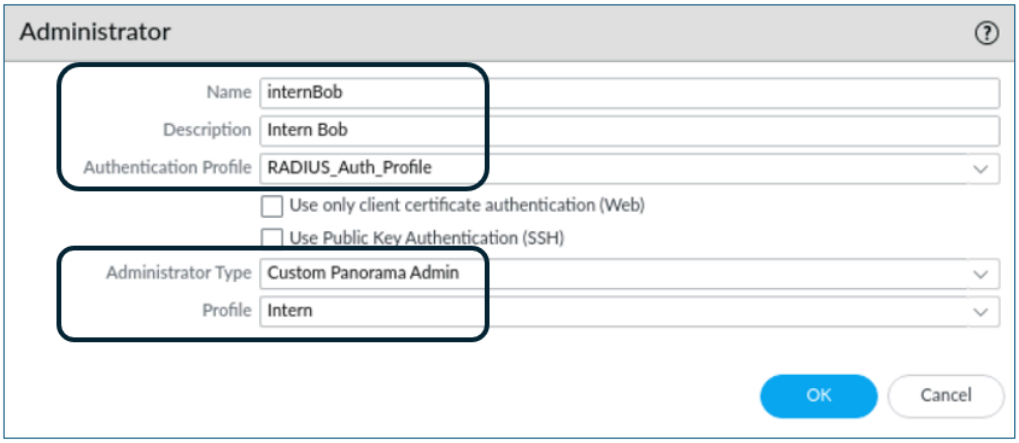
38. Click **OK** to close the **Admin Role Profile** configuration window.

Configure an Administrator Account

In this section, you will create an administrator account called **internBob** and assign it to the **Intern** Administrator Role Profile. Someone who logs in with the credentials for this account will have restricted access to elements of the Panorama web interface. This account also will use the **RADIUS_Auth_Profile**.

39. From the web interface, select **Panorama** > **Administrators**.
40. Click **Add**, and then create an Administrator account using the following values:

Parameter	Value
Name	**`internBob`**
Description	**Intern Bob**
Authentication Profile	**RADIUS_Auth_Profile**
Administrator Type	**Custom Panorama Admin**
Profile	Select **Intern**

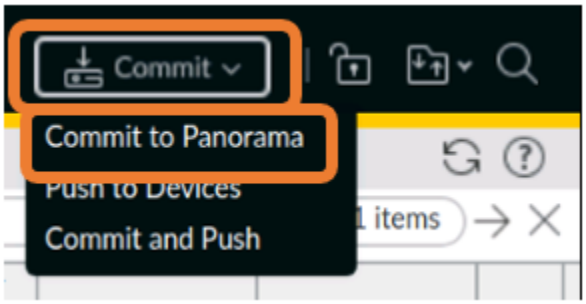


An account for internBob was preconfigured on the RADIUS server in the lab environment.

41. Click **OK** to close the **Administrator** configuration window.

Commit the Changes

42. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



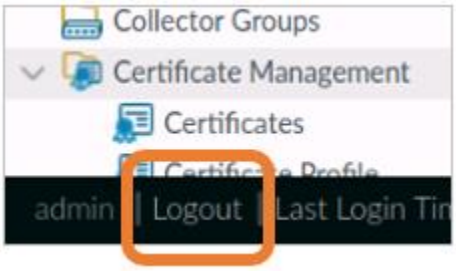
43. Click **Commit**.
44. Monitor the status of the commit.
45. When the commit status is complete, click **Close**.

You only made changes to Panorama in the previous section, so you do not need to push any configuration changes to the managed firewalls.

Validate Administrator Access

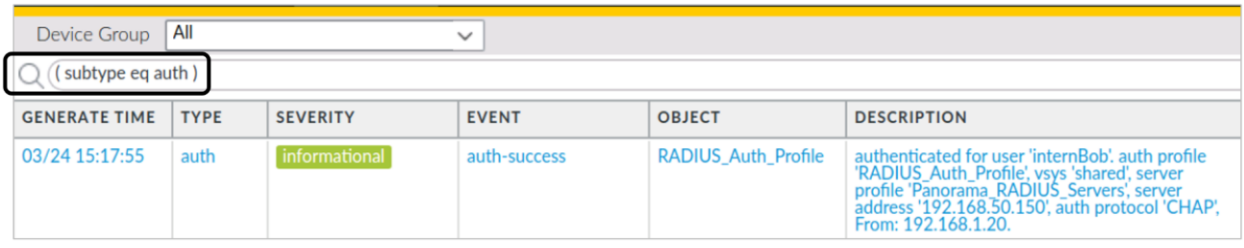
In this section, you will validate access for the administrator account **internBob**.

46. In the Configuration browser, click the **Logout** button in the bottom-left corner of Panorama:



47. Log in to Panorama with **`internBob`** as the **Username** and **`Pal0Alt0!`** as the **Password**.
48. Close the Welcome window if one appears.
49. Click **OK** if the Telemetry Data Collection window appears.
50. Note that only a subset of tabs are shown based on the settings for the Intern Admin Role Profile.
51. Check the **System** log to verify that the **internBob** account was authenticated against the RADIUS Profile by selecting the **Monitor** tab.
52. Select **All** from the **Device Group** drop-down list at the top of the window:

53. Select **Logs** > **System**.
54. In the filter field, enter **`( subtype eq auth )`** and press **Enter**.
55. You can see an **auth-success** event along with the details for internBob:



56. Log out of Panorama by clicking the **Logout** button in the bottom-left of the web interface.

57. Log back into Panorama using **`admin/Pal0Alt0!`** credentials.

Use Commit Lock

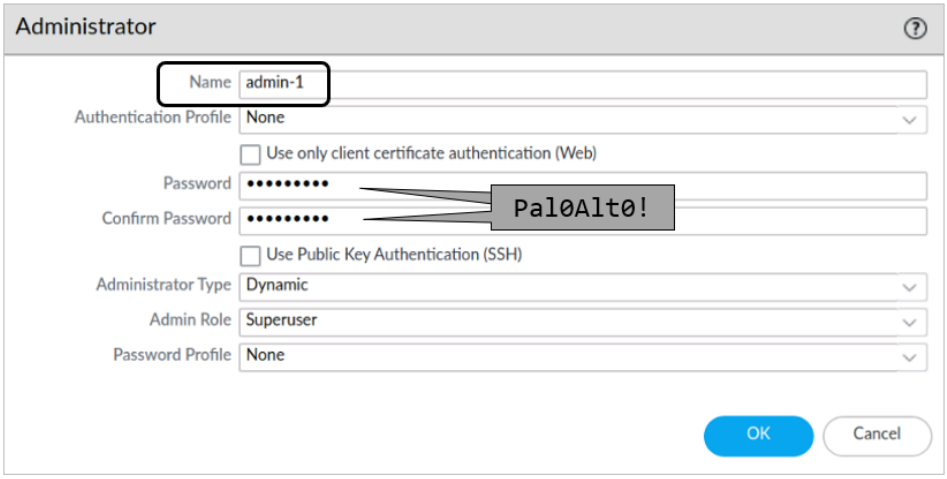
If two administrators are simultaneously making changes in Panorama and then commit at the same time, Panorama will queue these changes in the order it receives them. This behavior means that Admin-1 might make changes and commit them. Admin-2 might undo those changes when the changes are committed.

To prevent this kind of problem, administrators can employ a **Configuration Lock** or a **Commit Lock** (or both at the same time).

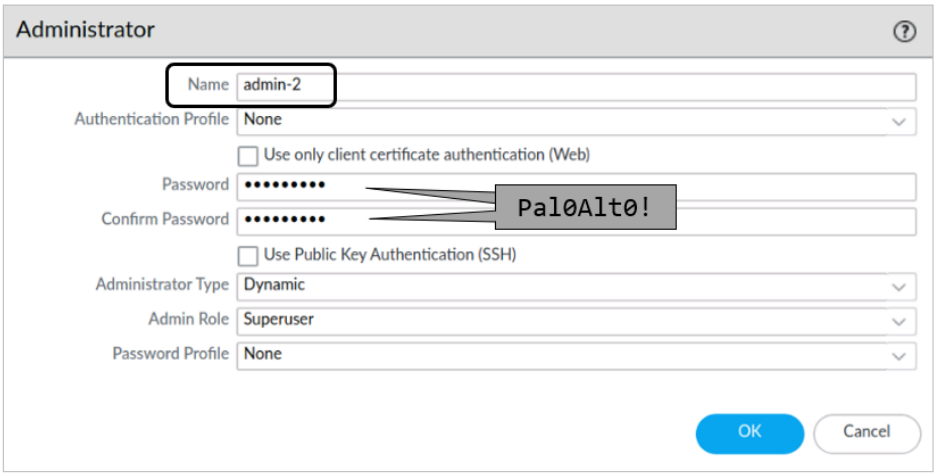
In this section, you will create two new admin accounts (**admin-1** and **admin-2**). Both administrator accounts will have full read/write access to Panorama and all managed firewalls.

You will log in as admin-1, take a **Config Lock**, and then log out. You will log in as admin-2 and try to make a change to see the effect a **Config Lock** has.

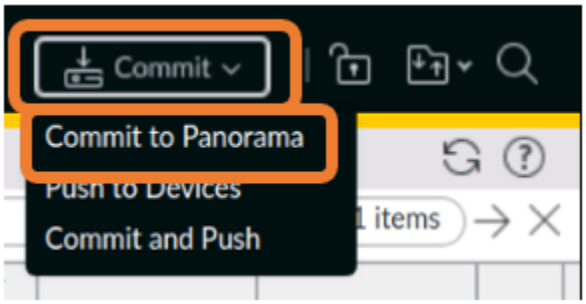
58. While you are logged in to Panorama as admin, select **Panorama** > **Administrators**.
59. Click **Add**.
60. Create a new Administrator called **admin-1** with **`Pal0Alt0!`** as the **Password**.
61. Set the **Administrator Type** to **Dynamic**.
62. Set the **Admin Role** to **Superuser**.
63. Leave the Password Profile set to **None**:



64. Click **OK**.
65. Click **Add** again and create another new **Administrator** called **admin-2**, also with **`Pal0Alt0!`** as the **Password**.
66. Set the **Administrator Type** to **Dynamic**.
67. Set the **Admin Role** to **Superuser**.
68. Leave the **Password Profile** set to **None**:



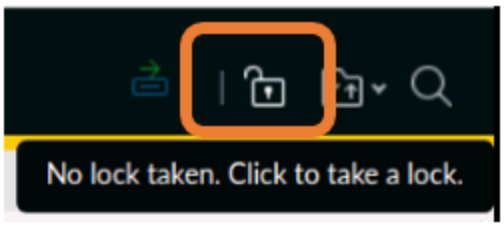
69. Click **OK**.
70. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



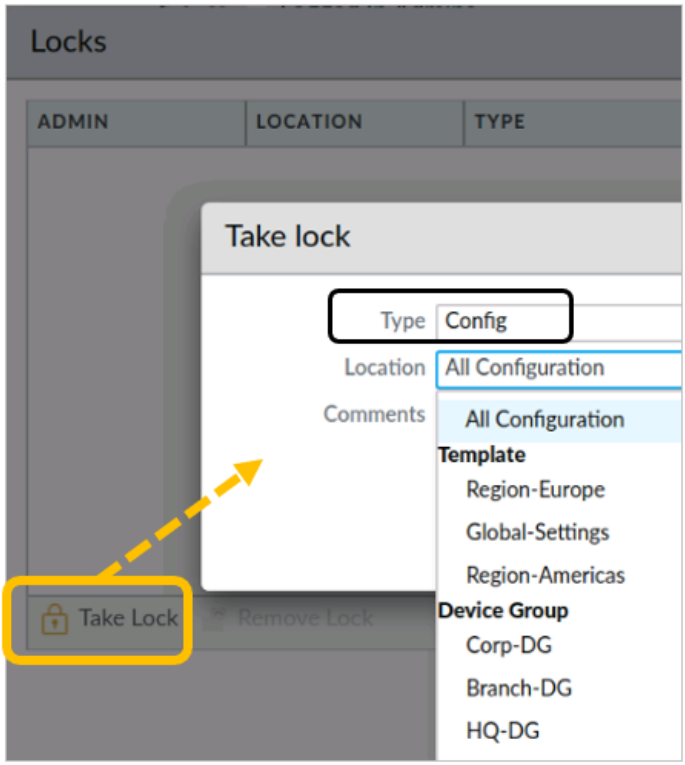
71. Click **Commit**.
72. Monitor the status of the commit.
73. When the commit status is complete, click **Close**.

You only made changes to Panorama in the previous section, so you do not need to push any configuration changes to the managed firewalls.

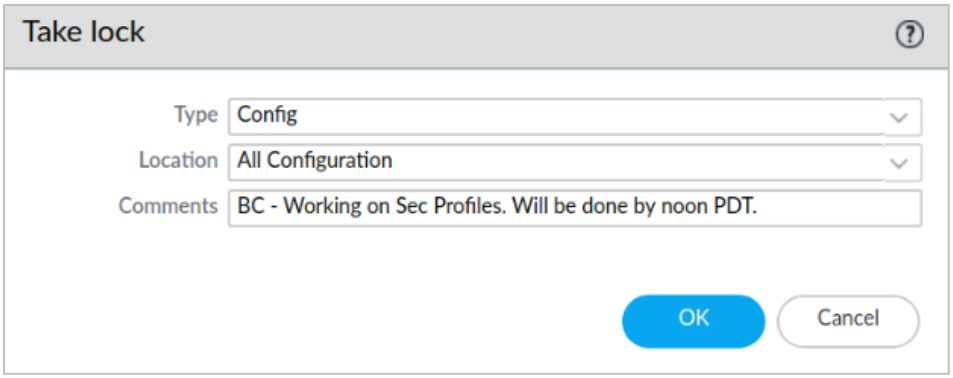
74. Log out of Panorama by clicking the **Logout** link in the bottom-left corner of the interface.
75. Log in with **`admin-1`** as the **Username** and **`Pal0Alt0!`** as the **Password**.
76. Close the **Welcome** window if one appears.
77. Click **OK** if the Telemetry Data Collection window appears.
78. Take a **Configuration Lock** by clicking the **padlock** icon in the upper-right corner of the window:



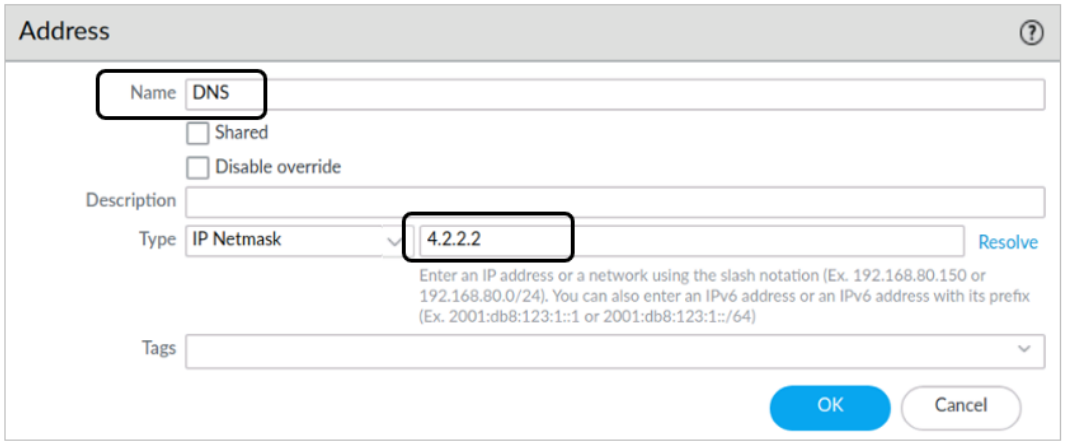
79. In the **Locks** window, click the **Take Lock** button in the bottom-left corner.
80. Change the **Type** to **`Config`**.
81. Leave the **Location** drop-down list set to **All Configuration**, but click the arrow for the field to see that you can select different aspects of the configuration to lock:



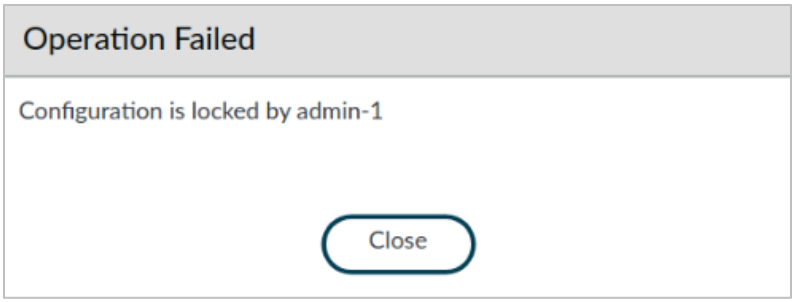
82. For **Comments**, enter your initials and a short message that would let other administrators know why you have locked the configuration:



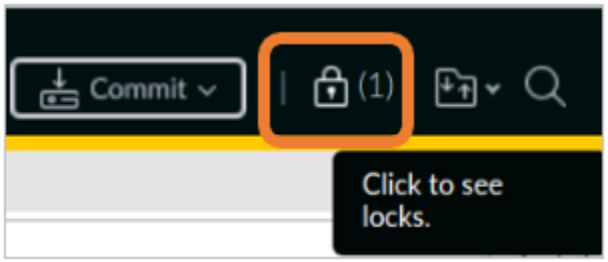
83. Click **OK** on the **Take lock** window.
84. Click **Close** on the **Locks** window.
85. Notice that you do not have to commit your changes to Panorama when you take a config or commit lock.
86. Log out of Panorama.
87. Log back in to Panorama with **`admin-2`** as the **Username** and **`Pal0Alt0!`** as the **Password**.
88. Close the **Welcome** window if one appears.
89. Click **OK** if the Telemetry Data Collection window appears.
90. Attempt to create a new configuration element by navigating to **Objects** > **Addresses**.
91. Select **Corp-DG** from the **Device Group** drop-down list.
92. Click **Add**.
93. For **Name**, enter **`DNS`**.
94. Leave **Type** set to **IP Netmask** and enter **`4.2.2.2`**:



95. Click **OK**.
96. Note the message you receive indicating that another administrator has locked the configuration:



97. Click **Close** on the **Operation Failed** message.
98. Click **Cancel** in the **Address** window.
99. Click the **locked padlock** icon in the upper-right corner:



Note that the icon is a closed padlock with a small number next to it, which indicates that another administrator has taken a lock of some type.

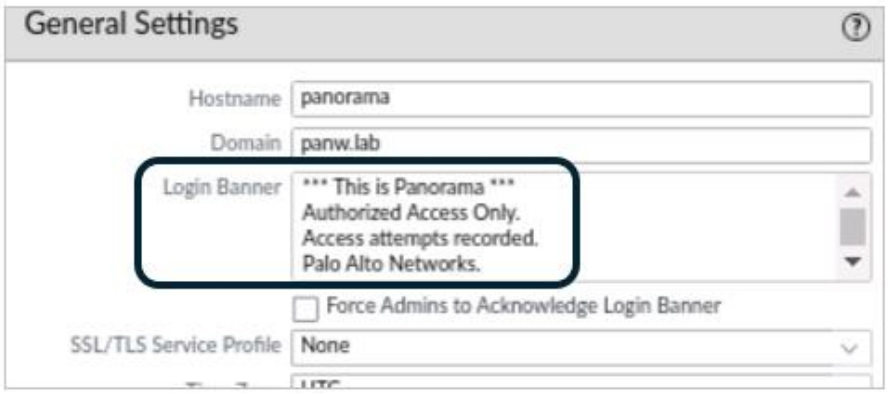
If you work with multiple administrators, always check the padlock icon before you begin making changes.

100. The **Locks** window shows you who has taken the lock, when they took it, and any comments they have entered:

A superuser can remove a lock that someone else has put in place; however, this practice somewhat defeats the purpose of locking a configuration.

A better operating procedure would be to contact the admin who took the lock rather than take it away without informing the admin.

101. Click **Close**.
102. Log out of Panorama.
103. Log in using **`admin-1`** as the username and **`Pal0Alt0!`** as the password.
104. Close the **Welcome** screen if one appears.
105. Click **OK** if the Telemetry Data Collection window appears.
106. Make a slight change to the **Login Banner** under **Panorama** > **Setup** > **Management** > **General Settings** by adding **`Palo Alto Networks`** to the end of the message:



107. Click **OK**.
108. Note that you are not blocked from making this change because you are logged in with the admin-1 account that took the Configuration Lock.
109. Click **Commit** > **Commit to Panorama**.
110. Click **Commit**. The commit should succeed.
111. After the successful commit, check the status of the lock icon at the top-right of the screen. It should be open (unlocked):

112. Click the **Lock** icon and note that no **Locks** are in place.

If you take a Configuration Lock or Commit Lock and commit your changes, Panorama automatically releases the lock and removes the entry from the Lock window.

113. Log out of Panorama and log back in with the **`admin/Pal0Alt0!`** account.

Stop. This is the end of the lab.

Lab 8 Scenario: Reporting

Your manager frequently will ask you for a report with details about firewall activity in the last few hours.

In the past, she has asked you to provide an immediate report about the following:

- Threats within the last 24 hours

You need to create a custom report that you can run at any time to provide your manager with this kind of information.

She also has asked you to provide weekly reports about the following:

- Application in use
- Blocked URL Categories

You need to verify that these reports are emailed to your manager once per week.

Lab Objectives

- Generate traffic through both firewalls
- Create a Custom Report for threats within the last 24 hours
- Create a Custom Report for Applications used within the last 7 days
- Create a Custom Report for URL Categories blocked within the last 7 days
- Create a Weekly Report Group
- Create an email schedule to send out weekly reports

High-Level Lab Steps

Load the Lab Start Configuration File

- Load and commit the **EDU-220-11.1a-Lab-8-Start.xml** configuration file on Panorama.

Commit the Configuration

- Commit the configuration to Panorama.

Push Configuration to Firewalls

- Push the Device Group and Template changes to the firewalls using **Force Template Values**

Generate Traffic Through Firewalls

- Use Remmina to connect to the Berlin-Client.
- Change the directory:
  cd /home/lab-user/Desktop/Lab-Files/EDU-220/ <ENTER>
- Launch the **b-url-traffic.sh** script:
  ./b-url-traffic.sh <ENTER>
- Allow the script to run uninterrupted.
- Use Remmina to connect to the Extranet-Server.
- Launch the **UsingLogs-V1.sh** script:
  ./ UsingLogs-V1.sh <ENTER>
- Allow this script to run until it completes (about ten minutes).

Create a Custom Report for Threats Within the Last 24 Hours

- Use the information below to create a **Custom Report** to display threats over the last 24 hours:

Parameter	Value
Name	**Threats Last 24 Hours**
Description	**Provides details about threats detected in 24 hours**
Database	**Threat (**Under **Summary Databases - Remote Device Data)**
Schedule	**Unchecked**
Time Frame	**Last 24 Hrs**

Parameter	Value
Sort By	**Count (Top 10)**
Group By	**Severity (10 Groups)**
Selected Columns	**Threat ID/Name** **Action**

- Use the **Run Now** option to display the results before saving the report.
- Export the report results to PDF.
- Open the report in the browser to view the details in PDF format.

Create a Custom Report for Applications Used Within the Last 7 Days

- Use the information below to create a **Custom Report** to display Applications that the firewall has identified over the last 7 days:

Parameter	Value
Name	**Apps Identified in Last 7 Days**
Description	**Provides details about Apps identified in last 7 days**
Database	**Traffic (**Under **Summary Databases – Panorama Data)**
Schedule	**Unchecked**
Time Frame	**Last 7 Days**
Sort By	**Bytes (Top 100)**
Group By	**Device Name (10 Groups)**
Selected Columns	**Application** **Bytes** **Action**

- Use the **Run Now** option to display the results before saving the report.
- Export the report results to PDF.
- Open the report in the browser to view the details in PDF format.

Create a Custom Report for URL Categories Blocked within the Last 7 Days

- Use the information below to create a **Custom Report** to display URL categories that the firewall has blocked over the last seven days:

Parameter	Value
Name	**URLs Blocked in Last 7 Days**
Description	**Provides details about URLs blocked in last 7 days**
Database	**URL (Under Detailed Logs (Slower) – Panorama Data)**
Schedule	**Unchecked**
Time Frame	**Last 7 Days**
Sort By	**Count (Top 100)**
Group By	**Device Name (10 Groups)**
Selected Columns	**Action** **URL Category List** **Category** **URL**
Query Builder	**(action eq block-url)**

- Use the **Run Now** option to display the results before saving the report.
- Export the report results to PDF.
- Open the report in the browser to view the details in PDF format.

Create a Weekly Report Group

- Use the information below to create a Report Group:

Parameter	Value
Name	**Weekly Reports**
Title Page	**Unchecked**
Title	**<blank>**
Predefined Reports	**Top Applications** **Top blocked URL user behavior**
Custom Reports	**Apps Identified in Last 7 Days** **URLs Blocked in Last 7 Days**

Create an Email Schedule

- Use the information below to create an **Email Schedule** to send your **`Weekly Reports`** out:

Parameter	Value
Name	**`Weekly Reports`**
PDF Report or Report Group	**`Weekly Reports`**
Email Profile	**`Panorama-Email`**
Recurrence	**`Every Monday`**

Commit the Changes to Panorama

- Commit the changes to Panorama.

Lab Cleanup

- Stop the traffic script on client-B and close the Remmina connection to client-B.
- Use **`exit`** to close the Remmina connection to the Extranet-Server.
- Close the Remmina Remote Desktop Client window.

Detailed Lab Steps

Load the Lab Start Configuration File

1. In the Panorama web interface, navigate to **Panorama** > **Setup** > **Operations**.
2. Select **Setup** > **Operations**.
3. Click **Load named Panorama configuration snapshot**.
4. Use the drop-down list for **Name** to select **EDU-220-11.1a-Lab-8-Start.xml**.
5. Leave the remaining settings unchanged.
6. Click **OK**.

Commit the Configuration

7. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**.
8. When the **Commit to Panorama** window appears, click **Commit**.
9. Monitor the status of the commit.
10. When the commit status is complete, click **Close**.

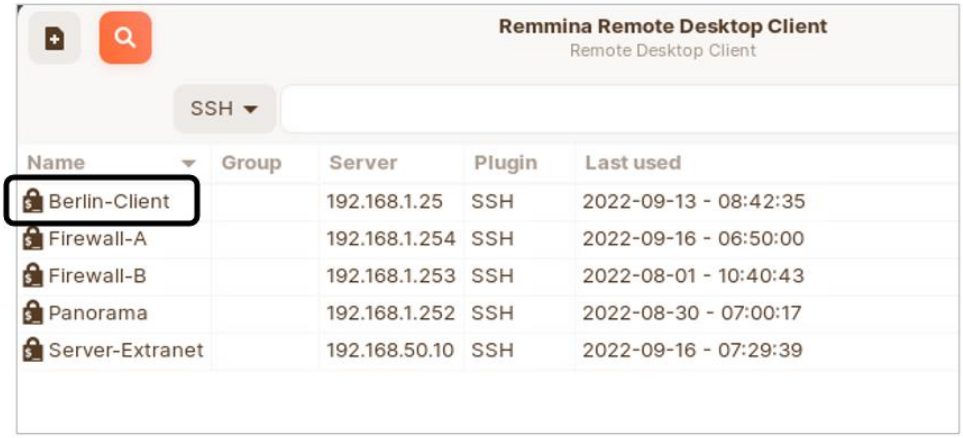
Push Configuration to Firewalls

11. Select **Commit** > **Push to Devices**.
12. Click **Edit Selections**.
13. Select the **Device Groups** tab and verify that the check boxes for the **berlin-fw** firewall and the **chicago-fw** firewall are selected.
14. Select the **Force Template Values** check box at the bottom.
15. Click **Yes** on the **Force Template Values** warning message.
16. On the **Templates** tab, check the check boxes for the Chicago firewall and the Berlin firewall.
17. Click **OK**.
18. Click **Push** to start the process.
19. Wait until the **Commit All** jobs are complete.
20. Click **Close**.

Generate Traffic Through Firewalls

21. On the client-A host, open the Remmina application by double-clicking the icon on the Desktop:

22. In the Remmina Remote Desktop Client window, double-click the entry for **Berlin-Client**:



This application will connect you to the Berlin workstation through SSH.

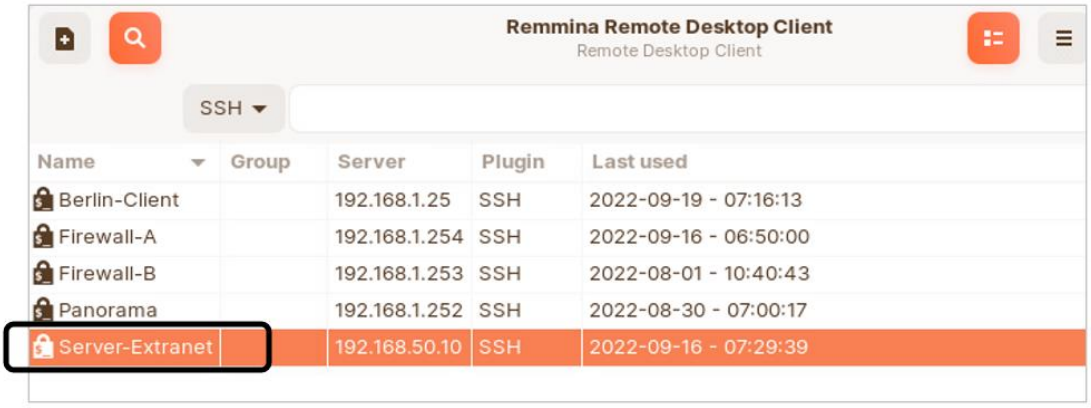
23. Launch the b-url-traffic.sh script:

```
./b-url-traffic.sh <ENTER>
```

The script generates various URL requests from Users in Berlin to the Internet and to the Extranet security zones.

Some portions of the script will generate errors in the output. These errors are expected and do not affect the outcome of the lab.

24. The script will loop continuously, and you should allow it to run uninterrupted until the end of this lab.
25. In the Remmina Remote Desktop Client window, double-click the entry for **Server-Extranet**:



This application will connect you to the Extranet server through SSH.

26. Remmina will establish an SSH connection to the Extranet server.

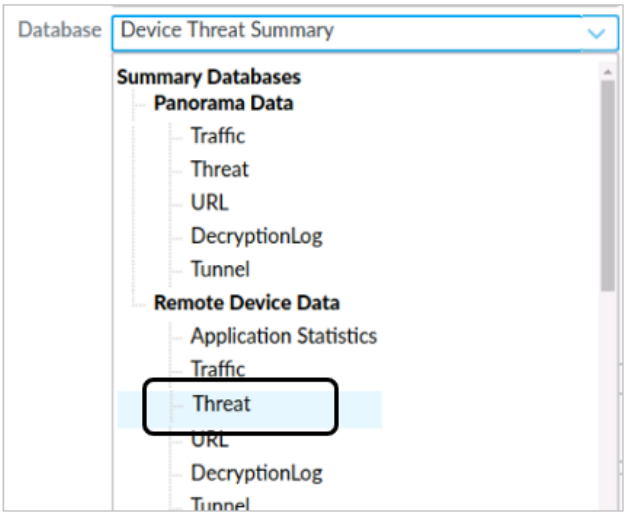
27. Launch the traffic generating script:
    `./UsingLogs-V1.sh <ENTER>`
    This script runs simulated application traffic through the Chicago firewall.
28. Press **`<ENTER>`** again to start the script.
29. Allow this script to run until it completes. The process takes about 10 minutes.
30. You can continue to the next section of this lab while the script runs.

Create a Custom Report for Threats Within the Last 24 Hours

In this section, you will create a new Custom Report that you can run when your manager asks you for information about threats within the last day.

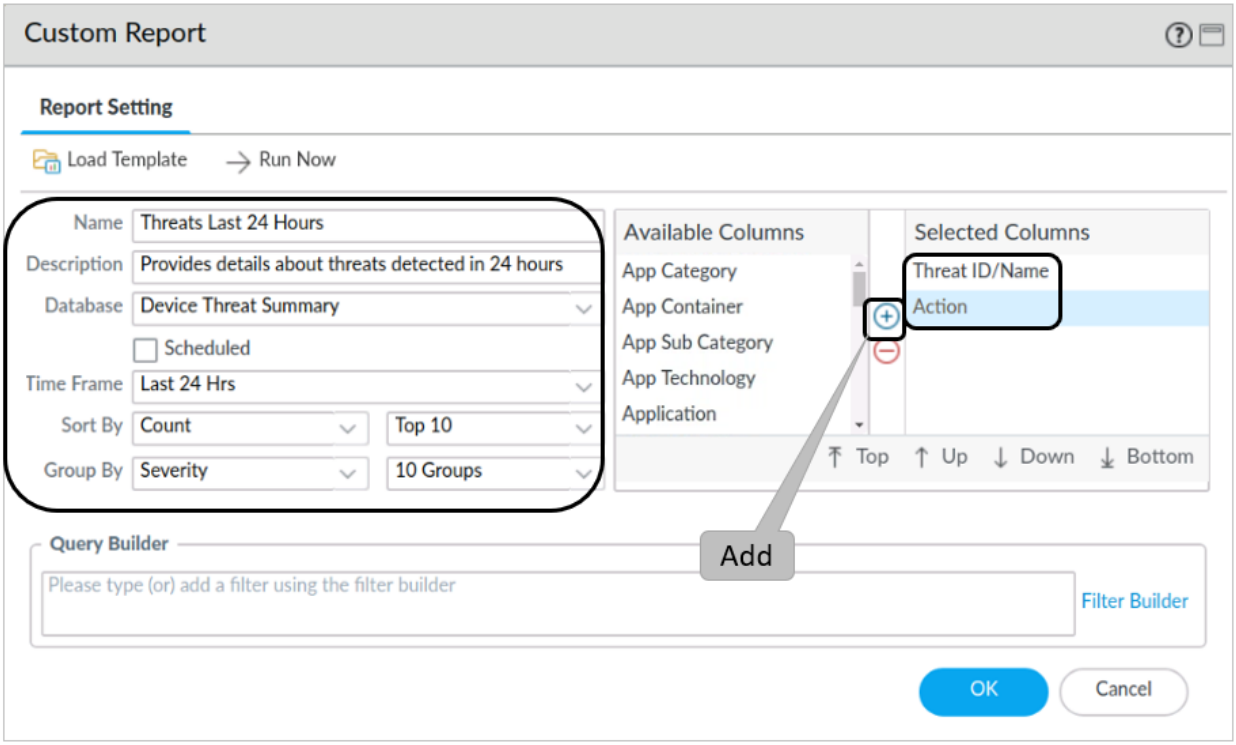
31. In the Panorama web interface, navigate to **Monitor** > **Manage Custom Reports**.
32. Select **All** from the **Device Group** drop-down list:

33. Click **Add**.
34. For **Name**, enter **`Threats Last 24 Hours`**.
35. For **Description**, enter **`Provides details about threats detected in 24 hours`**.
36. For **Database**, use the drop-down list and select **Threat** under **Summary Databases** > **Remote Device Data**:

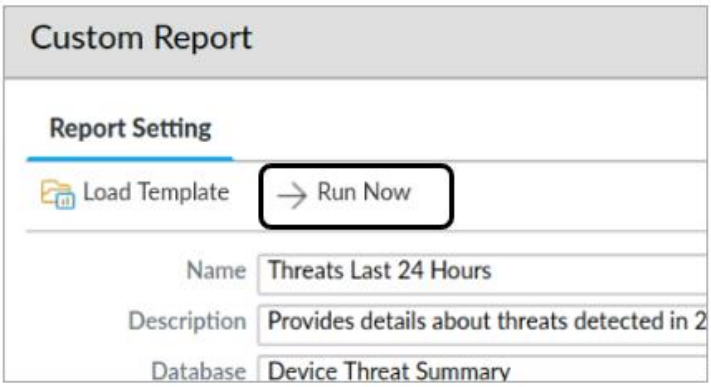


37. Leave the box for **Scheduled** unchecked.
38. For **Time Frame**, select **Last 24 Hrs**.
39. For **Sort By**, select **Count**.
40. Set the field next to **Sort By** to **Top 10**.
41. For **Group By**, select **Severity**.

42. Set the field next to **Group By** to **10 Groups**.
43. In the right section of the window, under **Available Columns**, locate **Threat ID/Name** in the list.
44. Highlight **Threat ID/Name** and click the **Add** button.
45. Locate the entry for **Action** in the **Available Columns** section.
46. Highlight **Action** and click the **Add** button.
47. Leave the remaining settings unchanged:

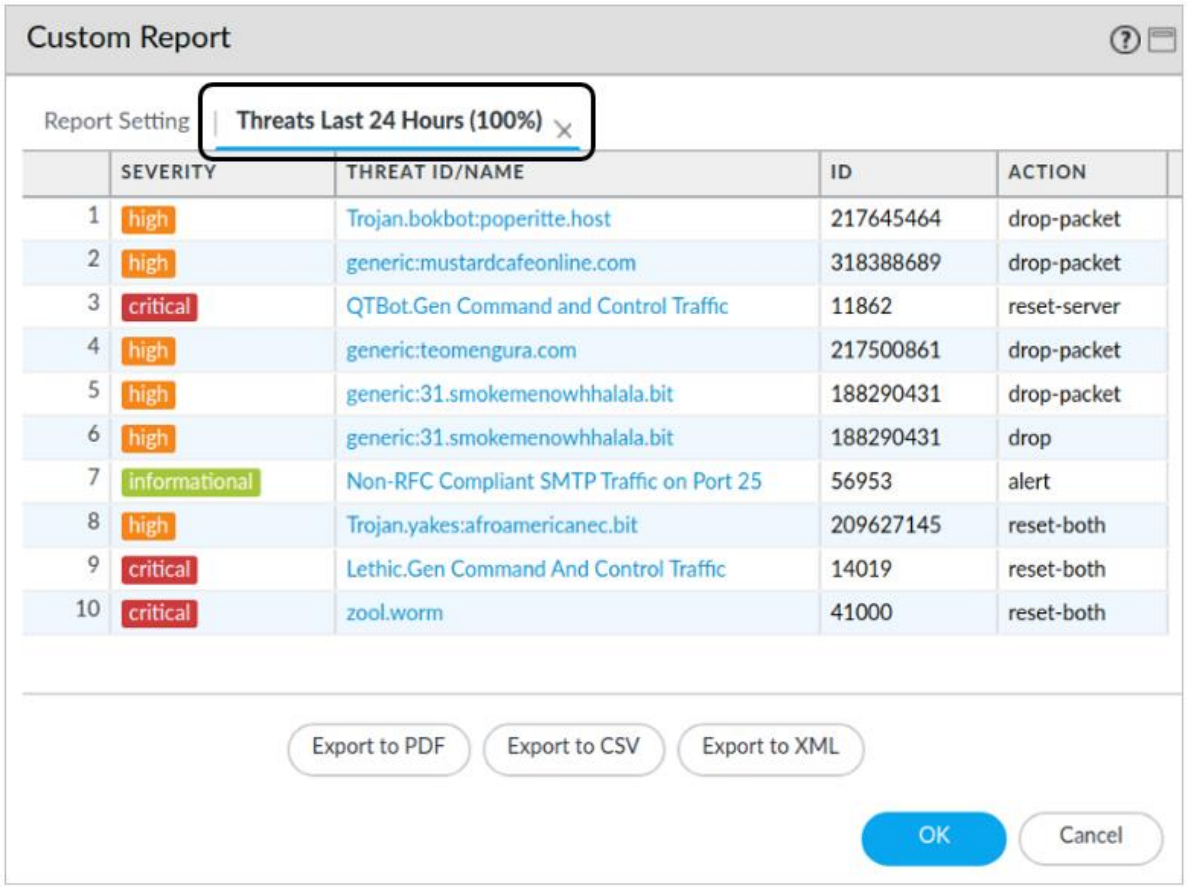


48. Before you close this window, click the **Run Now** button and see how the results look:



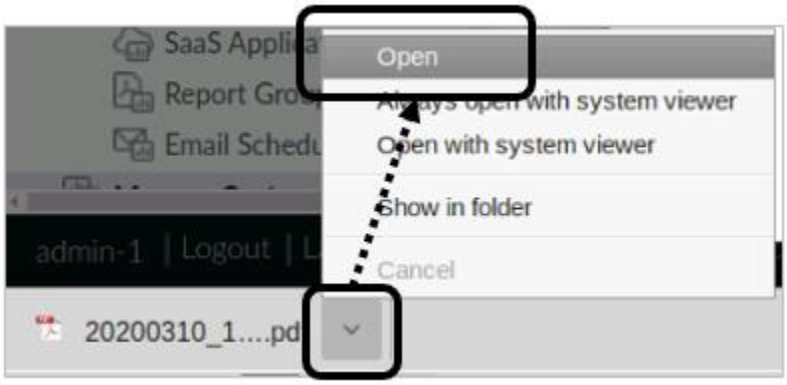
49. Panorama will generate the report.

50. Select the tab for **Threats Last 24 Hours (100%)**:



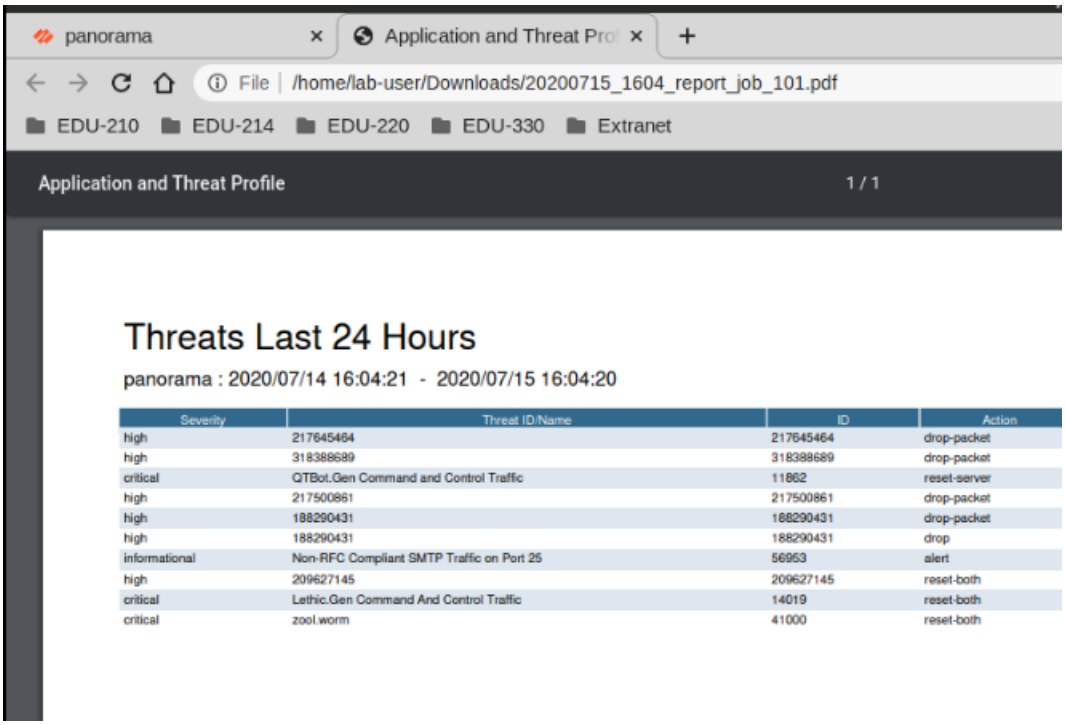
The information available in your report may vary from the example shown here.

51. Click the **Export to PDF** button.
52. Panorama will export the report.
53. In the bottom-left corner of the browser, use the arrow button to select **Open**:



If you do not see a download option at the bottom of the browser window, verify that the browser is not blocking popups. Check the upper right corner of the browser window in the address line for any indications of blocked pop-up windows.

54. The report will open in a separate tab in the Configuration browser:



Note that the information you see will differ from the example shown here.

55. Close the browser tab for the PDF report.
56. In the **Custom Report** window, click **OK**.
57. The **Custom Report** you created is now available in Panorama:

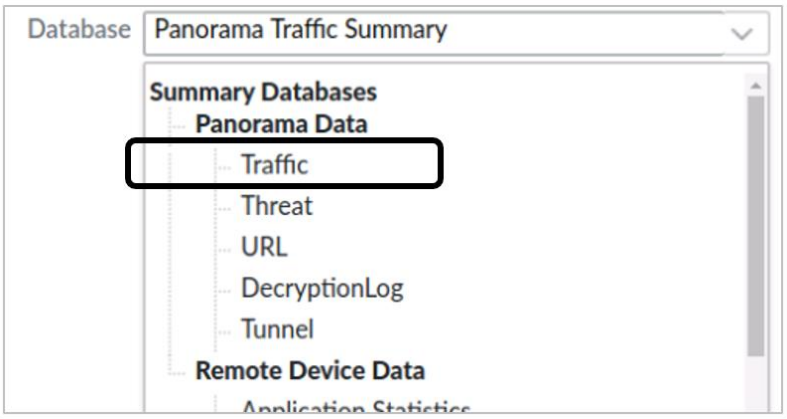
The next time your manager asks you for this report, you can run it, export the results as a PDF, and print or email the results to interested parties.

Create a Custom Report for Applications Used Within the Last 7 Days

In this section, you will create a new Custom Report that you can run when your manager asks you for information about Applications that the firewall has identified in the past seven days.

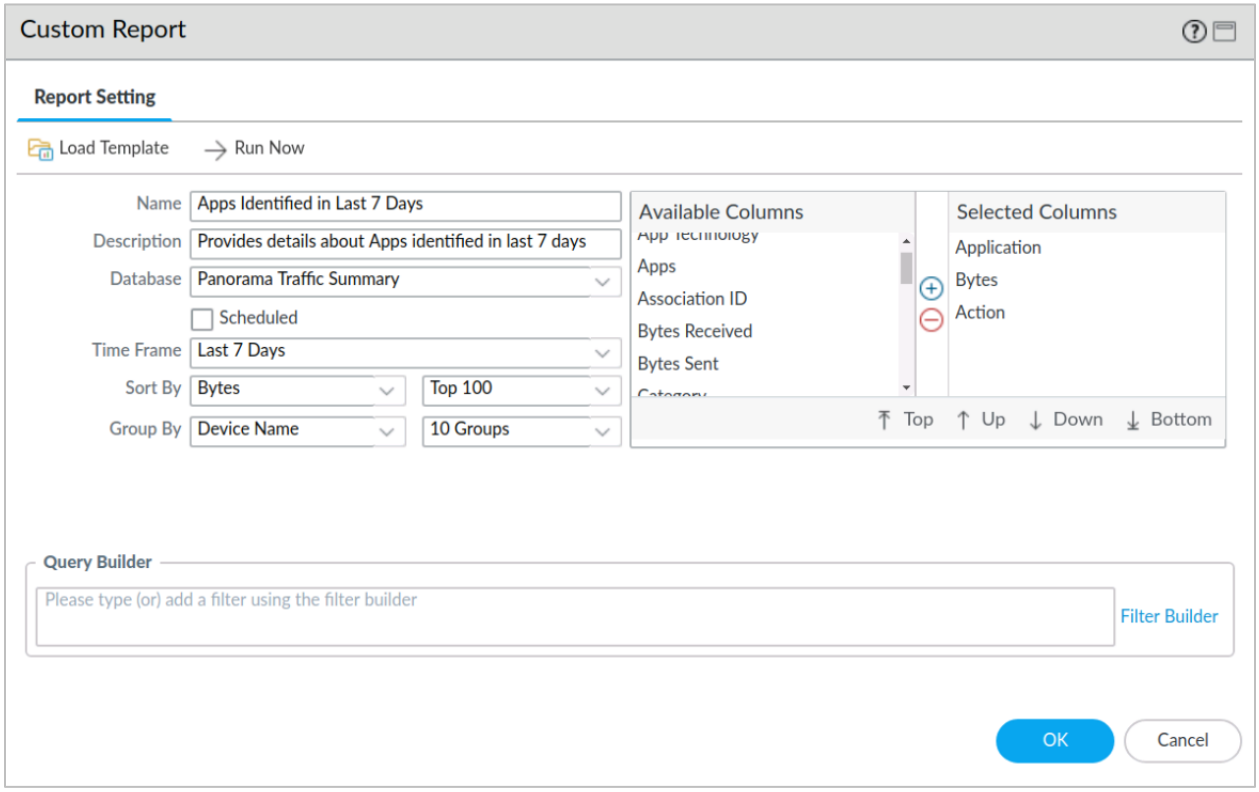
58. In the Panorama web interface, navigate to **Monitor** > **Manage Custom Reports**.
59. Select **All** from the **Device Group** drop-down list:

60. Click **Add**.
61. For **Name**, enter **`Apps Identified in Last 7 Days`**.
62. For **Description**, enter **`Provides details about Apps identified in last 7 days`**.
63. For **Database**, use the drop-down list and select **Traffic** under **Summary Databases – Panorama Data**:

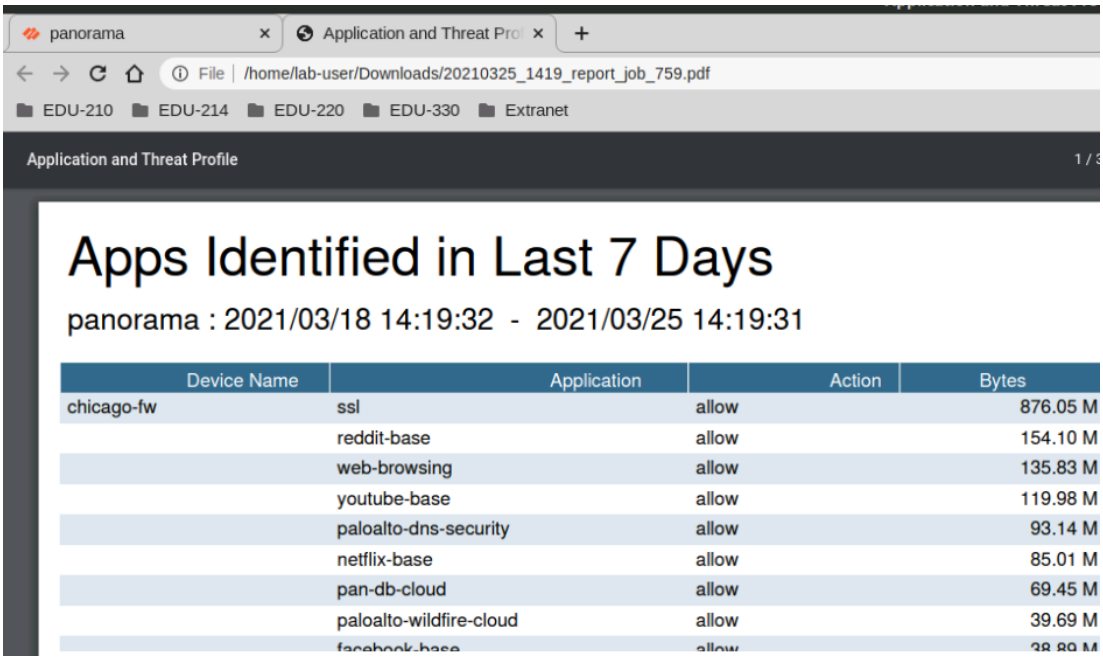


64. Leave the box for **Scheduled** unchecked.
65. For **Time Frame**, select **Last 7 Days**.
66. For **Sort By**, select **Bytes**.
67. Set the field next to **Sort By** to **Top 100**.
68. For **Group By**, select **Device Name**.
69. Set the field next to **Group By** to **10 Groups**.
70. Add **Application, Bytes**, and **Action** to the **Available Columns** section.

71. Leave the remaining settings unchanged:

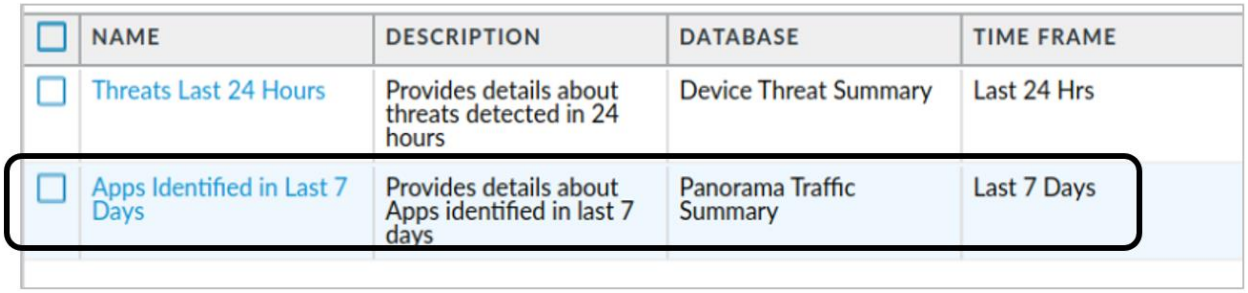


72. Before you close this window, click the **Run Now** button and see how the results look.
73. Panorama will generate the report.
74. Click the **Export to PDF** button and **Open** the report to view the results.
75. The report will open in a separate tab in the Configuration browser:



Note that the information you see will differ from the example shown here.

76. Close the browser tab for the PDF report.
77. In the **Custom Report** window, click **OK**.
78. The **Custom Report** you created is now available in Panorama:



NAME	DESCRIPTION	DATABASE	TIME FRAME
Threats Last 24 Hours	Provides details about threats detected in 24 hours	Device Threat Summary	Last 24 Hrs
Apps Identified in Last 7 Days	Provides details about Apps identified in last 7 days	Panorama Traffic Summary	Last 7 Days

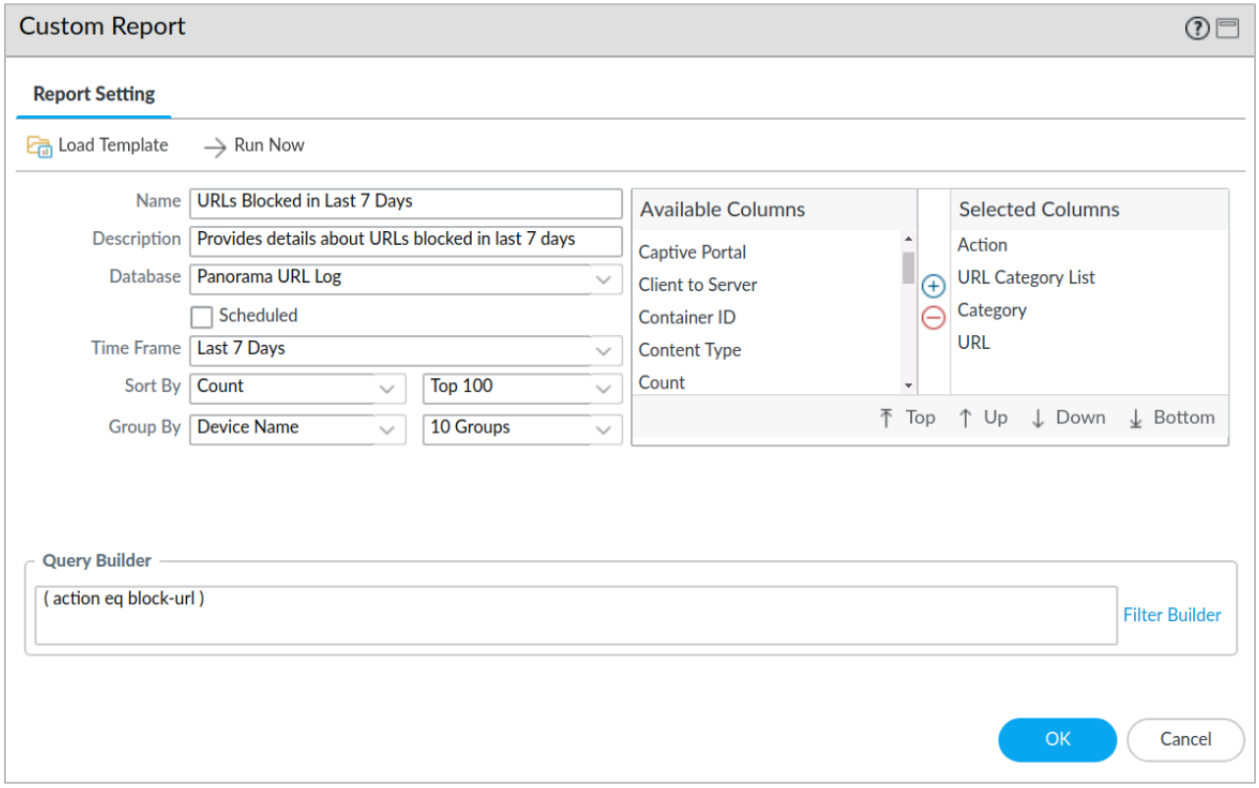
Create a Custom Report for URL Categories Blocked Within the Last 7 Days

In this section, you will create a new Custom Report that you can run when your manager asks you for information about URL Categories that the firewall has blocked in the past seven days.

79. In the Panorama web interface, navigate to **Monitor** > **Manage Custom Reports**.
80. Select **All** from the **Device Group** drop-down list:

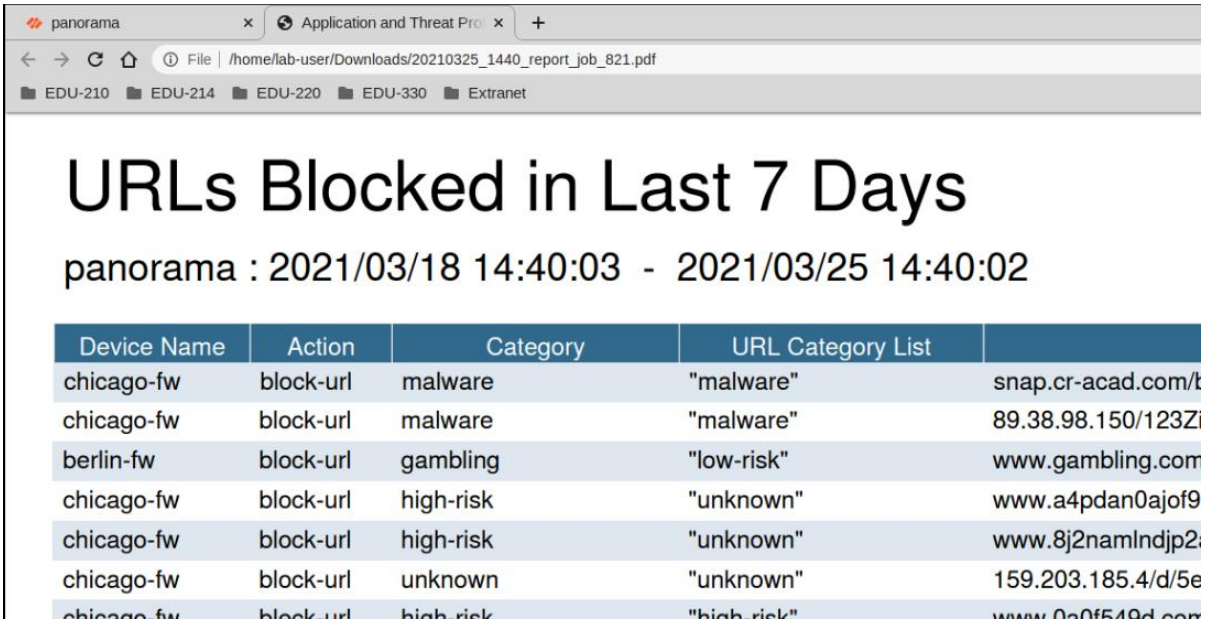
81. Click **Add**.
82. For **Name**, enter **`URLs Blocked in Last 7 Days`**.
83. For **Description**, enter **`Provides details about URLs blocked in last 7 days`**.
84. For **Database**, use the drop-down list and select **URL** under **Detailed Logs (Slower) – Panorama Data**.
85. Leave the box for **Scheduled** unchecked.
86. For **Time Frame**, select **Last 7 Days**.
87. For **Sort By**, select **Count**.
88. Set the field next to **Sort By** to **Top 100**.
89. For **Group By**, select **Device Name**.
90. Set the field next to **Group By** to **10 Groups**.
91. Add **Action, URL Category List, Category**, and **URL** to the **Available Columns** section.

92. In the **Query Builder** section, enter the following:
93. **`( action eq block-url )`**
94. Leave the remaining settings unchanged:



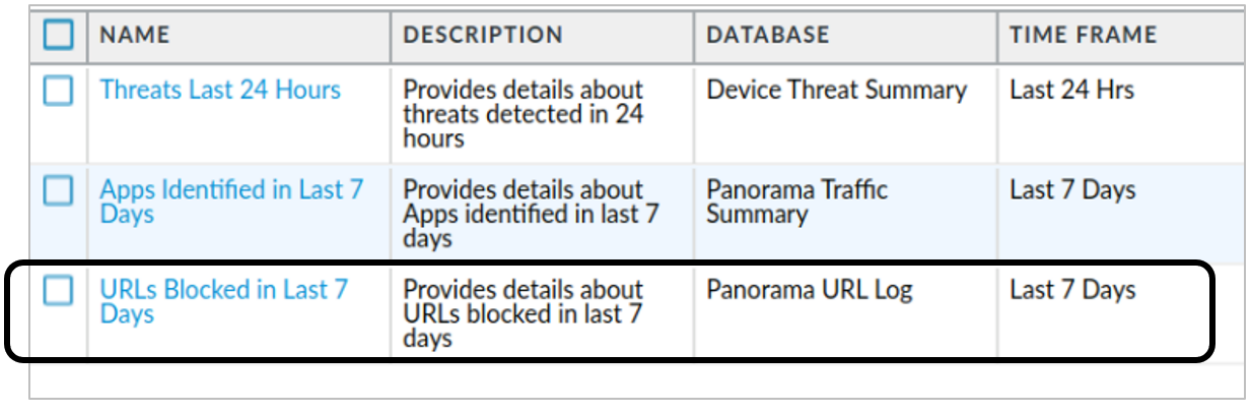
95. Before you close this window, click the **Run Now** button and see how the results look.
96. Panorama will generate the report.
97. Click the **Export to PDF** button and **Open** the report to view the results.

98. The report will open in a separate tab in the Configuration browser:



Note that the information you see will differ from the example shown here.

99. Close the browser tab for the PDF report.
100. In the **Custom Report** window, click **OK**.
101. The **Custom Report** you created is now available in Panorama:

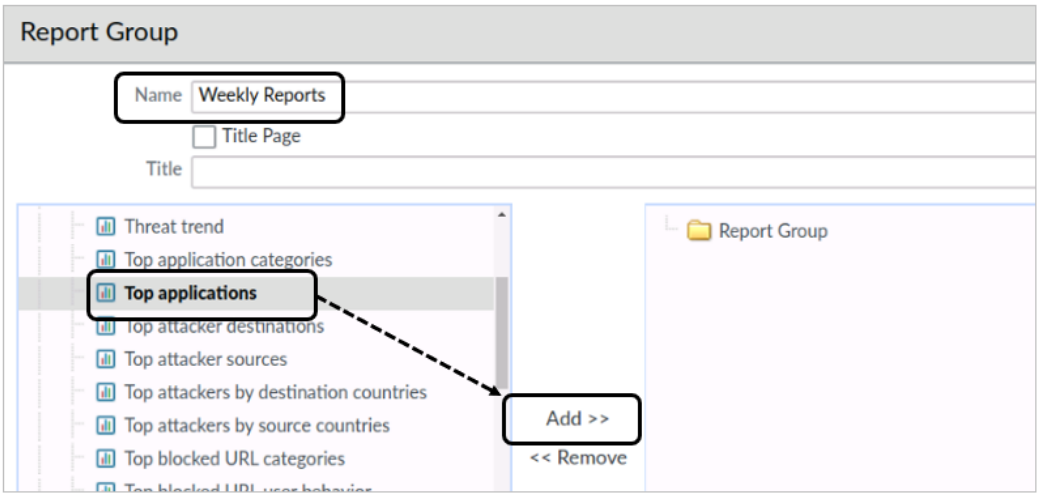


Create a Weekly Report Group

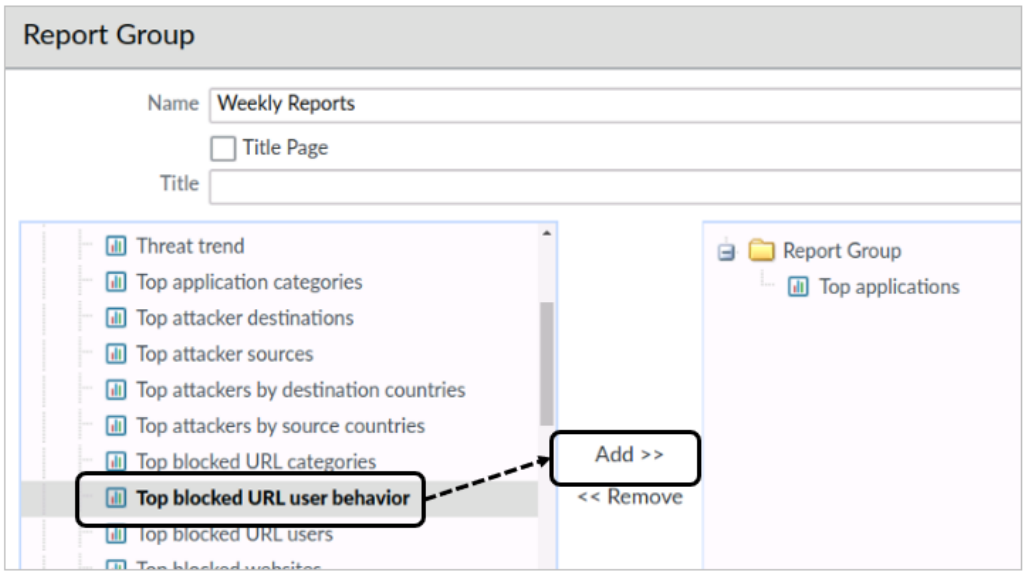
In this section, you will create a Report Group that contains an Applications report and a report about blocked user behavior for URLs.

102. Navigate to **Monitor > PDF Reports > Report Groups**.
103. Click **Add**.

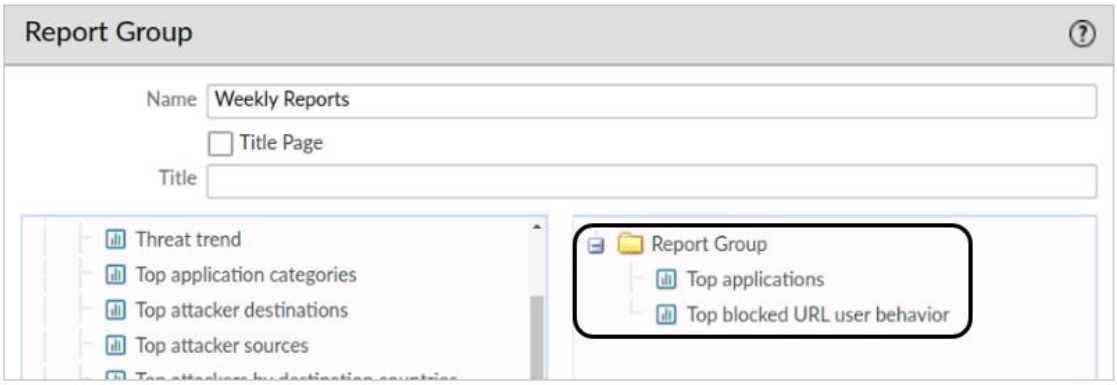
104. For **Name**, enter **`Weekly Reports`**.
105. Under the column for **Predefined Report**, scroll down and locate **Top Applications**.
106. Highlight the entry for **Top applications**.
107. Click **Add**:



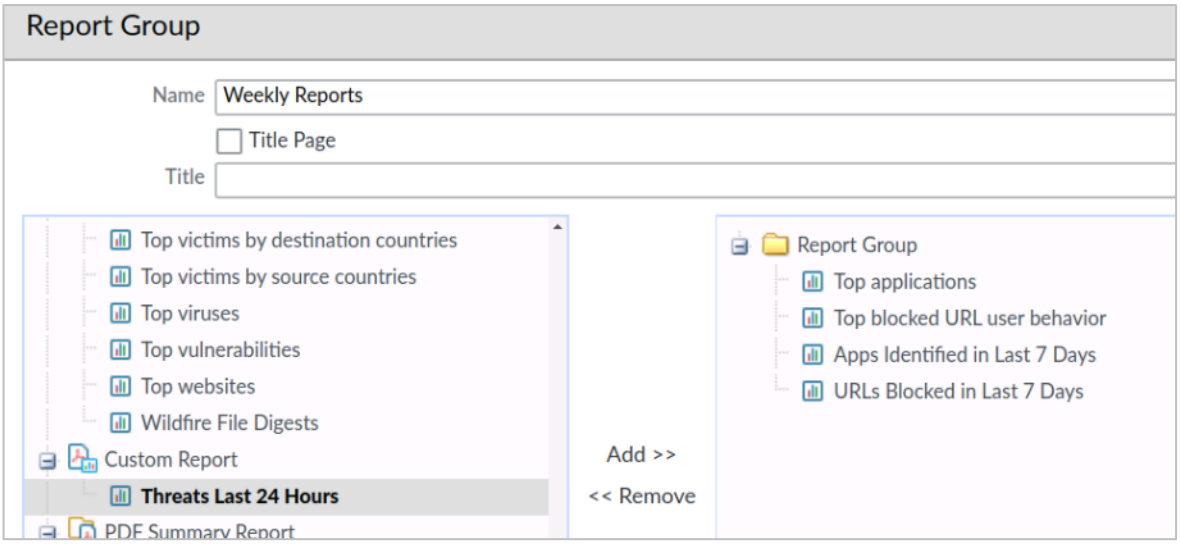
108. Scroll down and locate the entry for **Top blocked URL user behavior**.
109. Highlight the entry for **Top blocked URL user behavior** and click **Add**:



110. When the configuration process is complete, your **Report Group** on the right should have two entries:



111. Scroll down to the Custom Reports section.
112. Add the **Apps Identified in Last 7 Days** to the Report Group.
113. Add **URLs Blocked in Last 7 Days** to the Report Group.
114. When complete, your Weekly Reports Report Group should have four entries:



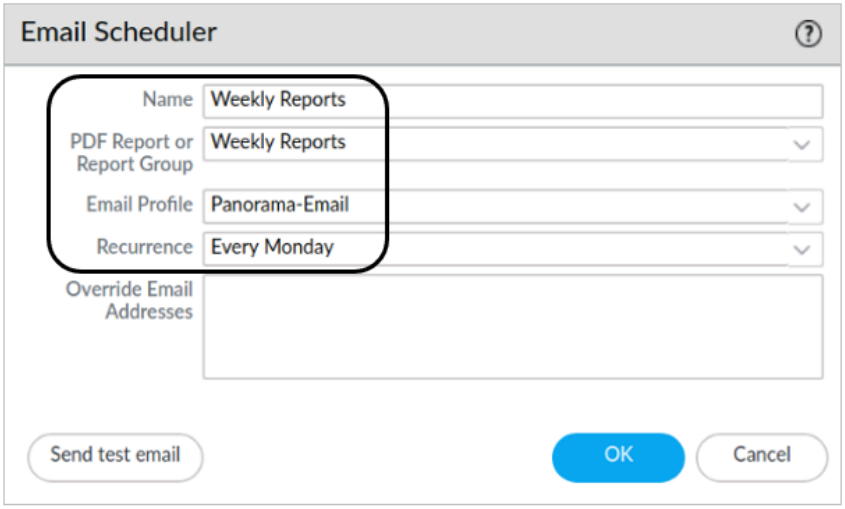
115. Click **OK**.

Create an Email Schedule

Rather than printing these reports each week and manually presenting them to your manager, you will create an Email Schedule so that these reports are automatically sent to her and any other interested parties.

116. Navigate to **Monitor > PDF Reports > Email Scheduler**.
117. Click **Add**.
118. For **Name**, enter **`Weekly Reports`**.
119. For **PDF Report or Report Group**, use the drop-down list to select **Weekly Reports**.

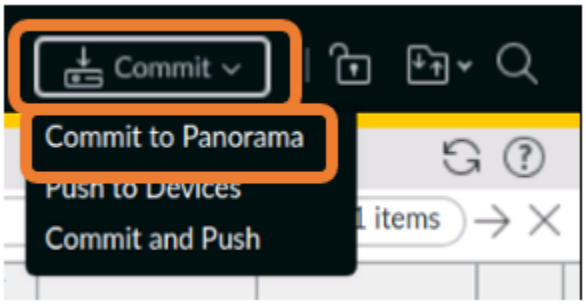
120. For **Email Profile**, use the drop-down list to select **Panorama-Email**.
121. For **Recurrence**, use the drop-down list to select **Every Monday**.
122. Leave the remaining items unchanged:



123. Click **OK**.

Commit the Changes to Panorama

124. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



125. Click **Commit**.
126. Monitor the status of the commit.
127. When the commit status is complete, click **Close**.

You only made changes to Panorama in the previous section, so you do not need to push any configuration changes to the managed firewalls.

Lab Cleanup

128. In the Remmina SSH connection window to client-B, use **`Ctrl+C`** to stop the running script.
129. Type **`exit <ENTER>`** to close the Remmina SSH connection to client-B.
130. In the Remmina SSH connection window to the Extranet-Server, type **`exit <ENTER>`**.
131. Close the Remmina Remote Desktop Client window.

Stop. This is the end of the lab.

Lab 9 Scenario: Troubleshooting

In this lab, you will perform the following tasks:

- Troubleshoot commit failure issues
- Review the health of the managed firewalls
- Retrieve information about Panorama using SNMP

You arrive at the office to discover that the Berlin firewall is failing when a commit is pushed to it. You will need to troubleshoot and resolve the errors preventing the configuration push.

You will also remove unused files from Panorama to make certain that there is adequate drive space on the device.

In order to gather statistical information about Panorama's health and performance, you will configure and test SNMP settings.

Lab Objectives

- Examine commit failure messages
- Verify that firewalls are connected to Panorama
- Troubleshoot firewall commit failure
- Remove unused files from Panorama
- Examine SNMP data available from Panorama

High-Level Lab Steps

Load Configuration and Push to Devices

- Load and commit the **EDU-220-11.1a-Lab-9-Start.xml** configuration file on Panorama.
- Push the Device Group and Template changes to the firewalls using **`Force Template Values`**

Examine Commit Error Messages

- Use the **Tasks** button to locate the two **`commit failed`** messages and examine the details of both messages.

Verify That Berlin Firewall is Connected to Panorama

- Connect to Panorama using Remmina and use the **`ping`** command to verify that Panorama has basic network connectivity to the berlin-fw.
- From the Panorama CLI, verify that the berlin-fw is connected.
- Connect to the berlin-fw through the CLI and verify that the firewall is connected to Panorama.

Troubleshoot the Berlin Firewall Commit Failure

- Use the details of the commit error messages to locate information about the commit failure to the Germany-Stack Template.
- Use the Global Find option in the Panorama web interface to locate configuration information about LR-1.
- Isolate the route statement that is generating the error.
- Modify the route entry to use ethernet1/2 and a Next Hop of 192.168.50.200
- Commit the changes to Panorama.

Push the Configuration to the Firewalls

- Push the Device Group and Template changes to the firewalls using **`Force Template Values`**
- Verify that the configuration push was successful for all Device Groups and Template Stacks

Delete Unused Files from Panorama

- Use the Panorama web interface to delete the **`11.0.0`** software file.
- Examine the **Dynamic Updates** in the Panorama web interface to determine which ones you can delete.
- Use the CLI to determine which content update files you can delete.

Configure SNMP on Panorama

- Verify that SNMP is configured on Panorama with the following settings:

Setting	Value
Physical Location	**Chicago, IL, USA**
Contact	**John Doe**
Use Event-specific Trap Definitions	**Checked**
Version	**V2c**
SNMP Community String	**notpublic**

- Enable SNMP on the Management interface

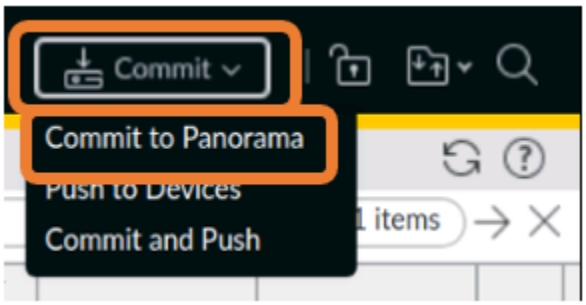
Poll Panorama for CPU Utilization

- Change to the **/home/lab-user/Desktop/Lab-Files/EDU-220** directory:
  cd /home/lab-user/Desktop/Lab-Files/EDU-220 <ENTER>
- Run the **snmpscript.sh**:
  ./snmpscript.sh <ENTER>
- Follow the instructions onscreen to verify that Panorama is responding to SNMP queries.

Detailed Lab Steps

Load Configuration and Push to Devices

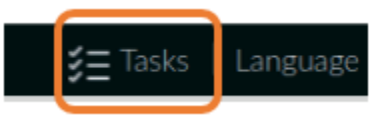
1. In the Panorama web interface, select **Panorama > Setup > Operations**.
2. Click **Load named Panorama configuration snapshot**.
3. Select **EDU-220-11.1a-Lab-9-Start.xml**, and then click **OK**.
4. Click **Close**.
5. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



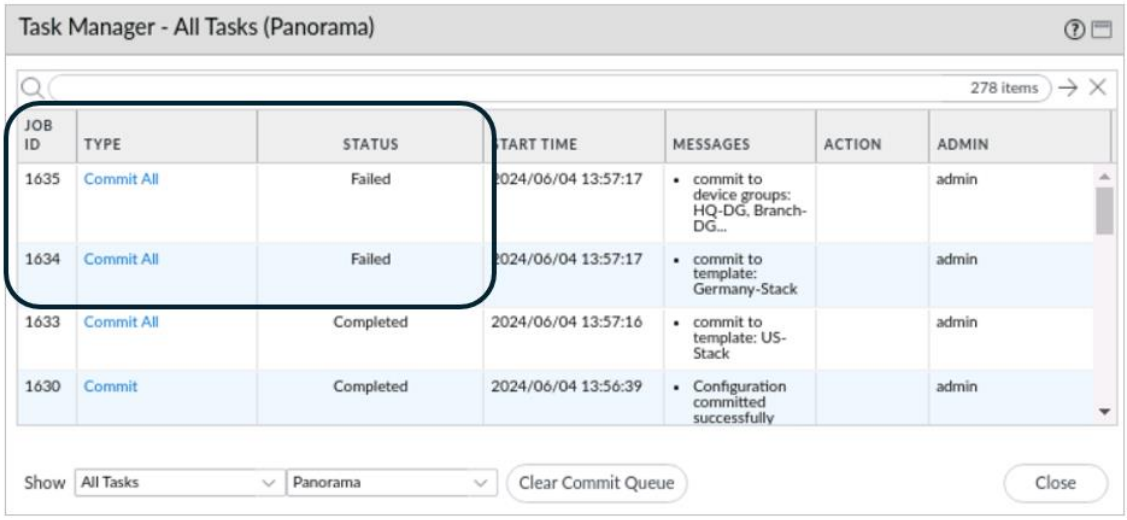
6. Click **Commit**.
7. Monitor the status of the commit.
8. When the commit status is complete, click **Close**.
9. Click the **Commit** button again in the upper-right corner.
10. Select **Push to Devices**.
11. When the **Push to Devices** window appears, click **Edit Selections**.
12. Verify that the **Merge with Device Candidate Config**, **Include Device and Network Templates**, and **Force Template Values** check boxes are selected:
13. After you select **Force Template Values**, click **Yes** on the warning box.
14. Under the **Device Group** tab, verify that the check box for **Corp-DG** is selected.
15. Select the **Templates** tab.
16. Verify that the check boxes for the Chicago firewall and the Berlin firewall are selected.
17. Click **OK**, and then click **Push**.

Examine Commit Error Messages

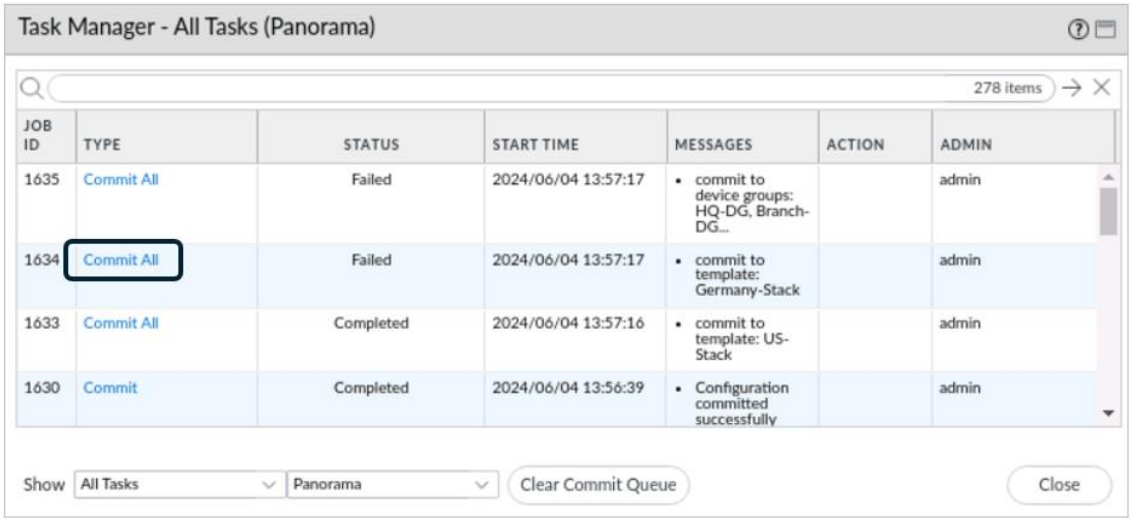
18. Click **Close** on the Task Manager window.
19. In the bottom-right corner of Panorama, click the **Tasks** button:



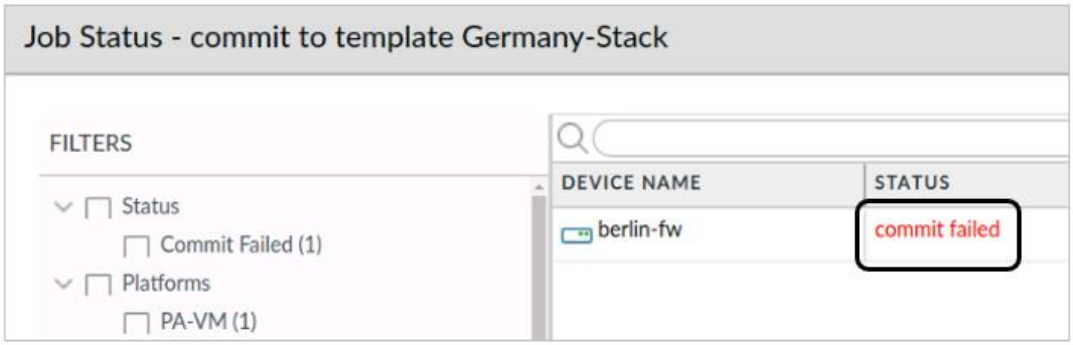
20. Notice that several of the commits have failed:



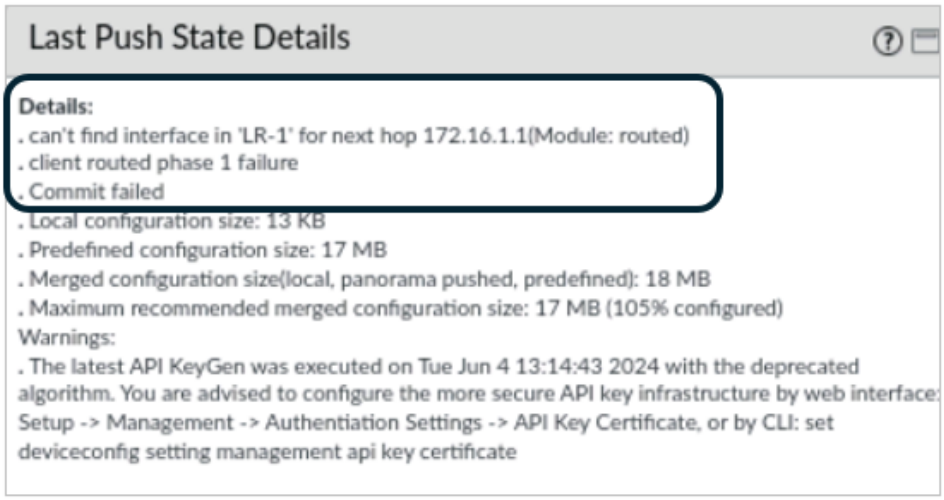
21. Click the **Commit All** link for the **Failed "commit to template: Germany-Stack"** entry:



22. In the **Jobs Status** window that appears, click the link for **commit failed**:

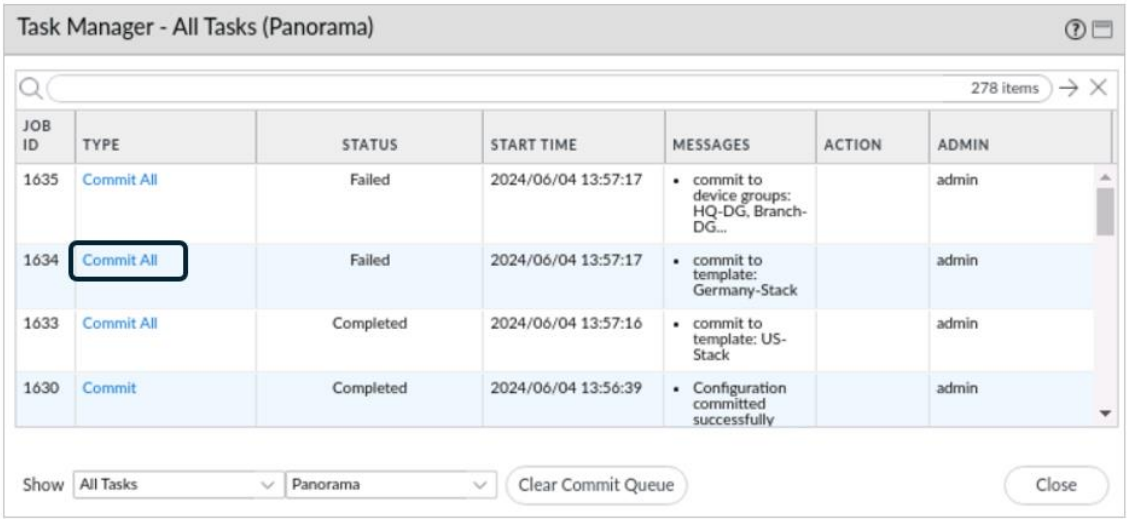


23. In the **Last Push State Details** window, Panorama provides information about why the push failed:

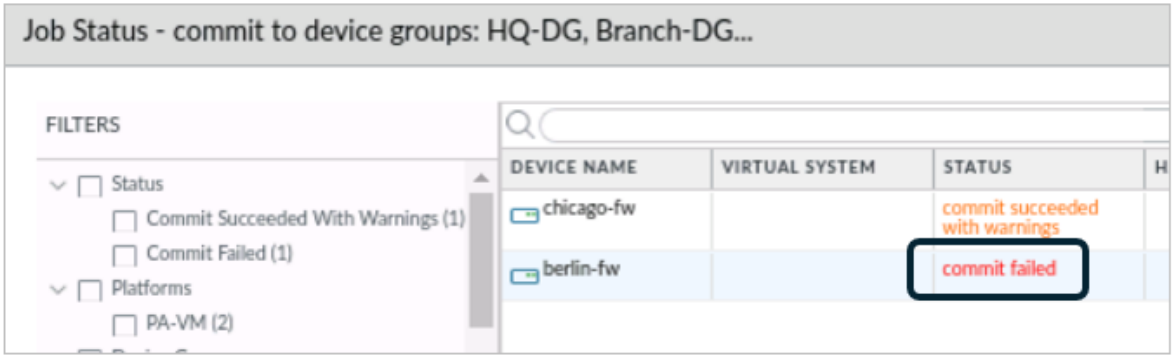


This message indicates an issue with routing for LR-1.

24. Click **Close** in the **Last Push State Details** window.
25. Click **Close** in the **Job Status** window.
26. Leave the **Task Manager** window open.
27. Click the **Commit All** link for the **Failed "commit to device groups: HQ-DG, Branch-DG…"** entry:



28. In the **Jobs Status** window that appears, note the Status for the firewalls:

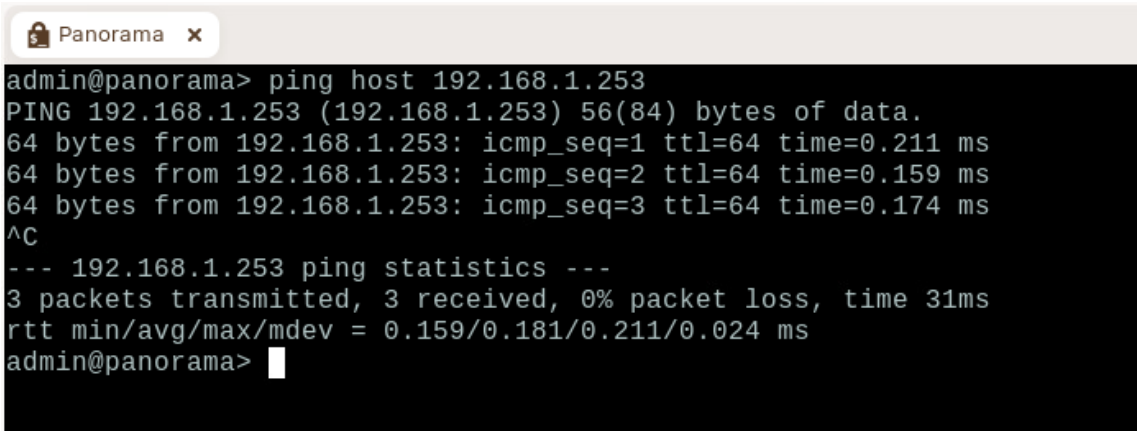


29. Leave this window open and continue to the next section.

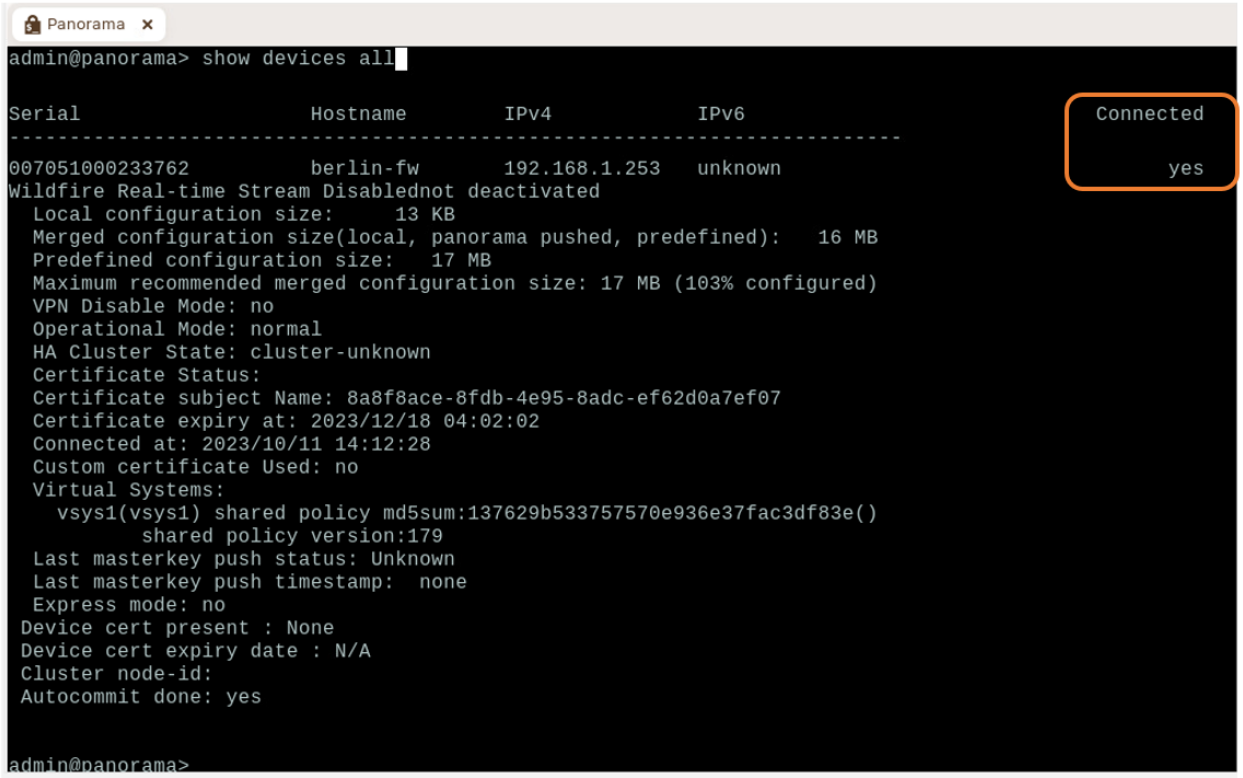
Verify That Berlin Firewall is Connected to Panorama

Before you immediately jump to any conclusions about this failure, first verify that Panorama and the berlin-fw can communicate with one another successfully. Use the CLI to verify that the Berlin firewall is connected to Panorama.

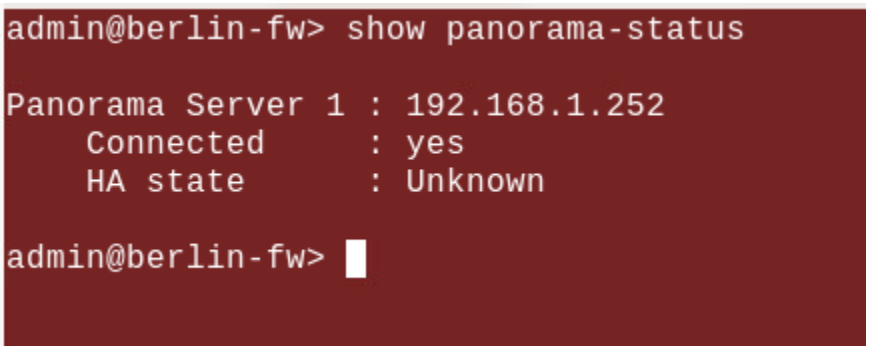
30. From the client-A desktop, open Remmina.
31. Connect to Panorama.
32. Use the following command to ping the management IP address of the berlin-fw from Panorama:
    `ping host 192.168.1.253`



33. After three or four successful replies, use **`CTRL+C`** to halt the ping.
34. Use the following command to view the connection status from Panorama to the Berlin firewall:
    `show devices all`
35. Press the spacebar to see the information about the berlin-fw:



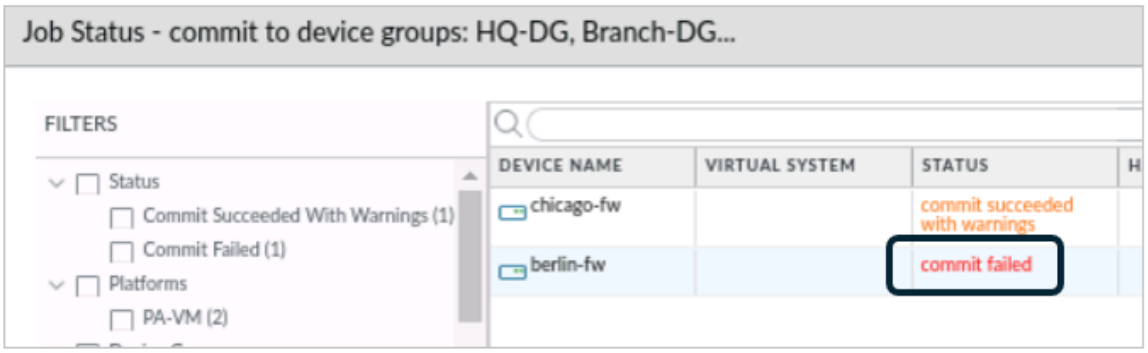
36. Although the column headers are not duplicated for each firewall listed, you can see that the berlin-fw is connected by the **yes** in the far-right side of the display.
37. You can also determine the status of the connection between a firewall and Panorama through the CLI of the firewall.
38. In Remmina, connect to the berlin-fw.
39. Use the following command to see the status of Panorama from the firewall:
    show panorama-status



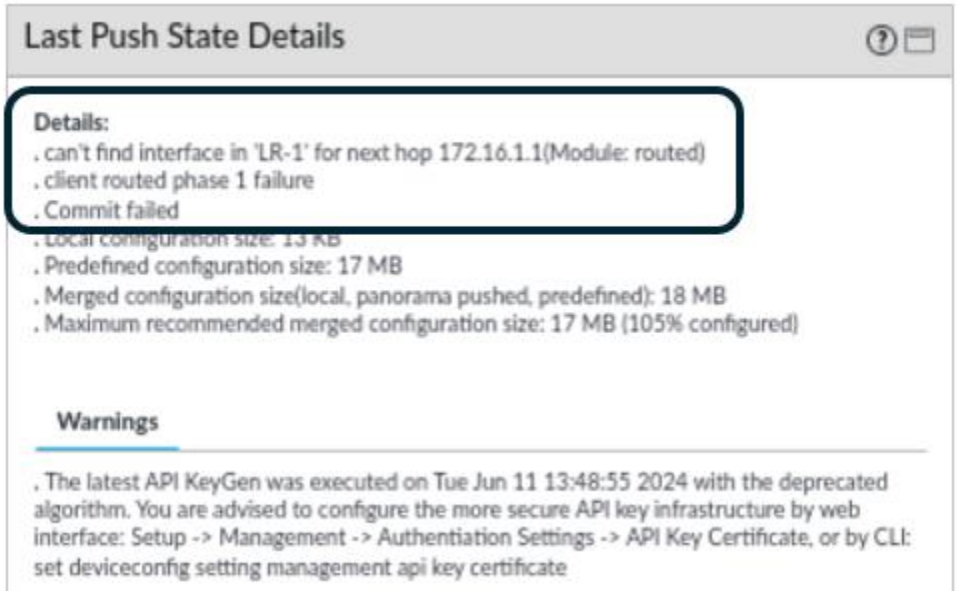
Troubleshoot the Berlin Firewall Commit Failure

Now that you have determined that Panorama and the berlin-fw are connected, you can move on to gathering more information about the cause of the commit failure.

40. In the **Job Status – commit to Template Germany-Stack** window, click directly on the **commit failed** message.



41. In the **Last Push State Details** window, Panorama provides additional information about why the push failed:



This message refers to an issue with routing for LR-1.

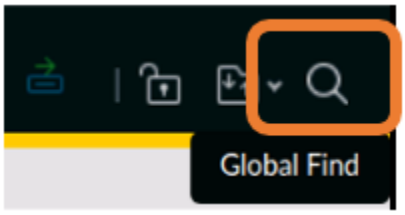
42. Click **Close** in the **Last Push State Details** window.
43. Click **Close** in the **Job Status** window.
44. Click **Close** in the **Task Manager**.

Based on the message details, you can conclude that there is a problem with the routing configuration that Panorama is trying to push to the Berlin firewall.

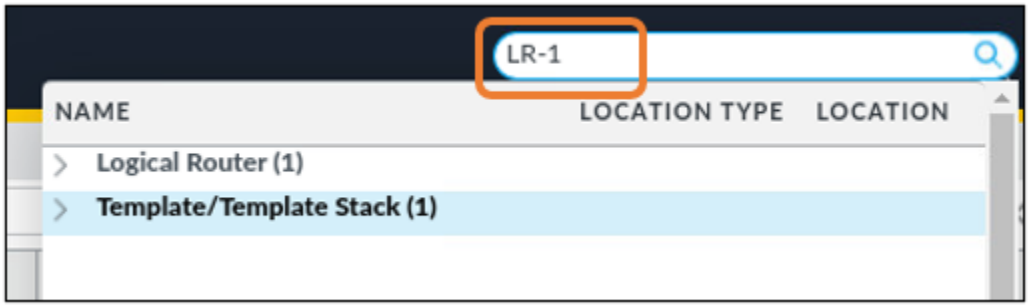
In a production environment with many Templates configured, determining exactly where this misconfiguration exists can be a challenge.

In this case, you will use the **Global Find** tool to locate the Template and logical router misconfiguration.

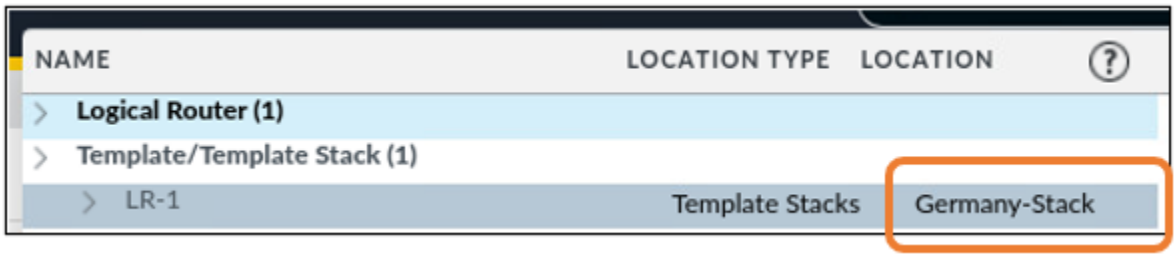
45. Click the **Global Find** button in the upper-right corner of the Panorama web interface:



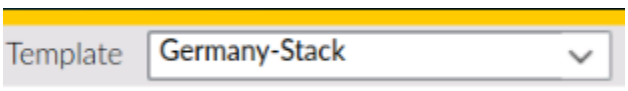
46. Enter **`LR-1`**, and then press **Enter** on your keyboard.
47. Panorama provides details about where the "**LR-1**" string occurs in any configuration elements:



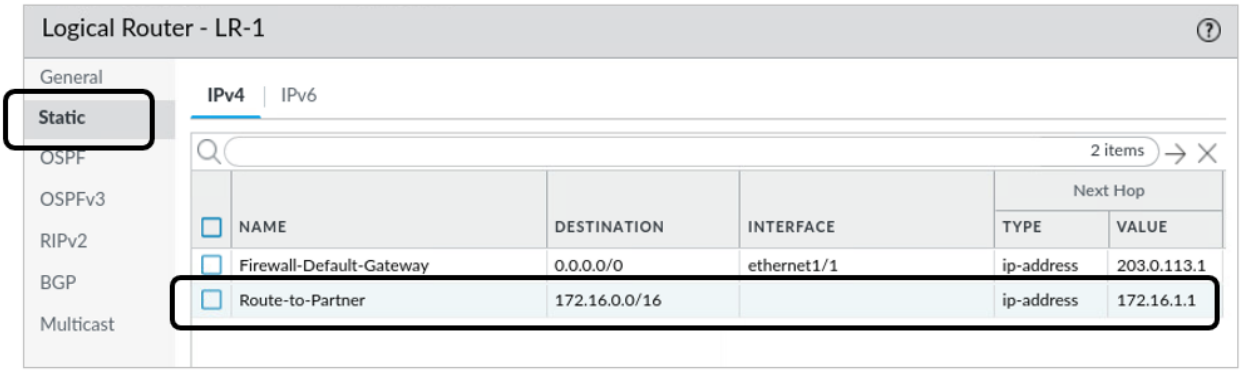
48. Expand the entry for **Template/Template Stack (1)**:



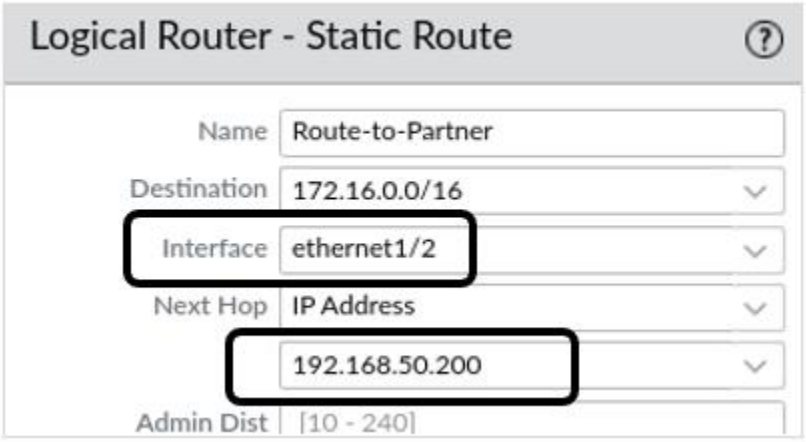
49. In this case, you can see that LR-1 appears in the Germany-Stack.
50. Navigate to **Network > Routing > Logical Routers**.
51. Select **Germany-Stack** from the **Template** drop-down list:



52. Click the entry for **LR-1** to edit it.
53. Select the tab for **Static**:



54. Notice that the **Interface** column for the **Route-to-Partner** entry is empty.
55. Click the **Route-to-Partner** entry to edit it.
56. For **Interface**, select **ethernet1/2**.
57. For **Next Hop**, enter **`192.168.50.200`**.
58. Leave the remaining settings unchanged:

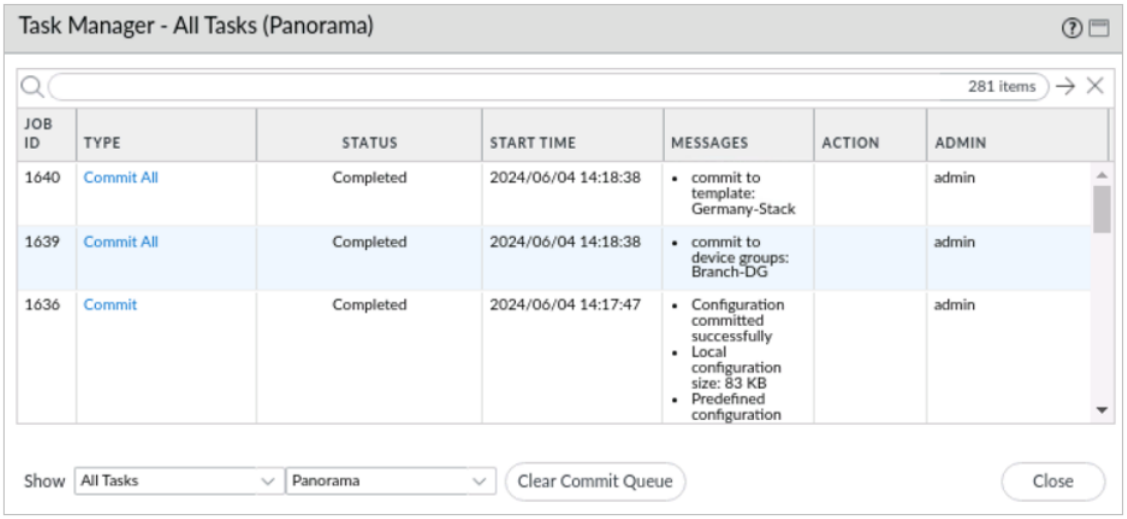


59. Click **OK** on the **Logical Router – Static Route – Ipv4** window.
60. Click **OK** on the **Logical Router – LR-1** window.
61. Commit the changes to Panorama.

Push the Configuration to the Firewalls

62. Click the **Commit** button in the upper-right corner.
63. Select **Push to Devices**.
64. When the **Push to Devices** window appears, click **Edit Selections**.
65. Verify that the **Merge with Device Candidate Config**, **Include Device and Network Templates**, and **Force Template Values** check boxes are selected:
66. After you select **Force Template Values**, click **Yes** on the warning box.

67. Under the **Device Group** tab, verify that the check box for **Corp-DG** is selected.
68. Select the **Templates** tab.
69. Verify that the check box for the Berlin firewall is selected.
70. Click **OK**, and then click **Push**.
71. Leave the **Task Manager** window open so you can monitor the **Push** status.
72. When each entry in the **Task Manager** changes to **Completed**, you can close the **Task Manager**:



You should not see any Failed status messages after the fixes you employed to the LR-1 static route.

73. These steps should fix the **Commit** issue with the Berlin firewall.

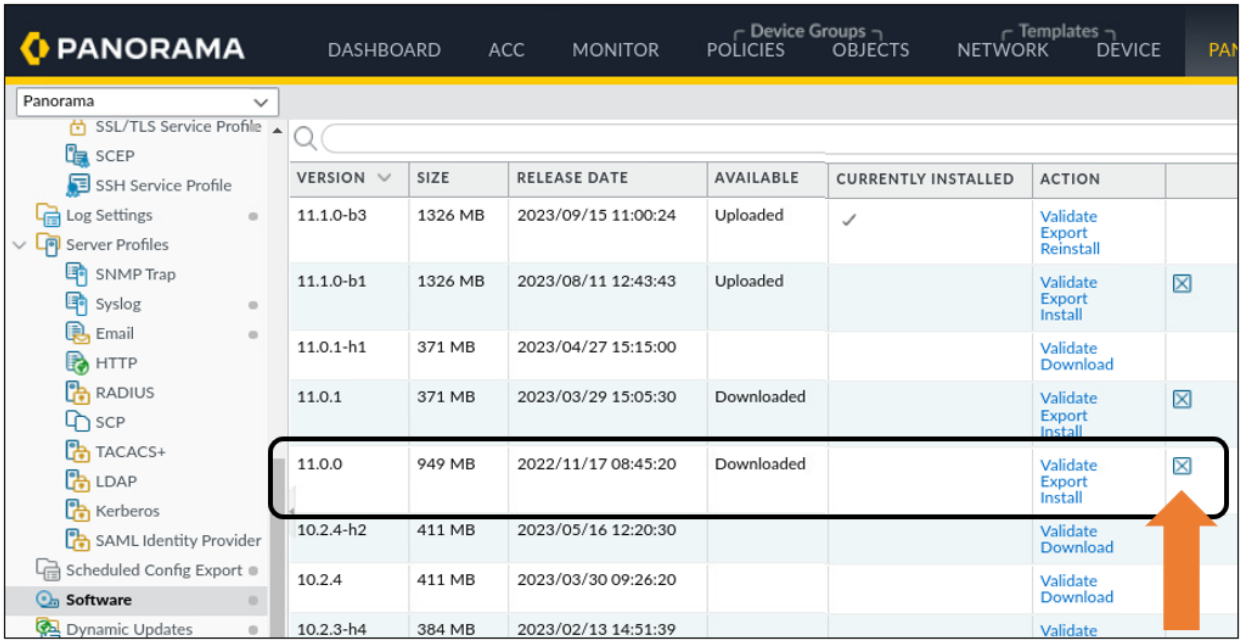
Delete Unused Files from Panorama

You can free up space on Panorama by deleting unused versions of PAN-OS. You can accomplish this task through the CLI or through the web interface.

74. In the web interface, navigate to **Panorama > Software**.
75. Scroll down and locate an older version of PANOS.

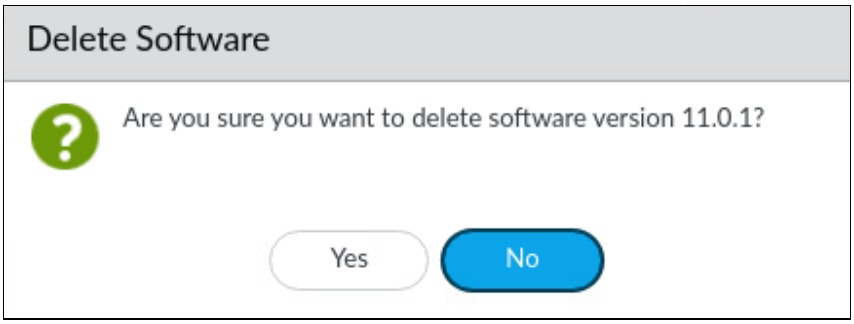
The version of PANOS you see in your lab environment may differ from the following example.

76. In the following example, note the box at the far right of the row for version 11.0.0:



This icon indicates that the file resides on Panorama.

77. Click the box icon.
78. Panorama provides a confirmation window.



79. Click **Yes**.
80. Panorama will delete the file and provide a notification.
81. Click **OK**.

Panorama will not allow you to delete the version of PAN-OS that is currently running on the Device.

You can also delete PAN-OS software files through the CLI.

82. Open Remmina and connect to Panorama.
83. Enter the following command followed by <TAB>:
    `delete software version <TAB>`

```
admin@panorama> delete software version
  10.0.0   10.0.0
  10.2.0   10.2.0
  11.0.0   11.0.0
  11.0.1   11.0.1
  <value>  Version
```

Note that the information you see may differ from the example shown here.

84. Panorama provides a list of the versions available to delete.
85. Enter the following command to delete version 10.0.0:
    delete software version 10.0.0 <ENTER>

```
admin@panorama> delete software version 10.0.0


admin@panorama>
```

Note that Panorama does not prompt you to confirm the deletion, so be certain about which versions you intend to remove.

However, if you try to remove the version of code currently running on Panorama, you will get the following warning:

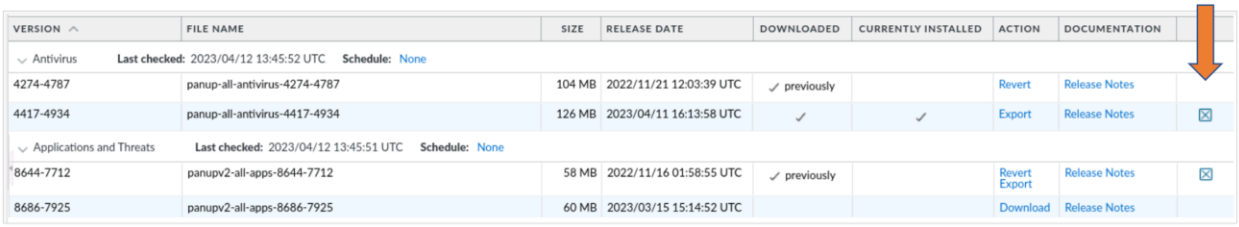
```
admin@panorama> delete software version 11.0.1

Can't purge image 'cms-11.0.1' installed on active sysroot


admin@panorama>
```

86. You can also delete content update files from the CLI.
87. Use the following command to view the content update files available on Panorama:
    delete content update <TAB>

```
admin@panorama> delete content update
  panupv2-all-apps-8613-7545.tgz   2022/08/30 13:31:08    53013.5K
  panupv2-all-apps-8644-7712.tgz   2022/11/21 14:32:07    60218.1K
  panupv2-all-apps-8696-7977.tgz   2023/04/12 13:40:00    62689.2K
  <value>                          Filename
```

Note that the information you see may differ from the example shown here.

88. You can delete any of the files listed to free up drive space, if necessary, through the CLI.
89. If you prefer to use the web interface to delete content update files, you can find them under **Panorama > Dynamic Updates**.
90. Click the box icon in the far-right column for any file you want to remove:

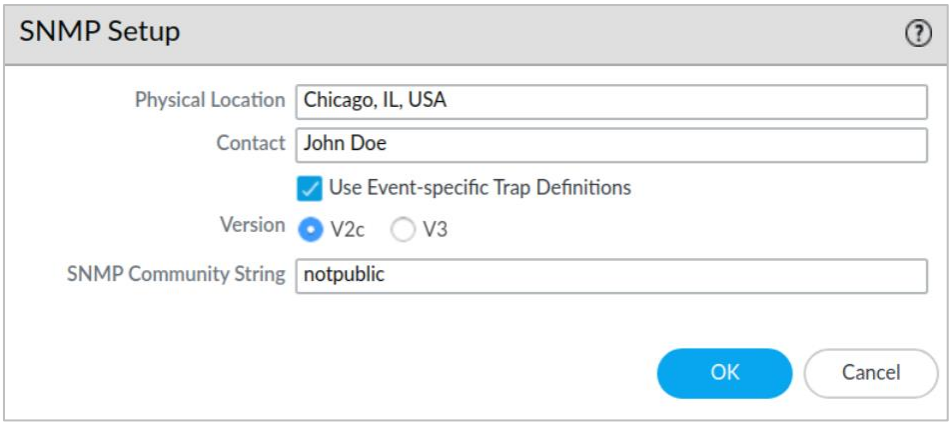


Configure SNMP on Panorama

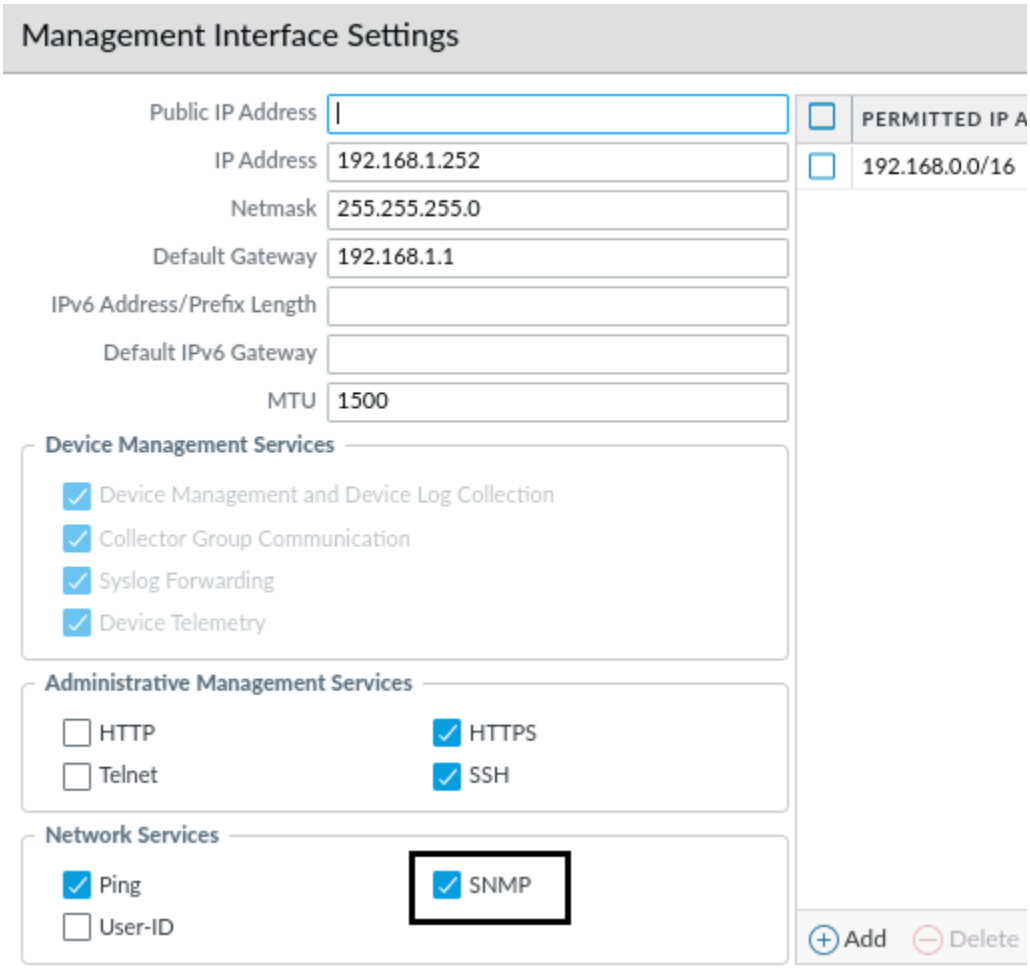
Your organization uses an SNMP monitoring tool to gather statistics from various network devices. You intend to add Panorama to the list of hosts that this SNMP tool monitors. Before you do so, you will need to enable SNMP on Panorama and identify the appropriate SNMP OIDs (Object Identifiers) for several performance-related items such as CPU utilization.

91. Navigate to **Panorama > Setup > Operations > Miscellaneous**.
92. Click the link for **SNMP Setup**.
93. Verify that the settings match the following:

Setting	Value
Physical Location	`Chicago, IL, USA`
Contact	`John Doe`
Use Event-specific Trap Definitions	`Checked`
Version	`V2c`
SNMP Community String	`notpublic`



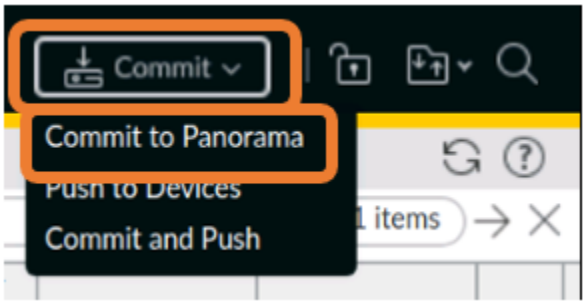
94. Click **OK**.
95. Select **Panorama** > **Setup** > **Interfaces**.
96. Click the **Management** entry.
97. Place a **check** in the box for **SNMP** under the **Network Services** section at the bottom of the window.



98. Leave the remaining settings unchanged.
99. Click **OK**.

Commit the Changes to Panorama

100. Click the **Commit** option in the upper-right corner, and then select **Commit to Panorama**:



101. Click **Commit**.
102. Monitor the status of the commit.
103. When the commit status is complete, click **Close**.

You only made changes to Panorama in the previous section, so you do not need to push any configuration changes to the managed firewalls.

Poll Panorama for SNMP Data

In this section, you will run a script that polls Panorama for SNMP information about the following system details:

- CPU Utilization
- System Uptime
- System Description

This script uses a tool called **`snmpget`** to query Panorama, and the details for each query have been predefined. In a production environment, your organization will likely have a sophisticated tool that carries out similar queries and provides graphical output of the results. This exercise is only designed to show you a few examples of what can be retrieved from Panorama via SNMP.

104. On the client-A host, open a Terminal window.
105. Change to the **`/home/lab-user/Desktop/Lab-Files/EDU-220`** directory:

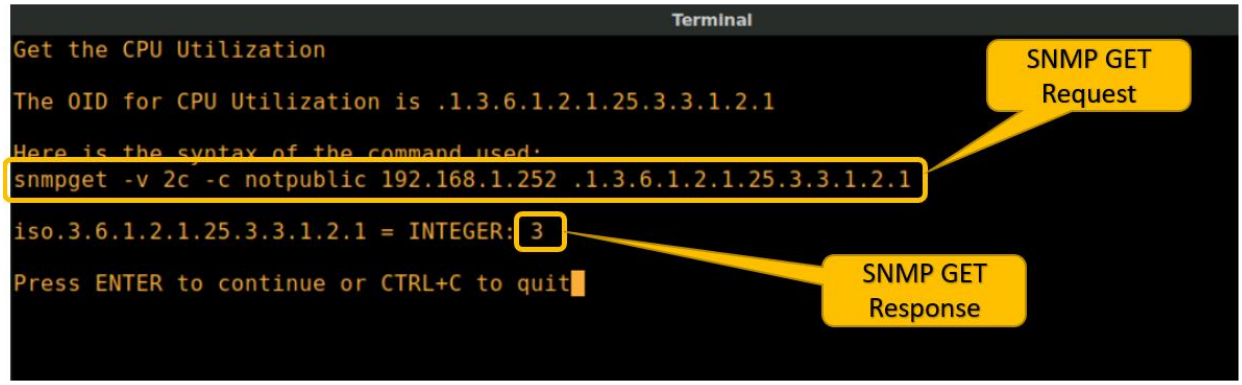
```
cd /home/lab-user/Desktop/Lab-Files/EDU-220 <ENTER>
```

106. Run the **`snmpscript.sh`**:

```
./snmpscript.sh <ENTER>
```

107. Follow the instructions onscreen.

As an example, the OID for CPU Utilization is .1.3.6.1.2.1.25.3.3.1.2.1



This script uses the **`snmpget`** utility and the appropriate parameters to query the Panorama IP address for the CPU OID.

For more information about using SNMP to monitor Palo Alto Networks firewalls and Panorama, log in to **live.paloaltonetworks.com** and search for "Enable SNMP Monitoring" to locate the most recent article.

Stop. This is the end of the lab.

Bonus Lab

In this lab, you will create a new API certificate on the firewall. This certificate can then be used to eliminate the API KeyGen warning message you receive when committing a configuration.

These steps can also be used on Panorama to update the API KeyGen algorithm.

Lab Objectives

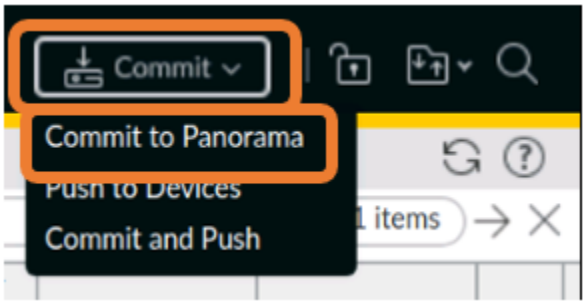
- Modify the Authentication Settings to use a new API Key Certificate

Detailed Lab Steps

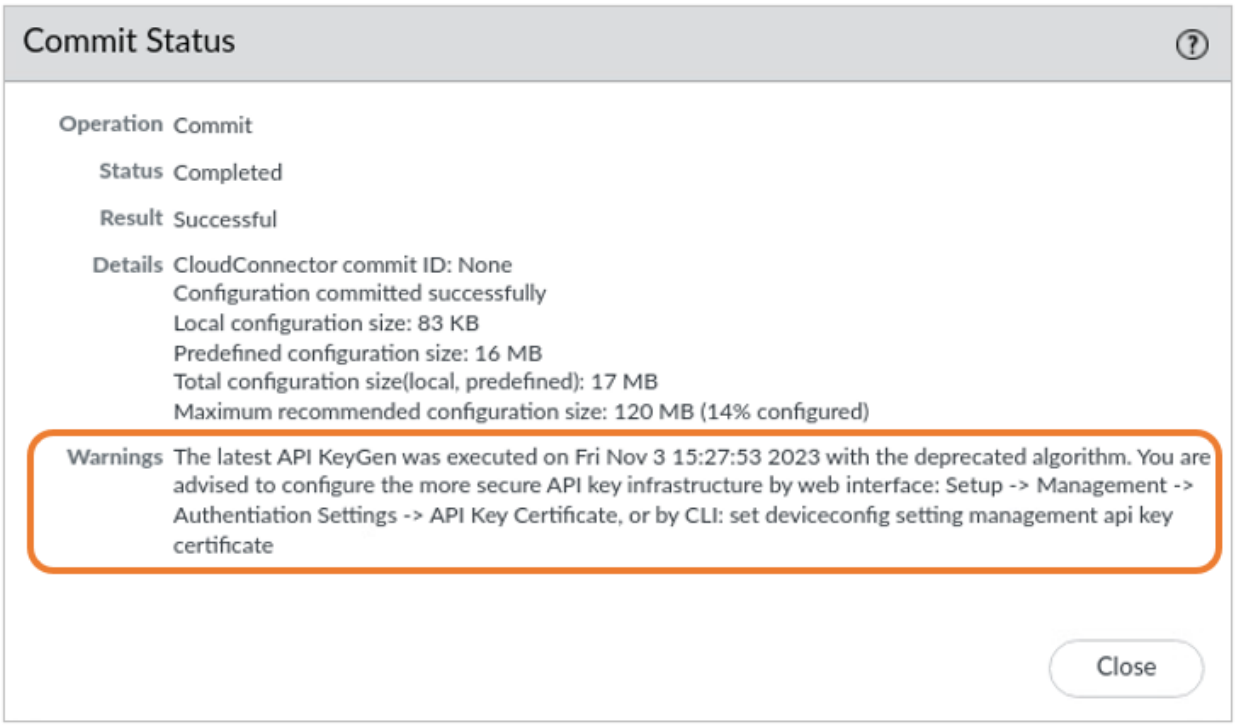
Apply a Baseline configuration to the Firewall

To start this lab exercise, import and load a preconfigured firewall configuration file.

1. Open configuration browser and connect to firewall-a.
2. In the Palo Alto Networks Panorama web interface, select **Device** > **Setup** > **Operations**.
3. Click **Load named configuration snapshot**.
4. Click the drop-down list next to the **Name** text box and select **`edu-220-11.1a-Lab-9-Start.xml`**.
5. Click **OK**.
   A window should open that confirms that the configuration is being loaded.
6. Click **Close**.
7. Click the **Commit** link at the upper right of the web interface, and then select **Commit to Panorama**:



8. :
9. Click **Commit** again and wait until the commit process is complete.
   Note the error message you receive regarding the API KeyGen algorithm:

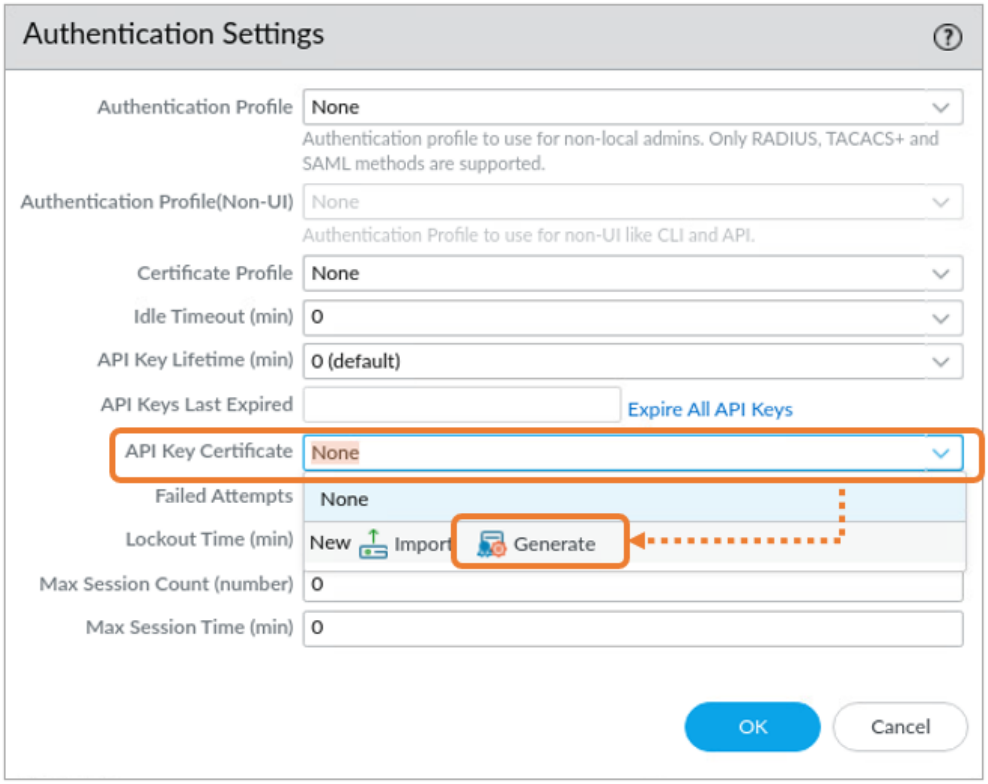


10. Click **Close** to continue.

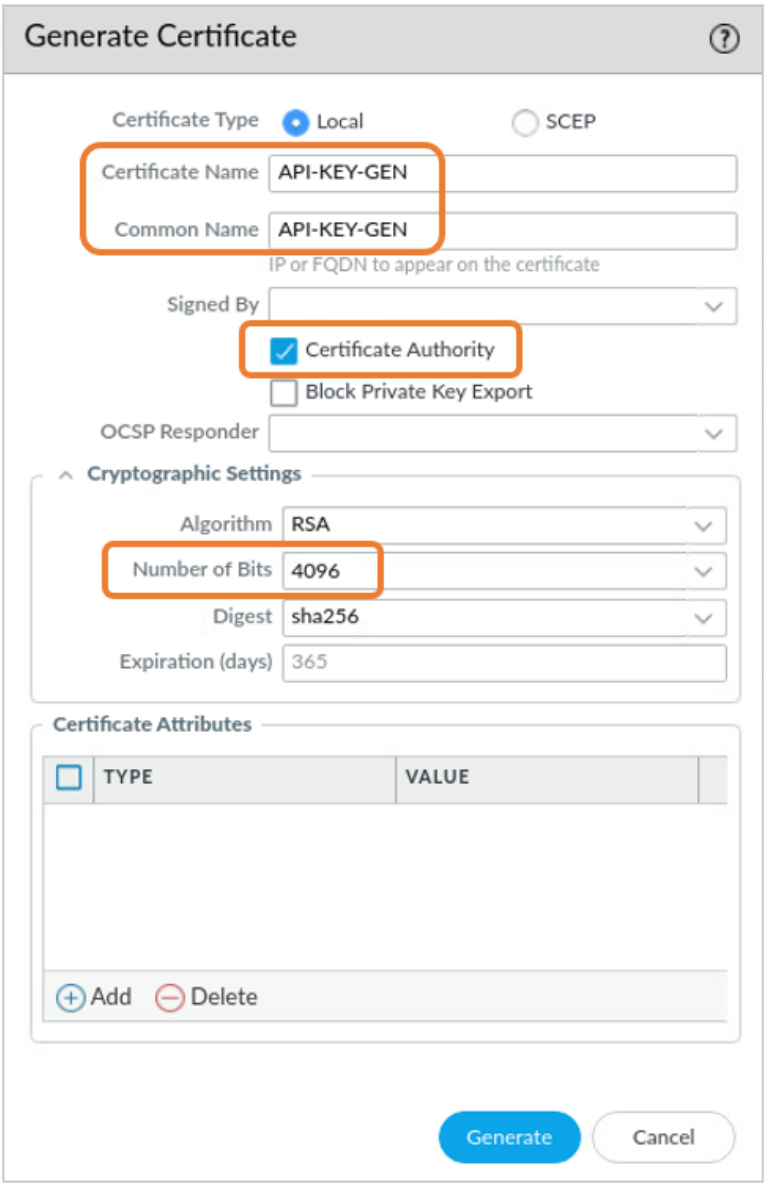
Modify Authentication Settings

In this section, you will create a certificate that Panorama will use to generate API Keys. Doing so will remove the error message you see when you commit a configuration. With this certificate in place, you will not see the error message when committing any configuration files you save from this point forward. If you load an older configuration file (one you created before applying the API Key certificate), you will receive the error message.

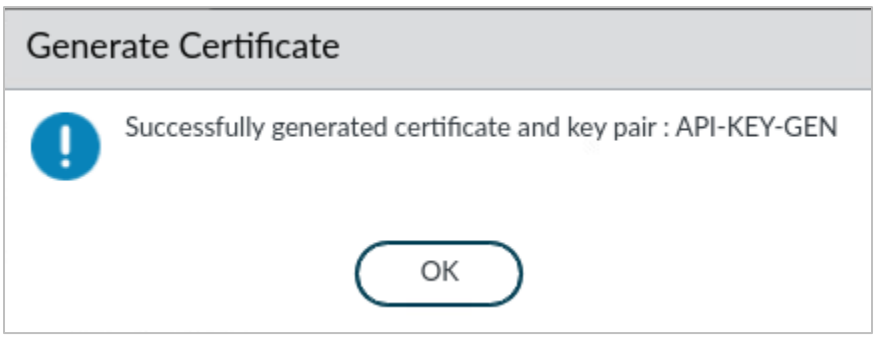
11. Go to **Panorama > Setup > Management**.
12. Scroll down and locate the section for **Authentication Settings**.
13. Click the gear icon to edit this section.
14. In the field labeled **API Key Certificate**, use the dropdown box to select **Generate**.



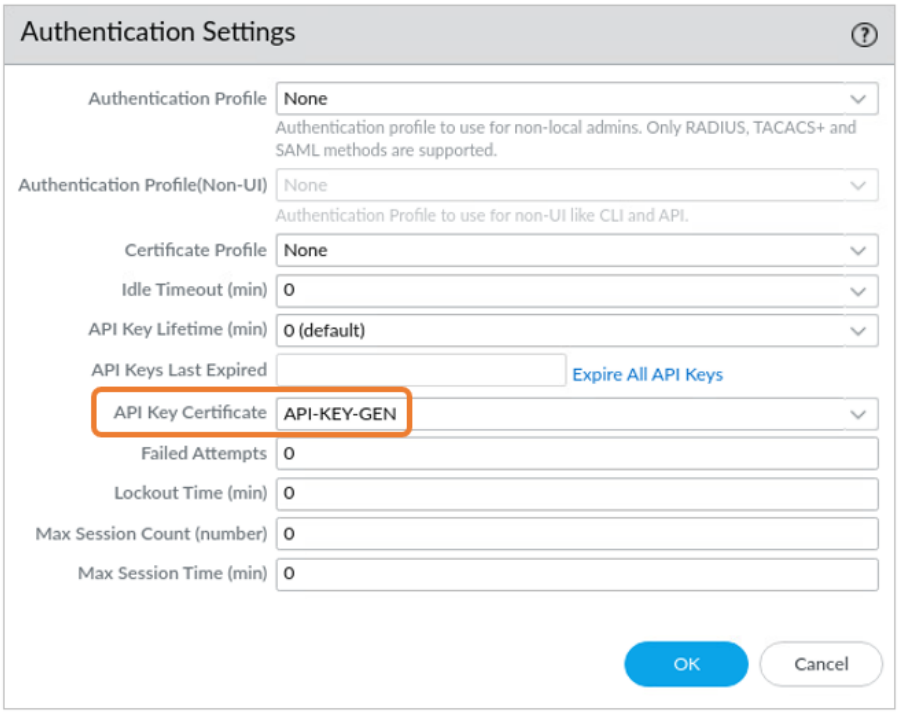
15. In the **Generate Certificate** window, enter **`API-KEY-GEN`** for Certificate Name.
16. For Common name, also enter **`API-KEY-GEN`**.
17. Check the **box** for Certificate Authority.
18. Under Cryptographic Settings, change the Number of Bits to **`4096`**.
19. Leave the remaining settings unchanged.



20. Click **Generate**.
21. Click **OK** on the Generate Certificate message box.



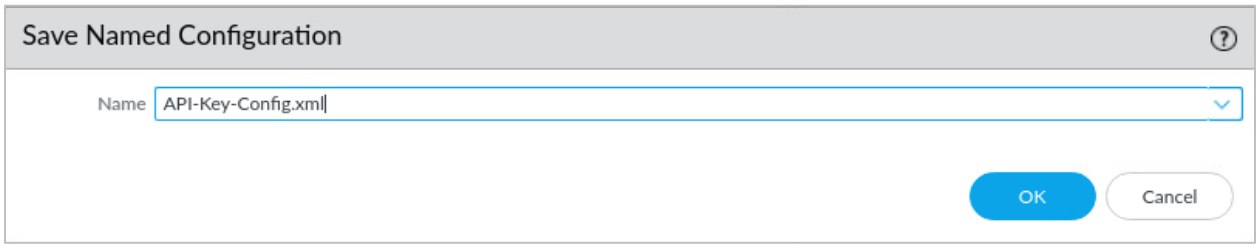
22. Your Authentication Settings window should now display the API-KEY-GEN certificate in the API Key Certificate field.



23. Leave the remaining settings unchanged.
24. Click **OK** to close the **Authentication Settings** window.
25. Click **Yes** to close the **API Key Certificate Change** window
26. Click the **Commit** link at the upper right of the web interface.
27. Click **Commit to Panorama** and wait until the commit process is complete.
28. Click **Commit** again and wait until the commit process is complete.
29. Click **Close** to continue.

Save the Configuration

30. Under **Panorama > Setup > Operations > Configuration Management**, click **Save named Panorama configuration snapshot**.
31. In the **Save Named Configuration** window, enter **`API-Key-Config.xml`** for Name.

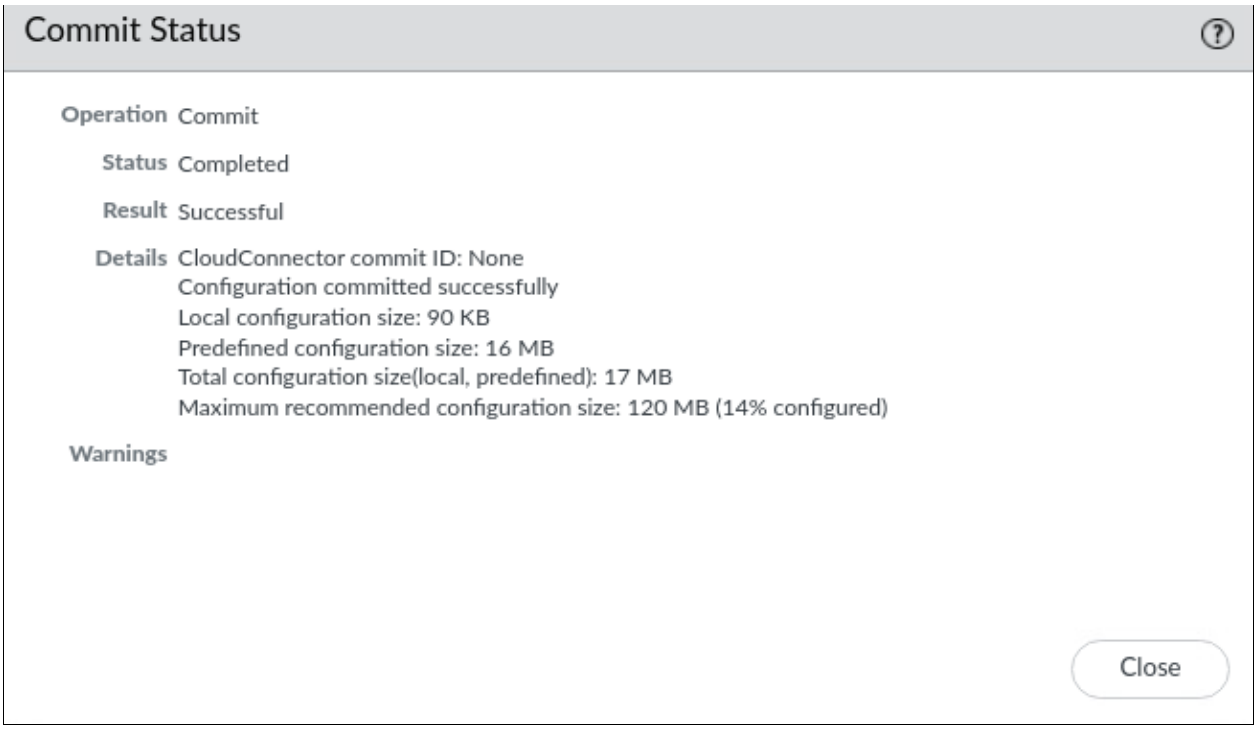


32. Click **OK**.

33. Click **Close** on the **Save Named Configuration** message window.
34. Under **Device > Setup > Operations**, click **Load named Panorama configuration snapshot**.
35. For **Name**, use the drop-down list to select the **`API-Key-Config.xml`** file.
36. Click **OK** to close the Load Named Configuration window.
37. Click **OK** to close the Loading Configuration message box.

Commit Your Changes and Verify Fix

38. Click the **Commit** link at the upper right of the web interface.
39. Click **Commit to Panorama, Commit again** and wait until the commit process is complete.
40. When the process is complete, note that you no longer receive any error messages regarding the API KeyGen algorithm.



41. Click **Close** when the Commit Status is complete.

Any configuration files you save on Panorama will now use the updated API Key Certificate.