Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide describes how to set up and use Panorama™ for centralized management; it is intended for administrators who want the basic framework to quickly set up the Panorama virtual appliance or the M-Series appliance for centralized administration of Palo Alto Networks firewalls.

If you have an M-Series appliance, this guide takes over after you finish rack mounting your M-Series appliance.

For more information, refer to the following sources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://www.paloaltonetworks.com/documentation or search the documentation.

- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to https://live.paloaltonetworks.com.

- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.

- For the most current PAN-OS and Panorama 7.1 release notes, go to https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os-release-notes.html.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
Manage Firewalls

To use Panorama for managing Palo Alto Networks firewalls, you must add the firewalls as managed devices and then assign them to device groups and to templates or template stacks. The following tasks best suit a first-time firewall deployment. Before proceeding, review Plan Your Deployment to understand the deployment options.

- Add a Firewall as a Managed Device
- Manage Device Groups
- Manage Templates and Template Stacks
- Transition a Firewall to Panorama Management
- Use Case: Configure Firewalls Using Panorama

To view the Objects and Policies tabs on the Panorama web interface, you must first create at least one device group. To view the Network and Device tabs, you must create at least one template. These tabs contain the options by which you configure and manage the firewalls on your network.
Add a Firewall as a Managed Device

To use Panorama for central management of firewalls, the first step is to add them as managed devices. Before starting, collect the firewall serial numbers and prepare each firewall as follows:

- **Perform initial configuration** on the firewall so that it is accessible and can communicate with Panorama over the network.
- **Add the Panorama IP address(es)** (one server or two, if Panorama is configured in a high availability pair) in the Panorama Settings section of the **Device > Setup > Management** tab and commit the changes.
- **Set up the data interfaces.** For each interface you plan to use, select the interface type and attach it to a security zone so that you can push configuration and policy from Panorama.

You can then add the firewalls as managed devices on Panorama.

When you add a firewall as a managed device, it uses an SSL connection with AES-256 encryption to register with Panorama. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.

### Add a Firewall as a Managed Device

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Add the firewall to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select Panorama &gt; Managed Devices and click Add.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter the serial number for each firewall (one entry per line) that you want to manage centrally using Panorama, and then click OK. The Managed Devices page displays the new firewall.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>(Optional)</strong> Add a Tag. Tags make it easier for you to find a firewall from a large list; they help you to dynamically filter and refine the list of firewalls that display. For example, if you add a tag called branch office, you can filter for all branch office firewalls across your network.</td>
</tr>
<tr>
<td>a.</td>
<td>Select the check box beside the firewall and click Tag.</td>
</tr>
<tr>
<td>b.</td>
<td>Click Add, enter a string of up to 31 characters (no empty spaces), and click OK.</td>
</tr>
<tr>
<td>4.</td>
<td>Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Verify that the firewall is connected to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the Panorama &gt; Managed Devices page, the Device State column displays whether the firewall is connected or disconnected to Panorama.</td>
<td></td>
</tr>
</tbody>
</table>
Manage Device Groups

- Add a Device Group
- Create a Device Group Hierarchy
- Create Objects for Use in Shared or Device Group Policy
- Revert to Inherited Object Values
- Manage Unused Shared Objects
- Manage Precedence of Inherited Objects
- Move or Clone a Policy Rule or Object to a Different Device Group
- Select a URL Filtering Vendor on Panorama
- Push a Policy Rule to a Subset of Firewalls
- Manage the Rule Hierarchy

Add a Device Group

After adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. PAN-OS doesn’t synchronize pushed rules across HA peers. To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.

Add a Device Group

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Panorama &gt; Device Groups, and click Add.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter a unique Name and a Description to identify the device group.</td>
</tr>
</tbody>
</table>
| Step 3 | In the Devices section, select check boxes to assign firewalls to the group. To search a long list of firewalls, use the Filters.  
You can assign any firewall to only one device group. You can assign each virtual system on a firewall to a different device group. |
| Step 4 | (Optional) Select Group HA Peers for firewalls that are HA peers.  
The firewall name of the passive or active-secondary peer is in parentheses. |
| Step 5 | Select the Parent Device Group (default is Shared) that will be just above the device group you are creating in the device group hierarchy. |
| Step 6 | If your policy rules will reference users and groups, assign a Master firewall. This will be the only firewall in the device group from which Panorama gathers username and user group information. |
| Step 7 | Click OK and Commit, for the Commit Type select Panorama, and click Commit again. |
| Step 8 | Click Commit, for the Commit Type select Device Group, select the device group you just created, and click Commit again. |
## Create a Device Group Hierarchy

| Create a Device Group Hierarchy | 1. Decide the device group levels, and which firewalls and virtual systems you will assign to each device group and the Shared location. You can assign any one firewall or virtual system (vsys) to only one device group. If a device group will be just an organizational container for lower level device groups, you don’t need to assign firewalls to it.  
2. Remove firewall or vsys assignments from existing device groups if those assignments don’t fit your planned hierarchy.  
   a. Select Panorama > Device Groups and select the device group.  
   b. In the Devices section, clear the check boxes of firewalls and virtual systems you want to remove, and click OK.  
3. If necessary, add more firewalls that you will assign to device groups: see Add a Firewall as a Managed Device. |
|---|---|
| Step 1 Plan the Device Group Hierarchy. | 1. In the Panorama > Device Groups page, click Add and enter a Name to identify the device group.  
2. In the Devices section, select check boxes to assign firewalls and virtual systems to the device group.  
3. Leave the Parent Device Group option at Shared (the default) and click OK. |
| Step 2 For each top-level device group, Add a Device Group. | • For new device groups at each lower level, repeat Step 2 but set the Parent Device Group to a device group at the next level above.  
• For each existing device group, in the Device Groups page, select the device group to edit it, select a Parent Device Group, and click OK.  
If you move a device group to a different parent, all its descendant device groups move with it, along with all firewalls, policy rules, and objects associated with the device group and its descendants. If the new parent is in another access domain, the moved device group will no longer have membership in the original access domain. If the new access domain has read-write access for the parent device group, it will also have read-write access for the moved device group. If the new access domain has read-only access for the parent, it will have no access for the moved device group. To reconfigure access for device groups, see Configure an Access Domain. |
| Step 3 For each lower-level device group, Add a Device Group. |
### Create a Device Group Hierarchy (Continued)

**Step 4** Configure, move, and clone objects and policy rules as needed to account for inheritance in the device group hierarchy.

- Create Objects for Use in Shared or Device Group Policy, or edit existing objects. You can edit objects only at their location: the device group to which they are assigned. Descendant device groups inherit read-only instances of the objects from that location. However, you can optionally Override inherited object values.
- Create or edit policies.
- Move or Clone a Policy Rule or Object to a Different Device Group.

**Step 5** Override inherited object values. Applicable only if object values in a particular device group must differ from the values inherited from an ancestor device group. After overriding an object, you can override it again in descendant device groups. However, you can never override shared or predefined (default) objects.

- In the **Objects** tab, select the object type (for example, **Objects > Addresses**).
- Select the **Device Group** that will have the override instance.
- Edit the values. You can’t edit the **Name** or **Shared** settings.
- Click **OK**. The Name column displays a yellow-overlapping-green icon for the object to indicate it is overridden.

  If necessary, you can later **Revert to Inherited Object Values**.

**Step 6** Save and commit your changes. Perform a Panorama and device group commit after any change to the hierarchy. You must also perform a template commit if a template references objects in a device group (for example, interfaces referencing addresses), and a firewall assigned to the template is no longer assigned to that device group because of a hierarchy change.

### Create Objects for Use in Shared or Device Group Policy

You can use an object in any policy rule that is in the Shared location, or in the same device group as the object, or in descendants of that device group (for details, see Device Group Objects).
### Create Objects for Use in Shared or Device Group Policy

- **Create a shared object.**
  In this example, we add a shared object for URL Filtering categories for which we want to trigger alerts.

1. Select the **Objects > Security Profiles > URL Filtering** tab and click **Add**.
   The **Objects** tab appears only after you **Add a Device Group** (at least one).
2. Enter a **Name** and a **Description**.
3. Select the **Shared** check box.
4. The **Disable Override** check box is cleared by default, which means you can override inherited instances of the object in all device groups. To disable overrides for the object, select the check box.
5. In the **Categories** tab, select the check box of every Category for which you want notification.
6. In the **Action** column, select **Alert**.
7. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

- **Create a device group object.**
  In this example, we add an address object for specific web servers on your network.

1. Select **Objects > Addresses** and select the **Device Group** in which you will use the object.
2. Click **Add** and enter a **Name** to identify the object.
3. Be sure to leave the **Shared** check box cleared.
4. The **Disable Override** check box is cleared by default, which means you can override inherited instances of the object in device groups that are descendants of the selected **Device Group**. To disable overrides for the object, select the check box.
5. Select the **Type** of address object and the associated value. For example, select **IP Range** and enter the IP address range for the web servers.
6. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.
7. Click **Commit**, for the **Commit Type** select **Device Group**, select the device group to which you added the object, and click **Commit** again.

- **View shared objects and device group objects in Panorama.**

  In the pages of the **Objects** tab, the Location column indicates whether an object is shared or is specific to a device group.

1. In the **Objects** tab, select the object type (**Objects > Addresses**, in this example).
2. Select the **Device Group** to which you added the object.
   The **Objects** tab only displays objects that are in the selected **Device Group** or are inherited from an ancestor device group or the Shared location.
3. Verify that the device group object appears. Note that the device group name in the Location column matches the selection in the **Device Group** drop-down.
Revert to Inherited Object Values

After overriding the values that a device group object inherits from an ancestor device group, you can revert the object to its ancestor values at any time. In the Objects tab, overridden objects have a yellow-overlapping-green icon (惫) in the Name column.

If you want to push ancestor values to all overridden objects instead of reverting a specific object, see Manage Precedence of Inherited Objects.
For the steps to override values, see Override inherited object values.
For details on object inheritance and overrides, see Device Group Objects.

Revert an Overridden Object

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Objects tab, select the object type (for example, Objects &gt; Addresses) and select the Device Group that has an override instance of the object.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the object, click Revert, and click Yes. The Name column displays a green icon for the object, indicating that it now inherits all values from an ancestor device group.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Commit, for the Commit Type select Device Group, select the device group in which you reverted the object, and click Commit again.</td>
</tr>
</tbody>
</table>

Manage Unused Shared Objects

When you commit Device Groups, by default Panorama pushes all shared objects to firewalls whether or not any shared or device group policy rules reference the objects. However, you can configure Panorama to push only the shared objects that rules reference in the device groups you commit. The Share Unused Address and Service Objects with Devices check box enables you to limit the objects that Panorama pushes to the managed firewalls.

On smaller firewalls, such as the PA-200, consider pushing only the relevant shared objects to the managed firewalls. This is because the number of objects that can be stored on a smaller firewall is considerably lower than that of the mid-size and larger models. Also, if you have many address and service objects that are unused, clearing the Share Unused Address and Service Objects with Devices check box reduces the commit times significantly on the firewalls because the configuration pushed to each firewall is smaller. Disabling this option may, however, increase the commit time on Panorama. This is because Panorama has to dynamically check whether policy rules reference a particular object.

| Step 1 | Select Panorama > Setup > Management, and edit the Panorama Settings. |
| Step 2 | Clear the Share Unused Address and Service Objects with Devices check box to push only the shared objects that rules reference, or select the check box to re-enable pushing all shared objects. |
| Step 3 | Click OK and Commit, for the Commit Type select Panorama, and click Commit again. |
Manage Precedence of Inherited Objects

By default, when device groups at different levels in the Device Group Hierarchy have an object with the same name but different values (because of overrides, as an example), policy rules in a descendant device group use the object values in that descendant instead of using object values inherited from ancestor device groups. Optionally, you can reverse this order of precedence to push values from the highest ancestor containing the object to all descendant device groups. After you enable this option, the next device group commit replaces any overridden objects in the descendant device groups with the inherited objects.

⚠️ If a firewall has locally defined objects with the same name as shared or device group objects that Panorama pushes, a commit failure occurs.
If you want to revert a specific overridden object to its ancestor values instead of pushing ancestor values to all overridden objects, see Revert to Inherited Object Values.

<table>
<thead>
<tr>
<th>Manage Precedence of Inherited Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
</tbody>
</table>

Move or Clone a Policy Rule or Object to a Different Device Group

On Panorama, if a policy rule or object that you will move or clone from a device group has references to objects that are not available in the target device group (Destination), you must move or clone the referenced objects and the referencing rule or object in the same operation. In a Device Group Hierarchy, remember that referenced objects might be available through inheritance. For example, shared objects are available in all device groups. You can perform a global find to check for references. If you move or clone an overridden object, be sure that overrides are enabled for that object in the parent device group of the Destination (see Create Objects for Use in Shared or Device Group Policy).

<table>
<thead>
<tr>
<th>Move or Clone a Policy Rule or Object to a Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Move or Clone a Policy Rule or Object to a Device Group (Continued)

Step 4 In the Destination drop-down, select the new device group or Shared. The default is the Device Group selected in Step 2.

Step 5 (Rules only) Select the Rule order:
• Move top (default)—The rule will come before all other rules.
• Move bottom—The rule will come after all other rules.
• Before rule—In the adjacent drop-down, select the rule that comes after the Selected Rules.
• After rule—In the adjacent drop-down, select the rule that comes before the Selected Rules.

Step 6 The Error out on first detected error in validation check box is selected by default, which means Panorama will display the first error it finds and stop checking for more errors. For example, an error occurs if the Destination device group doesn’t have an object that is referenced in the rule you are moving. When you move or clone many items at once, selecting this check box can simplify troubleshooting. If you clear the check box, Panorama will find all the errors before displaying them. Regardless of this setting, Panorama won’t move or clone anything until you fix all the errors for all the selected items.

Step 7 Click OK to start the error validation. If Panorama finds errors, fix them and retry the move or clone operation. If Panorama doesn’t find errors, it performs the operation.

Step 8 Click Commit, for the Commit Type select Panorama, and click Commit again.

Step 9 Click Commit, for the Commit Type select Device Group, select the original and destination device groups, and click Commit again.

Select a URL Filtering Vendor on Panorama

URL filtering enables firewalls to monitor and control web access for your users. The policy rules that you configure to control web access (Security, QoS, Captive Portal, and Decryption rules) reference URL categories. The URL filtering vendor you select on Panorama determines which URL categories are available for referencing in the rules that you add to device groups and push to firewalls.

By default, Panorama uses PAN-DB, a URL filtering database that is tightly integrated into PAN-OS and the Palo Alto Networks threat intelligence cloud. PAN-DB provides high-performance local caching to maximize in-line performance for URL lookups. The other vendor option is BrightCloud, a third-party URL database.

Unlike firewalls, Panorama does not download the URL database and does not require a URL filtering license.

The following topics describe how to change the URL filtering vendor on Panorama or on both Panorama and managed firewalls. You can also change the URL filtering vendor on just the firewalls.

- Must Panorama and Firewalls Have Matching URL Filtering Vendors?
- Change the URL Filtering Vendor on HA Panorama
- Change the URL Filtering Vendor on non-HA Panorama
- Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB
- Migrate Panorama and non-HA Firewalls from BrightCloud to PAN-DB
Must Panorama and Firewalls Have Matching URL Filtering Vendors?

On any single Panorama management server or firewall, only one URL filtering vendor can be active: PAN-DB or BrightCloud. When selecting a vendor for Panorama, you must consider the vendor and PAN-OS version of the managed firewalls:

- PAN-OS 5.0.x and earlier versions—Panorama and the firewalls require matching URL filtering vendors.
- PAN-OS 6.0 or later versions—Panorama and the firewalls do not require matching URL filtering vendors. If a vendor mismatch is detected, the firewall maps the URL categories in the URL Filtering profiles and rules that it received from Panorama to URL categories that align with those of the vendor enabled on the firewall.

Therefore, for a deployment in which some firewalls run PAN-OS 6.0 or later and some firewalls run earlier PAN-OS versions, Panorama must use the same URL filtering vendor as the firewalls that run earlier PAN-OS versions. For example, if firewalls that run PAN-OS 5.0 use PAN-DB, and firewalls that run PAN-OS 7.0 use BrightCloud, Panorama must use PAN-DB.

Change the URL Filtering Vendor on HA Panorama

In a high availability (HA) deployment, each Panorama peer must be in a non-functional state when you change the URL filtering vendor. Therefore, to avoid disrupting Panorama operations, change the URL filtering vendor on the passive Panorama (Panorama2 in this example) and then trigger failover before changing the vendor on the active Panorama (Panorama1 in this example).

<table>
<thead>
<tr>
<th>Change URL Filtering Vendor on HA Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
</tbody>
</table>

| 1. | Log in to the Panorama web interface. |
| 2. | Select **Panorama > High Availability** and **Suspend local Panorama**. When you perform this step on Panorama1, failover occurs and Panorama2 becomes active. |
| 3. | Select **Panorama > Setup > Management** and edit the General Settings. |
| 4. | Select the **URL Filtering Database** vendor: **paloaltonetworks** (PAN-DB) or **brightcloud**. |
| 5. | Select **Panorama > High Availability** and **Make local Panorama functional**. When you perform this step on Panorama1 with **preemption** enabled on both HA peers, Panorama1 automatically reverts to active status and Panorama2 reverts to passive status. |

| 1. | Select **Objects > Security Profiles > URL Filtering**. |
| 2. | Click **Add** and verify that the **Categories** tab of the URL Filtering profile dialog displays the URL categories associated with the selected vendor. |

Change the URL Filtering Vendor on non-HA Panorama

Perform this procedure to change the URL filtering vendor on a Panorama management server that is not deployed in a high availability (HA) configuration.
### Change URL Filtering Vendor on non-HA Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
2. Select the URL Filtering Database vendor: paloaltonetworks (PAN-DB) or brightcloud. |
| 2.   | Verify that the URL categories are available for referencing in policies. | 1. Select Objects > Security Profiles > URL Filtering.  
2. Click Add and verify that the Categories tab of the URL Filtering profile dialog displays the URL categories associated with the selected vendor. |

### Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB

Perform this procedure to migrate the URL filtering vendor from BrightCloud to PAN-DB on Panorama and firewalls when the firewalls are deployed in a high availability (HA) configuration. In this example, the active (or active-primary) firewall is named fw1 and the passive (or active-secondary) firewall is named fw2. The migration automatically maps BrightCloud URL categories to PAN-DB URL categories.

### Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 1.   | Determine which firewalls require new PAN-DB URL filtering licenses. | 1. Log in to Panorama and select Panorama > Device Deployment > Licenses.  
2. Check the URL column to determine which firewalls have PAN-DB licenses and whether the licenses are valid or expired.  
A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be active.  
If you’re not sure whether a PAN-DB URL filtering license is active, access the firewall web interface, select Device > Licenses, and verify that the Active field displays Yes in the PAN-DB URL Filtering section.  
3. Purchase a new license for each firewall that does not have a valid PAN-DB license.  
In HA deployments, each firewall peer needs a distinct PAN-DB license and authorization code. Palo Alto Networks sends an email containing activation codes for the licenses you purchase. If you can’t find this email, contact Customer Support before proceeding. |
| 2.   | Change the URL filtering vendor to PAN-DB on Panorama. | Access the Panorama web interface and perform one of the following tasks:  
• Change the URL Filtering Vendor on HA Panorama  
• Change the URL Filtering Vendor on non-HA Panorama |
| 3.   | Configure the TCP session settings on both firewall HA peers to ensure sessions that are not yet synchronized will fail over when you suspend a peer. | Log in to the CLI of each firewall and run the following command:  
• set session tcp-reject-non-syn no |
Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB (Continued)

Step 4  Migrate the URL filtering vendor to PAN-DB on each firewall HA peer.

1. Access the firewall web interface, select Device > High Availability > Operational Commands, and Suspend local device.
   Performing this step on fw1 triggers failover to fw2.

2. Select Device > Licenses.

3. In the License Management section, select Activate feature using authorization code, enter the Authorization Code and click OK.
   Activating the PAN-DB license automatically deactivates the BrightCloud license.

4. In the PAN-DB URL Filtering section, Download the seed file, select your region, and click OK.

5. Access the Panorama web interface, click Commit, set the Commit Type to Device Group, select the firewall, and click Commit again.

6. Access the firewall web interface, select Device > High Availability > Operational Commands, and Make local device functional.
   When you perform this step on fw1 with preemption enabled on both firewalls, fw1 automatically reverts to active (or active-primary) status and fw2 reverts to passive (or active-secondary) status.

Step 5  Revert both firewall HA peers to the original TCP session settings.

Run the following command at the CLI of each firewall:

```
> set session tcp-reject-non-syn yes
```

Migrate Panorama and non-HA Firewalls from BrightCloud to PAN-DB

Perform this procedure to migrate the URL filtering vendor from BrightCloud to PAN-DB on Panorama and firewalls when the firewalls are not deployed in a high availability (HA) configuration. The migration automatically maps BrightCloud URL categories to PAN-DB URL categories.
Migrate Panorama and non-HA Firewalls from BrightCloud to PAN-DB

**Step 1**  Determine which firewalls require new PAN-DB URL filtering licenses.

1. Log in to Panorama and select **Panorama > Device Deployment > Licenses**.
2. Check the URL column to determine which firewalls have PAN-DB licenses and whether the licenses are valid or expired.
   A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be active.
   If you're not sure whether a PAN-DB URL filtering license is active, access the firewall web interface, select **Device > Licenses**, and verify that the **Active** field displays **Yes** in the PAN-DB URL Filtering section.
3. Purchase new licenses for the firewalls that don't have valid PAN-DB licenses.
   Palo Alto Networks sends an email containing activation codes for the licenses you purchase. If you can't find this email, contact Customer Support before proceeding.

**Step 2**  Change the URL filtering vendor to PAN-DB on Panorama.

Access the Panorama web interface and perform one of the following tasks:

- Change the URL Filtering Vendor on HA Panorama
- Change the URL Filtering Vendor on non-HA Panorama

**Step 3**  Migrate the URL filtering vendor to PAN-DB on each firewall.

1. Access the firewall web interface and select **Device > Licenses**.
2. In the License Management section, select **Activate feature using authorization code**, enter the **Authorization Code**, and click **OK**.
   Activating the PAN-DB license automatically deactivates the BrightCloud license.
3. In the PAN-DB URL Filtering section, **Download** the seed file, select your region, and click **OK**.
4. In the Panorama web interface, click **Commit**, set the **Commit Type** to **Device Group**, select the firewall, and click **Commit** again.

Push a Policy Rule to a Subset of Firewalls

A policy target allows you to specify the firewalls in a device group to which to push policy rules. It allows you to exclude one or more firewalls or virtual systems, or to apply a rule only to specific firewalls or virtual systems in a device group.

The ability to target a rule enables you to keep policies centralized on Panorama; it offers visibility and efficiency in managing the rules. Instead of creating local rules on a only or virtual system, targeted rules allow you to define the rules (as shared or device group pre- or post-rules) on Panorama (for details, see **Device Group Policies**).
### Push a Policy Rule to a Subset of Firewalls

| Step 1 | Create a rule.  
| In this example, we define a pre-rule in the Security rulebase that permits users on the internal network to access the servers in the DMZ. |

| Step 2 | Target the rule to include or exclude a subset of firewalls. |

| To apply the rule to a selected set of firewalls: |
| 1. Select the **Target** tab in the Policy Rule window. |
| 2. Select the firewalls on which you want the rule to apply.  
| If you do not select firewalls to target, the rule is added to all of the (unchecked) firewalls in the device group. |
| By default, although the check box for the virtual systems in the device group is unchecked, all the virtual systems will inherit the rule on commit. Select the check box for one or more virtual systems to which you want the rule to apply. |
| 3. (Optional) To exclude a subset of firewalls from inheriting the rule, select the check box **Install on all but specified devices**.  
| If you select **Install on all but specified devices** and do not select any firewall, the rule is added to none of the firewalls in the device group. |
| 4. Click **OK** to add the rule. |
| 5. Save the configuration changes. |
| a. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again. |
| b. Click **Commit**, for the **Commit Type** select **Device Group**, select the device group to which you just added the rule, and click **Commit** again. |

### Manage the Rule Hierarchy

The order of policy rules is critical for the security of your network. Within any policy layer (shared, device group, or locally defined rules) and rulebase (for example, shared Security pre-rules), the firewall evaluates rules from top to bottom in the order they appear in the pages of the **Policies** tab. The firewall matches a packet against the first rule that meets the defined criteria and ignores subsequent rules. Therefore, to enforce the most specific match, move the more specific rules above more generic rules.
Manage Firewalls

Manage the Rule Hierarchy

<table>
<thead>
<tr>
<th>Step 1</th>
<th>View the rule hierarchy for each rulebase.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the Policies tab and click Preview Rules.</td>
</tr>
<tr>
<td>2.</td>
<td>Filter the preview by Rulebase (for example, Security or QoS).</td>
</tr>
<tr>
<td>3.</td>
<td>Filter the preview to display the rules of a specific Device Group and the rules it inherits from the Shared location and ancestor device groups. You must select a device group that has firewalls assigned to it.</td>
</tr>
<tr>
<td>4.</td>
<td>Filter the preview by Device to display its locally defined rules.</td>
</tr>
<tr>
<td>5.</td>
<td>Click the green arrow icon to apply your filter selections to the preview (see Figure: Rule Hierarchy).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Delete or disable rules, if necessary.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To determine which rules a firewall doesn't currently use, select that firewall in the Context drop-down on Panorama, select the rulebase (for example, Policies &gt; Security), and select the Highlight Unused Rules check box. A dotted orange background indicates the rules that the firewall doesn't use.</td>
</tr>
<tr>
<td>1.</td>
<td>Select the rulebase (for example, Policies &gt; Security &gt; Pre Rules) that contains the rule you will delete or disable.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the Device Group that contains the rule.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the rule, and click Delete or Disable as desired. Disabled rules appear in italicized font.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Reposition rules within a rulebase, if necessary.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To reposition local rules on a firewall, access its web interface by selecting that firewall in the Context drop-down before performing this step.</td>
</tr>
<tr>
<td>1.</td>
<td>Select the rulebase (for example, Policies &gt; Security &gt; Pre Rules) that contains the rule you will move.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the Device Group that contains the rule.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the rule, select Move, and select:</td>
</tr>
<tr>
<td></td>
<td>• Move Top—Moves the rule above all other rules in the device group (but not above rules inherited from Shared or ancestor device groups).</td>
</tr>
<tr>
<td></td>
<td>• Move Up—Moves the rule above the one that precedes it (but not above rules inherited from Shared or ancestor device groups).</td>
</tr>
<tr>
<td></td>
<td>• Move Down—Moves the rule below the one that follows it.</td>
</tr>
<tr>
<td></td>
<td>• Move Bottom—Moves the rule below all other rules.</td>
</tr>
<tr>
<td></td>
<td>• Move to other device group—See Move or Clone a Policy Rule or Object to a Different Device Group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>If you modified the rules, save the changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Commit, for the Commit Type select Device Group, select the device group that contains the rules you changed or deleted, and click Commit again.</td>
</tr>
</tbody>
</table>
Manage Templates and Template Stacks

Use templates and template stacks to define the common base configurations that enable firewalls to operate in your network. See Templates and Template Stacks for an overview of the issues you should consider when deciding which firewalls to add to which templates, ordering templates in a stack to manage layers of common and firewall group-specific settings, and overriding template settings with firewall-specific values.

To delete a template, you must first locally Disable/Remove Template Settings on the firewall. Only administrators with the superuser role can disable a template.

▲ Template Capabilities and Exceptions
▲ Add a Template
▲ Configure a Template Stack
▲ Override a Template Setting
▲ Disable/Remove Template Settings

Template Capabilities and Exceptions

You can use Templates and Template Stacks to define a wide array of settings, but you can perform the following tasks only locally on each managed firewall:

- Configure a device block list.
- Clear logs.
- Enable operational modes such as multi-vsys mode, Federal Information Processing Standards (FIPS) mode, or Common Criteria (CC) mode.
- Configure the IP addresses of a firewall HA pair.
- Configure a master key and diagnostics.
- Compare configuration files (Config Audit).

To Manage Licenses and Updates (software or content) for firewalls, use Panorama tab options, not templates.

Add a Template

You must add at least one template before Panorama will display the Device and Network tabs required to define the network set up and device configuration elements for firewalls. Panorama supports up to 512 templates.

You can avoid duplicating many configurations among templates by combining them into a template stack: see Templates and Template Stacks and Configure a Template Stack.
# Add a Template

**Step 1** Add a template.

1. Select **Panorama > Templates**.
2. Click **Add** and enter a unique **Name** to identify the template.
3. If the template has a virtual system (vsys) with configurations (for example, interfaces) that you want Panorama to push to firewalls that don’t have virtual systems, select it in the **Default VSYS** drop-down.
4. In the **Devices** section, select check boxes to assign firewalls to the template.

   Whenever you add a new managed firewall to Panorama, you must assign it to the appropriate template; Panorama does not automatically assign new firewalls. When you perform a template commit, Panorama pushes the configuration to every firewall assigned to the template.

5. **(Optional)** Select **Group HA Peers** to display a single check box for firewalls that are in a high availability (HA) configuration. Icons indicate the HA state: green for active and yellow for passive. The firewall name of the secondary peer is in parentheses.

   For active/passive HA, add both peers to the same template so that both will receive the configurations. For active/active HA, whether you add both peers to the same template depends on whether each peer requires the same configurations. For a list of the configurations that PAN-OS synchronizes between HA peers, see **High Availability Synchronization**.

6. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

7. Click **Commit**, for the **Commit Type** select **Template**, select the firewalls assigned to the template you just added, and click **Commit** again.

**Step 2** Verify that the template is available.

After you add the first template, Panorama displays the **Device** and **Network** tabs. These tabs display a **Template** drop-down. Check that the drop-down displays the template you just added.

**Step 3** Use the template to push a configuration change to firewalls.

> Renaming a vsys is allowed only on the local firewall. If you rename a vsys on Panorama, you will create an entirely new vsys, or the new vsys name may get mapped to the wrong vsys on the firewall.

Let’s define a primary Domain Name System (DNS) server for the firewalls in the template.

1. In the **Device** tab, select the **Template** from the drop-down.
2. Select **Device > Setup > Services > Global**, and edit the Services section.
3. Enter an IP address for the **Primary DNS Server**.
4. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.
5. Click **Commit**, for the **Commit Type** select **Template**, select the firewalls assigned to the template, and click **Commit** again.

© Palo Alto Networks, Inc.  
Panorama 7.1 Administrator’s Guide • 117
Add a Template (Continued)

Step 4  Verify that the firewall is configured with the template settings that you pushed from Panorama.

1. In the Context drop-down, select one of the firewalls to which you pushed the template setting.
2. Select Device > Setup > Services > Global. The IP address that you pushed from the template appears. The Services section header displays a template icon (green cog) to indicate that settings in the section have values pushed from a template.

Configure a Template Stack

A template stack is a combination of templates: Panorama pushes the settings from every template in the stack to the firewalls you assign to that stack. Panorama supports up to 128 template stacks and each stack can have up to 16 templates. For details and planning, see Templates and Template Stacks.

Configure a Template Stack

Step 1  Plan the templates and their order in the stack.

For each template you will assign to the stack, Add a Template.

When planning the priority order of templates within the stack (for overlapping settings), remember that Panorama doesn’t check the order for invalid relationships. For example, consider a stack in which the ethernet1/1 interface is of type Layer 3 in Template_A but of type Layer 2 with a VLAN in Template_B. If Template_A has a higher priority, Panorama will push ethernet1/1 as type Layer 3 but assigned to a VLAN.

Also note that a template configuration can’t reference a configuration in another template, even if both templates are in the same stack. For example, a zone configuration in Template_A can’t reference a zone protection profile in Template_B.

Step 2  Create a template stack.

1. Select Panorama > Templates and click Add Stack.
2. Enter a unique Name to identify the stack.
3. For each of the Templates the stack will combine (up to 16), click Add and select the template. The dialog lists the added templates in order of priority with respect to duplicate settings, where values in the higher templates override those that are lower in the list. To change the order, select a template and click Move Up or Move Down.
4. In the Devices section, select check boxes to assign firewalls. You can’t assign individual virtual systems, only an entire firewall. You can assign any firewall to only one template or stack. After you finish selecting, click OK.
### Configure a Template Stack (Continued)

<table>
<thead>
<tr>
<th>Step 3</th>
<th><strong>Edit the Network and Device settings, if necessary.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>While Panorama pushes mode-specific settings only to firewalls that support those modes, this selective push doesn't adjust mode-specific values. For example, if a template has firewalls in Federal Information Processing Standards (FIPS) mode and an IKE Crypto profile that uses non-FIPS algorithms, the template commit will fail. To avoid such errors, use the <strong>Mode</strong> drop-down in the <strong>Network</strong> and <strong>Device</strong> tabs to filter mode-specific features and value options. In an individual firewall context, you can override settings that Panorama pushes from a stack in the same way you override settings pushed from a template: see <strong>Override a Template Setting</strong>. <strong>Renaming a vsys is allowed only on the local firewall. If you rename a vsys on Panorama, you will create an entirely new vsys, or the new vsys name may get mapped to the wrong vsys on the firewall.</strong></td>
</tr>
</tbody>
</table>
|        | **1.** Depending on the settings you will configure, select the **Network** or **Device** tab and select the stack in the **Template** drop-down. The tab settings are read-only when you select a stack.  
**2.** Filter the tabs to display only the mode-specific settings you want to edit:  
- In the **Mode** drop-down, select or clear the **Multi VSYS**, **Operational Mode**, and **VPN Mode** filter options.  
- Set all the **Mode** options to reflect the mode configuration of a particular firewall by selecting it in the **Device** drop-down.  
**3.** You can edit settings only at the template level, not at the stack level. To identify and access the template that contains the setting you want to edit:  
- If the page displays a table, select **Columns > Template** in the drop-down of any column header. The Template column displays the source template for each setting. If multiple templates have the same setting, the Template column displays the higher priority template. Click the template name in this column: the **Template** drop-down changes to that template, at which point you can edit the setting.  
- If the page doesn't display a table, hover over the template icon (green cog) for a setting; a tooltip displays the source template. If multiple templates have the same setting, the tooltip displays the higher priority template. In the **Template** drop-down, select the template that the tooltip displays to edit the setting.  
**4.** Edit the settings as needed.  
**5.** Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.  
**6.** Click **Commit**, for the **Commit Type** select **Template**, select the firewalls assigned to the template stack, and click **Commit** again. |

<table>
<thead>
<tr>
<th>Step 4</th>
<th><strong>Verify that the template stack works as expected.</strong></th>
</tr>
</thead>
</table>
|        | **Perform the same verification steps as when you Add a Template but select the template stack from the **Template** drop-down:**  
**1.** Use the template to push a configuration change to firewalls.  
**2.** Verify that the firewall is configured with the template settings that you pushed from Panorama. |

### Override a Template Setting

While **Templates and Template Stacks** enable you to apply a base configuration to multiple firewalls, you might want to configure firewall-specific settings that don't apply to all the firewalls in a template or template stack. Overrides allow for exceptions or modifications to meet your deployment needs. For example, if you
use a template to create a base configuration but a few firewalls in a test lab environment need different settings for the Domain Name System (DNS) server IP address or the Network Time Protocol (NTP) server, you can override the template settings.

If you want to disable or remove all the template or stack settings on a firewall instead of overriding a single setting, see Disable/Remove Template Settings.

<table>
<thead>
<tr>
<th>Override a Template Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Access the web interface of the firewall.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Navigate to the setting you will override. In this example, you will override the DNS server IP address that you assigned using a template in Add a Template.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 1</strong></th>
<th><strong>Step 2</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>Device</strong> &gt; <strong>Setup</strong> &gt; <strong>Services</strong> &gt; <strong>Global</strong> and edit the Services section.</td>
<td></td>
</tr>
<tr>
<td>Click the template icon (green cog) for the <strong>Primary DNS Server</strong> to enable overrides for that field.</td>
<td></td>
</tr>
<tr>
<td>Enter a new IP address for the <strong>Primary DNS Server</strong>. Note that the dialog now displays a template override icon (orange-overlapping-green cogs) to indicate that the value is overridden.</td>
<td></td>
</tr>
<tr>
<td>Click <strong>OK</strong> and <strong>Commit</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

Disable/Remove Template Settings

If you want to stop using a template or template stack for managing the configuration on a managed firewall, you can disable the template or stack. When disabling, you can copy the template/stack values to the local configuration of the firewall or delete the values.

If you want to override a single setting instead of disabling or removing every template or stack setting, see Override a Template Setting. See Templates and Template Stacks for details on how to use these for managing firewalls.

<table>
<thead>
<tr>
<th>Disable/Remove Template Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Access the web interface of the managed firewall as an administrator with the Superuser role. You can directly access the firewall by entering its IP address in the browser URL field or, in Panorama, select the firewall in the Context drop-down.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Select <strong>Device</strong> &gt; <strong>Setup</strong> &gt; <strong>Management</strong> and edit the Panorama Settings.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Click <strong>Disable Device and Network Template</strong>.</td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) Select <strong>Import Device and Network Template before disabling</strong>, to save the configuration settings locally on the firewall. If you do not select this option, PAN-OS will delete all Panorama-pushed settings from the firewall.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Click <strong>OK</strong> twice and then click <strong>Commit</strong> to save the changes.</td>
</tr>
</tbody>
</table>
Transition a Firewall to Panorama Management

If you have already deployed Palo Alto Networks firewalls and configured them locally, but now want to use Panorama for centrally managing them, you must perform pre-migration planning. The migration involves importing firewall configurations into Panorama and verifying that the firewalls function as expected after the transition. If some settings are unique to individual firewalls, you can continue accessing the firewalls to manage the unique settings. You can manage any given firewall setting by pushing its value from Panorama or by configuring it locally on the firewall, but you cannot manage the setting through both Panorama and the firewall. If you want to exclude certain firewall settings from Panorama management, you can either:

- Migrate the entire firewall configuration and then, on Panorama, delete the settings that you will manage locally on firewalls. You can also Override a Template Setting that Panorama pushes to a firewall instead of deleting the setting on Panorama.
- Load a partial firewall configuration, including only the settings that you will use Panorama to manage.

Firewalls do not lose logs during the transition to Panorama management.

Plan the Transition to Panorama Management

Plan the Transition to Panorama Management

Migrate a Firewall to Panorama Management

Migrate a Firewall HA Pair to Panorama Management

Load a Partial Firewall Configuration into Panorama

Plan the Transition to Panorama Management

The following tasks are a high-level overview of the planning required to migrate firewalls to Panorama management:

- Decide which firewalls to migrate.
- Determine the Panorama and firewall software and content versions, and how you will Manage Licenses and Updates. For important details, see Panorama, Log Collector, and Firewall Version Compatibility.
- Plan Your Deployment for Panorama with respect to the URL filtering database (BrightCloud or PAN-DB), log collection, and administrator roles.
- Plan how to manage shared settings.
  
  Plan the Device Group Hierarchy, Templates and Template Stacks in a way that will reduce redundancy and streamline the management of settings that are shared among all firewalls or within firewall sets. During the migration, you can select whether to import objects from the Shared location on the firewall into Shared on Panorama, with the following exceptions:

  - If a shared firewall object has the same name and value as an existing shared Panorama object, the import excludes that firewall object.
  - If the name or value of the shared firewall object differs from an existing shared Panorama object, Panorama imports the firewall object into each new device group that is created for the import.
  - If a configuration imported into a template references a shared firewall object, or if a shared firewall object references a configuration imported into a template, Panorama imports the object as a shared
object regardless of whether you select the Import devices’ shared objects into Panorama’s shared context check box.

- Determine if the firewall has configuration elements (policies, objects, and other settings) that you don’t want to import, either because Panorama already contains similar elements or because those elements are firewall-specific (for example, timezone settings) and you won’t use Panorama to manage them. You can perform a global find to determine if similar elements exist on Panorama.
- Decide the common zones for each device group. This includes a zone-naming strategy for the firewalls and virtual systems in each device group. For example, if you have zones called Branch LAN and WAN, Panorama can push policy rules that reference those zones without being aware of the variations in port or media type, model, or logical addressing schema.
- Create a post-migration test plan. You will use the test plan to verify that the firewalls work as efficiently after the migration as they did before. The plan might include tasks such as:
  - Monitor the firewalls for at least 24 hours after the migration.
  - Monitor Panorama and firewall logs for anomalies.
  - Check administrator logins on Panorama.
  - Test various types of traffic from multiple sources. For example, check bandwidth graphs, session counts, and deny-rule traffic log entries (see Use Panorama for Visibility). The testing should cover a representative sample of policy configurations.
  - Check with your network operations center (NOC) and security operations center (SOC) for any user-reported issues.
  - Include any other test criteria that will help verify firewall functionality.

Migrate a Firewall to Panorama Management

When you import a firewall configuration, Panorama automatically creates a template to contain the imported network and device settings. To contain the imported policies and objects, Panorama automatically creates one device group for each firewall or one device group for each virtual system (vsys) in a multi-vsys firewall.

When you perform the following steps, Panorama imports the entire firewall configuration. Alternatively, you can Load a Partial Firewall Configuration into Panorama.

Panorama can import configurations from firewalls that run PAN-OS 5.0 or later releases and can push configurations to those firewalls. The exception is that Panorama 6.1 and later releases cannot push configurations to firewalls running PAN-OS 6.0.0 through 6.0.3.

Panorama can import configurations from firewalls that are already managed devices but only if they are not already assigned to device groups or templates.

<table>
<thead>
<tr>
<th>Migrate a Firewall to Panorama Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Plan the migration.</td>
</tr>
</tbody>
</table>

Copyright © 2007-2017 Palo Alto Networks
### Migrate a Firewall to Panorama Management (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Add the firewall as a managed device.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add a Firewall as a Managed Device:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Log in to Panorama, select <strong>Panorama &gt; Managed Devices</strong> and click <strong>Add</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Enter the serial number of the firewall and click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>If you will import multiple firewall configurations, enter the serial number of each one on a separate line. Optionally, you can copy and paste the serial numbers from a Microsoft Excel worksheet.</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Set up a connection from the firewall to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Log in to the firewall, select <strong>Device &gt; Setup</strong>, and edit the Panorama Settings.</td>
<td></td>
</tr>
<tr>
<td><strong>2.</strong> In the <strong>Panorama Servers</strong> fields, enter the IP addresses of the Panorama management server.</td>
<td></td>
</tr>
<tr>
<td><strong>3.</strong> Click <strong>OK</strong> and <strong>Commit</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
## Migrate a Firewall to Panorama Management (Continued)

### Step 4: Import the firewall configuration into Panorama.

If you later decide to re-import a firewall configuration, first remove the firewall or its virtual systems from the device groups and template where you originally imported them. (Firewalls don’t lose logs when you remove them from device groups or templates.) Because the imported policies and objects remain in the device groups, you must manually move, edit, or delete them when necessary. When re-importing, use the **Device Group Name Prefix** fields to define device group names that differ from the ones Panorama created in the original import.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From Panorama, select <strong>Panorama &gt; Setup &gt; Operations</strong>, click <strong>Import device configuration to Panorama</strong>, and select the <strong>Device</strong>. Then select <strong>Panorama can’t import a configuration from a firewall that is assigned to an existing device group or template.</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter a <strong>Template Name</strong>. The default value is the firewall name. You can’t use the name of an existing template.</td>
</tr>
<tr>
<td>3.</td>
<td>For a multi-vsys firewall, optionally add a character string as a <strong>Device Group Name Prefix</strong> for all the device groups.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional) Edit the <strong>Device Group</strong> names. If this is a multi-vsys firewall, each device group has a vsys name by default. Otherwise, the default value is the firewall name. You can’t use the names of existing device groups. The Import devices’ shared objects into Panorama’s shared context check box is selected by default, which means Panorama compares imports objects that belong to the Shared location in the firewall to Shared in Panorama. If an imported object is not in the Shared context of the firewall, it is applied to each device group being imported. If you clear the check box, Panorama copies will not compare imported objects, and apply all shared firewall objects into device groups being imported instead of Shared. This could create duplicate objects, so selecting the check box is a best practice in most cases. To understand the consequences of importing shared or duplicate objects into Panorama, see <a href="#">Plan how to manage shared settings</a>.</td>
</tr>
<tr>
<td>5.</td>
<td>Select a <strong>Rule Import Location</strong> for the imported policy rules: <strong>Pre Rulebase</strong> or <strong>Post Rulebase</strong>. Regardless of your selection, Panorama imports default security rules (intrazone-default and interzone-default) into the post-rulebase. If Panorama has a rule with the same name as a firewall rule that you import, Panorama displays both rules. Delete one of the rules before performing a Panorama commit to prevent a commit error.</td>
</tr>
<tr>
<td>6.</td>
<td>Click <strong>OK</strong>. Panorama displays the import status, result, details about your selections, details about what was imported, and any warnings. Click <strong>Close</strong>.</td>
</tr>
</tbody>
</table>
Migrate a Firewall to Panorama Management (Continued)

**Step 5**  Fine-tune the imported configuration.

1. In Panorama, select Panorama > Config Audit, select the Running config and Candidate config for the comparison, click Go, and review the output.
2. Update the device group and template configurations as needed based on the configuration audit and any warnings that Panorama displayed after the import. For example:
   - Delete redundant objects and policy rules.
   - Move or Clone a Policy Rule or Object to a Different Device Group.
   - Move firewalls to different device groups or templates.
   - Move a device group that Panorama created during the import to a different parent device group: Select Panorama > Device Groups, select the device group you want to move, select a new Parent Device Group, and click OK.

**Step 6**  Push the firewall configuration bundle to the firewall to remove all policy rules and objects from its local configuration. This step is necessary to prevent duplicate rule or object names, which would cause commit errors when you push the device group configuration from Panorama to the firewall in the next step.

1. Click Commit, for the Commit Type select Panorama, and click Commit again. Panorama creates a firewall configuration bundle named <firewall_name>_import.tgz, in which all policies and objects are removed.
2. In Panorama, select Panorama > Setup > Operations and click Export or push device config bundle.
3. Select the Device from which you imported the configuration, click OK, and click Push & Commit. Panorama pushes the bundle and initiates a commit on the firewall.

**Step 7**  Push the device group and template configurations to the firewall to complete the transition to centralized management.

If you are migrating multiple firewalls, perform all the preceding steps—including this one—for each firewall before continuing.

1. In Panorama, click Commit and for the Commit Type select Device Group.
2. Select the Merge with Device Candidate Config, Include Device and Network Templates and Force Template Values check boxes.
3. Select the device groups that contain the imported firewall configurations and click Commit.

**Step 8**  Consolidate all the imported firewall configurations.

Required if you are migrating multiple firewalls. Settings might be duplicated among the firewalls. For example, if you imported an object with the same name from two firewalls, you must delete one object in Panorama before performing a commit on Panorama.

1. After importing all the firewall configurations, update the device groups and templates as needed to eliminate redundancy and streamline configuration management: see Fine-tune the imported configuration. (You don’t need to push firewall configuration bundles again.)
2. Configure any firewall-specific settings.
   - If the firewalls will have local zones, you must create them before performing a device group or template commit; Panorama can’t poll the firewalls for zone name or zone configuration. If you will use local firewall rules, ensure their names are unique (not duplicated in Panorama). If necessary, you can Override a Template Setting with a firewall-specific value.
3. In Panorama, click Commit, for the Commit Type select Device Group, select the device groups, select the Include Device and Network Templates check box, and click Commit.
Migrate a Firewall to Panorama Management (Continued)

**Step 9** Perform your post-migration test plan.

Perform the verification tasks that you devised during the migration planning to confirm that the firewalls work as efficiently with the Panorama-pushed configuration as they did with their original local configuration: see Create a post-migration test plan.

Migrate a Firewall HA Pair to Panorama Management

If you have a pair of firewalls in an HA configuration that you want to manage using Panorama, you have the option to import the configuration local to your firewall HA pair to Panorama without needing to recreate any configurations or policies. You will first import the firewall configurations to Panorama, which are then created into a device group and template. You will perform a special configuration push of the device group and template to the firewalls to overwrite the local firewall configurations and synchronize the firewalls with Panorama.

Migrate a Firewall HA Pair to Panorama Management

**Step 1** Plan the migration.

See the checklist in Plan the Transition to Panorama Management.

**Step 2** Disable configuration synchronization between the HA peers.

Repeat these steps for both firewalls in the HA pair.

1. Log in to the web interface on each firewall, select **Device > High Availability > General** and edit the Setup section.
2. Clear **Enable Config Sync** and click **OK**.
3. **Commit** the configuration changes on each firewall.

**Step 3** Connect each firewall to Panorama.

Repeat these steps for both firewalls in the HA pair.

1. Log in to the web interface on each firewall, select **Device > Management** and edit the Panorama Settings.
2. In the **Panorama Servers** fields, enter the IP addresses of the Panorama management servers, confirm **Panorama Policy and Objects** and **Device and Network Template** are enabled and select **OK**.
3. **Commit** the configuration changes on each firewall.

**Step 4** Add each firewall as a managed device.

Add a Firewall as a Managed Device:

1. Log in to Panorama, select **Panorama > Managed Devices** and click **Add**.
2. Enter the serial number of each firewall and click **OK**.
3. Select **Commit > Commit to Panorama** and **Commit** your changes.
4. Verify that the Device State for each firewall is Connected.
### Migrate a Firewall HA Pair to Panorama Management (Continued)

#### Step 5 Import each firewall configuration into Panorama.

If you later decide to re-import a firewall configuration, first remove the firewall device groups and template where you originally imported them. (Firewalls don’t lose logs when you remove them from device groups or templates.) Because the imported policies and objects remain in the device groups, you must manually move, edit, or delete them when necessary. When re-importing, use the Device Group Name Prefix fields to define device group names that differ from the ones Panorama created in the original import.

1. From Panorama, select **Panorama > Setup > Operations**, click **Import device configuration to Panorama**, and select the **Device**.

   Panorama can’t import a configuration from a firewall that is assigned to an existing device group or template.

2. Edit the **Template Name**. The default value is the firewall name. You can’t use the name of an existing template.

3. *(Optional)* Edit the **Device Group** names. For a multi-vsyst firewall, each device group has a vsys name by default, so add a character string as a Device Group Name Prefix for each. Otherwise, the default value is the firewall name. You can’t use the names of existing device groups.

   **The Import devices’ shared objects into Panorama’s shared context** check box is selected by default, which means Panorama compares imports objects that belong to the Shared location in the firewall to Shared in Panorama. If an imported object is not in the shared context of the firewall, it is applied to each device group being imported. If you clear the check box, Panorama copies will not compare imported objects, and apply all shared firewall objects into device groups being imported instead of Shared. This could create duplicate objects, so selecting the check box is a best practice in most cases. To understand the consequences of importing shared or duplicate objects into Panorama, see Plan how to manage shared settings.

4. Repeat Step 1-3 above on the second firewall. The process will create a device group and template for the firewall.

5. **Commit to Panorama**.

   The import process does not import the HA IP addresses and management IP address of the firewalls. These IP addresses will continue to be defined locally on the device.

6. Add the HA firewall pair into the same device group and template. If the HA pair are in an active/active configuration, skip this step. If the HA pair are in an active/passive configuration and have differing configurations, avoid combining both firewalls into a single template.

   a. Select **Panorama > Device Group**, select the device group of the second firewall and **Delete** it.

   b. Select the device group for the first firewall, select the second firewall, click **OK** and **Commit to Panorama** to add it to the same device group as the HA peer.

   c. Select **Panorama > Templates**, select the template for the second firewall and **Delete** it.

   d. Select the template for the first firewall, add the second firewall, select **OK** and **Commit to Panorama** to add it to the same template as the HA peer.
**Transition a Firewall to Panorama Management (Continued)**

### Step 6  
Push the configuration to the firewalls.

Push the device configuration bundle to the firewalls in order to remove all local policy configurations from the firewalls and replace them with the configuration you manage from Panorama.

- **HA Config Sync in Step 3 must be disabled on both firewalls before you push the device group and template.**

1. Push the configuration to the passive firewall.
   a. In Panorama, select Panorama > Setup > Operations and select Export or push device config bundle.
   b. Select the passive firewall Device, select OK and Push & Commit.
   c. Select OK after the export has completed successfully.
   d. Click Commit
   e. Select Templates and enable Force Template Values.
   f. Select Device Group and enable Include Device and Network Templates and Force Template Values.
   g. Commit the configuration on the passive firewall only.
   h. Select Panorama > Managed Devices, and verify that the device group and template are in sync for the passive firewall. Verify policy rules, objects and network settings on the passive firewall match the active firewall.

2. Suspend the active firewall to trigger a failover. On the active firewall, select Device > High Availability > Operational Commands and Suspend local device, and click OK to promote the passive firewall to active. Verify that traffic is passing and everything is operating as expected.

3. Repeat Step 1 (a to h) above on the firewall you suspended.

4. On Panorama, click Commit and Commit the configuration to the suspended firewall only.

5. Restore the suspended firewall as the active HA peer. Select Device > High Availability > Operational Commands and Make local device functional to trigger a failover and transition the currently passive firewall peer back as the active HA peer.

### Step 7  
Enable configuration synchronization between the HA peers.

Repeat these steps for both firewalls in the HA pair if you plan on maintaining a local configuration that needs to be synchronized.

1. Log in to the web interface on each firewall, select Device > High Availability > General and edit the Setup section.
2. Select Enable Config Sync and click OK.
3. Commit the configuration changes on each firewall.
Load a Partial Firewall Configuration into Panorama

If some configuration settings on a firewall are common to other firewalls, you can load those specific settings into Panorama and then push them to all the other firewalls or to the firewalls in particular device groups and templates.

**Load a Partial Firewall Configuration into Panorama**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Plan the transition to Panorama.</th>
<th>See the checklist in <a href="#">Plan the Transition to Panorama Management</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Resolve how to manage duplicate settings, which are those that have the same names in Panorama as in a firewall. Before you load a partial firewall configuration, Panorama and that firewall might already have duplicate settings. Loading a firewall configuration might also add settings to Panorama that are duplicates of settings in other managed firewalls. If Panorama has policy rules or objects with the same names as those on a firewall, a commit failure will occur when you try to push device group settings to that firewall. If Panorama has template settings with the same names as those on a firewall, the template values will override the firewall values when you push the template.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Export the entire firewall configuration to your local computer.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Import the firewall configuration snapshot into Panorama.</td>
<td></td>
</tr>
</tbody>
</table>

1. On the firewall, select **Device > Setup > Operations**.
2. Click **Save named configuration snapshot**, enter a Name to identify the configuration, and click **OK**.
3. Click **Export named configuration snapshot**, select the Name of the configuration you just saved, and click **OK**. The firewall exports the configuration as an XML file.

1. On Panorama, select **Panorama > Setup > Operations**.
2. Click **Import named Panorama configuration snapshot**, **Browse** to the firewall configuration file you exported to your computer, and click **OK**.

After using this option to import a firewall configuration file, you can’t use the Panorama web interface to load it. You must use the XML API or CLI, as described in the next step.
Load a Partial Firewall Configuration into Panorama (Continued)

Step 5  Load the desired part of the firewall configuration into Panorama.
To specify a part of the configuration (for example, all application objects), you must identify the:
- Source xpath—The XML node in the firewall configuration file from which you are loading.
- Destination xpath—The node in the Panorama configuration to which you are loading.

Use the XML API or CLI to identify and load the partial configuration:
1. Use the firewall XML API or CLI to identify the source xpath. For example, the xpath for application objects in vsys1 of the firewall is:
   `/config/devices/entry[@name='localhost.localdomain ']/vsys/entry[@name='vsys1']/application`
2. Use the Panorama XML API or CLI to identify the destination xpath. For example, to load application objects into a device group named US-West, the xpath is:
   `/config/devices/entry[@name='localhost.localdomain ']/device-group/entry[@name='US-West']/application`
3. Use the Panorama CLI to load the configuration and commit the change:
   ```
   # load config partial from <filename> from-xpath <source-xpath> to-xpath <destination-xpath> mode [append|merge|replace]
   For example, enter the following to load the application objects from vsys1 on an imported firewall configuration named fw1-config.xml into a device group named US-West on Panorama:
   ```
   ```
   # load config partial from fw1-config.xml from-xpath devices/entry[@name='localhost.localdomain ']/vsys/entry[@name='vsys1']/application to-xpath /config/devices/entry[@name='localhost.localdomain ']/device-group/entry[@name='US-West']/application mode merge
   # commit
   ```

Step 6  Push the partial configuration from Panorama to the firewall to complete the transition to centralized management.
1. On the firewall, delete any rules or objects that have the same names as those in Panorama. If the device group for that firewall has other firewalls with rules or objects that are duplicated in Panorama, perform this step on those firewalls also. For details, see Step 2.
2. On Panorama, click Commit, for the Commit Type select Panorama, and click Commit again.
3. On Panorama, click Commit and for the Commit Type select Device Group.
4. Select the Merge with Device Candidate Config, Include Device and Network Templates and Force Template Values check boxes.
5. Select the device groups that contain the imported firewall configurations and click Commit.
6. If the firewall has a device or network setting that you won’t use Panorama to manage, Override a Template Setting on the firewall.
<table>
<thead>
<tr>
<th>Step 7</th>
<th>Perform your post-migration test plan.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform the verification tasks that you devised during the migration planning to confirm that the firewall works as efficiently with the Panorama-pushed configuration as it did with its original local configuration: see Create a post-migration test plan.</td>
</tr>
</tbody>
</table>
Use Case: Configure Firewalls Using Panorama

Let's say that you want to use Panorama in a high availability configuration to manage a dozen firewalls on your network: you have six firewalls deployed across six branch offices, a pair of firewalls in a high availability configuration at each of two data centers, and a firewall in each of the two regional head offices.

The first step in creating your central management strategy is to determine how to group the firewalls into device groups and templates to efficiently push configurations from Panorama. You can base the grouping on the business functions, geographic locations, or administrative domains of the firewalls. In this example, you create two device groups and three templates to administer the firewalls using Panorama:

▲ Device Groups in this Use Case
▲ Templates in this Use Case
▲ Set Up Your Centralized Configuration and Policies
Device Groups in this Use Case

In **Use Case: Configure Firewalls Using Panorama**, we need to define two device groups based on the functions the firewalls will perform:

- **DG_BranchAndRegional** for grouping firewalls that serve as the security gateways at the branch offices and at the regional head offices. We placed the branch office firewalls and the regional office firewalls in the same device group because firewalls with similar functions will require similar policy rulebases.
- **DG_DataCenter** for grouping the firewalls that secure the servers at the data centers.

We can then administer shared policy rules across both device groups as well as administer distinct device group rules for the regional office and branch office groups. Then for added flexibility, the local administrator at a regional or branch office can create local rules that match specific source, destination, and service flows for accessing applications and services that are required for that office. In this example, we create the following hierarchy for security rules. You can use a similar approach for any of the other rulebases.

<table>
<thead>
<tr>
<th>Device Groups</th>
<th>DG_BranchAndRegional</th>
<th>DG_DataCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>Regional</td>
<td>Datacenter</td>
</tr>
<tr>
<td>Shared pre-rule</td>
<td>Allow DNS and SNMP services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.</td>
<td></td>
</tr>
<tr>
<td>Device Group pre-rule</td>
<td>Allow Facebook to all users in the marketing group in the regional offices only.</td>
<td>Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.</td>
</tr>
<tr>
<td>Local rules on a device</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Device Group post-rule</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Shared post-rule</td>
<td>To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.</td>
<td></td>
</tr>
</tbody>
</table>

Templates in this Use Case

When grouping firewalls for templates, we must take into account the differences in the networking configuration. For example, if the interface configuration is not the same—the interfaces are unlike in type, or the interfaces used are not alike in the numbering scheme and link capacity, or the zone to interface mappings are different—the firewalls must be in separate templates. Further, the way the firewalls are configured to access network resources might be different because the firewalls are spread geographically; for example, the DNS server, syslog servers and gateways that they access might be different. So, to allow for an optimal base configuration, in **Use Case: Configure Firewalls Using Panorama** we must place the firewalls in separate templates as follows:

- **T_Branch** for the branch office firewalls
- T_Regional for the regional office firewalls
- T_DataCenter for the data center firewalls

If you plan to deploy your firewalls in an active/active HA configuration, assign each firewall in the HA pair to a separate template. Doing so gives you the flexibility to set up separate networking configurations for each peer. For example, you can manage the networking configurations in a separate template for each peer so that each can connect to different northbound and southbound routers, and can have different OSPF or BGP peering configurations.

Set Up Your Centralized Configuration and Policies

In Use Case: Configure Firewalls Using Panorama, we would need to perform the following tasks to centrally deploy and administer firewalls:

▲ Add the Managed Firewalls and Deploy Updates
▲ Use Templates to Administer a Base Configuration
▲ Use Device Groups to Push Policy Rules
▲ Preview the Rules and Commit Changes

Add the Managed Firewalls and Deploy Updates

The first task in Use Case: Configure Firewalls Using Panorama is to add the firewalls as managed devices and deploy content updates and PAN-OS software updates to those firewalls.

<table>
<thead>
<tr>
<th>Add the Managed Firewalls and Deploy Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> For each firewall that Panorama will manage, Add a Firewall as a Managed Device.</td>
</tr>
<tr>
<td>In this example, add 12 firewalls.</td>
</tr>
</tbody>
</table>
### Add the Managed Firewalls and Deploy Updates (Continued)

**Step 2** Deploy the content updates to the firewalls. If you purchased a Threat Prevention subscription, the content and antivirus databases are available to you. First install the Applications or Applications and Threats database, then the Antivirus.

To review the status or progress for all tasks performed on Panorama, see Use the Panorama Task Manager.

| 1. | Select Panorama > Device Deployment > Dynamic Updates. |
| 2. | Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available. |
| 3. | Click Download. When the download completes, the value in the Action column changes to Install. |
| 4. | In the Action column, click Install. Use the filters or user-defined tags to select the managed firewalls on which you would like to install this update. |
| 5. | Click OK, then monitor the status, progress, and result of the content update for each firewall. The Result column displays the success or failure of the installation. |

| 1. | Select Panorama > Device Deployment > Software. |
| 2. | Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available. |
| 3. | Locate the version that you need for each hardware model and click Download. When the download completes, the value in the Action column changes to Install. |
| 4. | In the Action column, click the Install link. Use the filters or user-defined tags to select the managed firewalls on which to install this version. |
| 5. | Enable the check box for Reboot device after install or Upload only to device (do not install) and click OK. The Results column displays the success or failure of the installation. |

### Use Templates to Administer a Base Configuration

The second task in Use Case: Configure Firewalls Using Panorama is to create the templates you will need to push the base configuration to the firewalls.

**Use Templates to Administer a Base Configuration**

**Step 1** For each template you will use, Add a Template and assign the appropriate firewalls to each.

In this example, create templates named T_Branch, T_Regional, and T_DataCenter.
### Use Templates to Administer a Base Configuration (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Define a DNS server, NTP server, syslog server, and login banner. Repeat this step for each template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the <strong>Device</strong> tab, select the <strong>Template</strong> from the drop-down.</td>
</tr>
<tr>
<td>2.</td>
<td>Define the DNS and NTP servers:</td>
</tr>
<tr>
<td>a.</td>
<td>Select <strong>Device &gt; Setup &gt; Services &gt; Global</strong> and edit the Services.</td>
</tr>
<tr>
<td>b.</td>
<td>In the <strong>Services</strong> tab, enter an IP address for the <strong>Primary DNS Server</strong>. For any firewall that has more than one virtual system (vsys), for each vsys, add a DNS server profile to the template (<strong>Device &gt; Server Profiles &gt; DNS</strong>).</td>
</tr>
<tr>
<td>c.</td>
<td>In the <strong>NTP</strong> tab, enter an IP address for the <strong>Primary NTP Server</strong>.</td>
</tr>
<tr>
<td>d.</td>
<td>Click <strong>OK</strong> to save your changes.</td>
</tr>
<tr>
<td>3.</td>
<td>Add a login banner: select <strong>Device &gt; Setup &gt; Management</strong>, edit the General Settings, enter text for the <strong>Login Banner</strong> and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure a <strong>Syslog</strong> server profile (<strong>Device &gt; Server Profiles &gt; Syslog</strong>).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Enable HTTPS, SSH, and SNMP access to the management interface of the managed firewalls. Repeat this step for each template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the <strong>Device</strong> tab, select the <strong>Template</strong> from the drop-down.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Setup &gt; Management</strong>, and edit the Management Interface Settings.</td>
</tr>
<tr>
<td>3.</td>
<td>Under Services, select the HTTPS, SSH, and SNMP check boxes, and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Create a Zone Protection profile for the firewalls in the data center template (T_DataCenter).</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the <strong>Network</strong> tab and, in the <strong>Template</strong> drop-down, select T_DataCenter.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Network Profiles &gt; Zone Protection</strong> and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>For this example, enable protection against a SYN flood—In the <strong>Flood Protection</strong> tab, select the <strong>SYN</strong> check box, set the <strong>Action</strong> to <strong>SYN Cookies</strong>, set the <strong>Alert</strong> packets/second to 100, set the <strong>Activate</strong> packets/second to 1000, and set the <strong>Maximum</strong> packets/second to 10000.</td>
</tr>
<tr>
<td>4.</td>
<td>For this example, enable alerts—in the <strong>Reconnaissance Protection</strong> tab, select the <strong>Enable</strong> check boxes for TCP Port Scan, Host Sweep, and UDP Port Scan. Ensure the Action values are set to <strong>alert</strong> (the default value).</td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>OK</strong> to save the Zone Protection profile.</td>
</tr>
</tbody>
</table>
### Use Templates to Administer a Base configuration (Continued)

| Step 5 | Configure the interface and zone settings in the data center template (T_DataCenter), and then attach the Zone Protection profile you just created. Before performing this step, you must have configured the interfaces locally on the firewalls. As a minimum, for each interface, you must have defined the interface type, assigned it to a virtual router (if needed), and attached a security zone. |
| Step 6 | Commit your template changes. |

1. Select the **Network** tab and, in the **Template** drop-down, select T_DataCenter.
2. Select **Network > Interface** and, in the Interface column, click the interface name.
3. Select the **Interface Type** from the drop-down.
4. In the **Virtual Router** drop-down, click **New Virtual Router**. When defining the router, ensure the **Name** matches what is defined on the firewall.
5. In the **Security Zone** drop-down, click **New Zone**. When defining the zone, ensure that the **Name** matches what is defined on the firewall.
6. Click **OK** to save your changes to the interface.
7. Select **Network > Zones**, and select the zone you just created. Verify that the correct interface is attached to the zone.
8. In the **Zone Protection Profile** drop-down, select the profile you created, and click **OK**.

### Use Device Groups to Push Policy Rules

**The third task in Use Case: Configure Firewalls Using Panorama** is to create the device groups to manage policy rules on the firewalls.

| Step 1 | Create device groups and assign the appropriate firewalls to each device group: see Add a Device Group. |
| In this example, create device groups named DG_BranchAndRegional and DG_DataCenter. When configuring the DG_BranchAndRegional device group, you must assign a **Master** firewall. This is the only firewall in the device group that gathers user and group mapping information for policy evaluation. |

---

*Use Device Groups to Push Policy Rules*

| Step 1 | Create device groups and assign the appropriate firewalls to each device group: see Add a Device Group. |
| In this example, create device groups named DG_BranchAndRegional and DG_DataCenter. When configuring the DG_BranchAndRegional device group, you must assign a **Master** firewall. This is the only firewall in the device group that gathers user and group mapping information for policy evaluation. |

---

*Use Device Groups to Push Policy Rules*
### Use Device Groups to Push Policy Rules (Continued)

#### Step 2
Create a shared pre-rule to allow DNS and SNMP services.

1. Create a shared application group for the DNS and SNMP services.
   - Select Objects > Application Group and click Add.
   - Enter a Name and select the Shared check box to create a shared application group object.
   - Click Add, type DNS, and select dns from the list. Repeat for SNMP and select snmp, snmp-trap.
   - Click OK to create the application group.

2. Create the shared rule.
   - Select the Policies tab and, in the Device Group drop-down, select Shared.
   - Select the Security > Pre-Rules rulebase.
   - Click Add and enter a Name for the security rule.
   - In the Source and Destination tabs for the rule, click Add and enter a Source Zone and a Destination Zone for the traffic.
   - In the Applications tab, click Add, type the name of the applications group object you just created, and select it from the drop-down.
   - In the Actions tab, set the Action to Allow, and click OK.

#### Step 3
Define the corporate acceptable use policy for all offices. In this example, create a shared rule that restricts access to some URL categories and denies access to peer-to-peer traffic that is of risk level 3, 4, or 5.

1. Select the Policies tab and, in the Device Group drop-down, select Shared.
2. Select Security > Pre-Rules and click Add.
3. In the General tab, enter a Name for the security rule.
4. In the Source and Destination tabs, click Add and select any for the traffic Source Zone and Destination Zone.
5. In the Application tab, define the application filter:
   - Click Add and click New Application Filter in the footer of the drop-down.
   - Enter a Name, and select the Shared check box.
   - In the Risk column, select levels 3, 4, and 5.
   - In the Technology column, select peer-to-peer.
   - Click OK to save the new filter.
6. In the Service/URL Category tab, URL Category section, click Add and select the categories you want to block (for example, streaming-media, dating, and online-personal-storage).
7. You can also attach the default URL Filtering profile—In the Actions tab, Profile Setting section, select the Profile Type option Profiles, and select the URL Filtering option default.
8. Click OK to save the security pre-rule.
<table>
<thead>
<tr>
<th>Use Device Groups to Push Policy Rules (Continued)</th>
</tr>
</thead>
</table>
| **Step 4** Allow Facebook for all users in the Marketing group in the regional offices only. Enabling a security rule based on user and group has the following prerequisite tasks:  
  - Set up User-ID on the firewalls.  
  - Enable User-ID for each zone that contains the users you want to identify.  
  - Define a master firewall for the DG_BranchAndRegional device group (Step 1). |
| **Step 5** Allow access to the Amazon cloud application for the specified hosts/servers in the data center. |
| **Step 6** To enable logging for all internet-bound traffic on your network, create a rule that matches trust zone to untrust zone. |

| 1. Select the **Policies** tab and, in the **Device Group** drop-down, select DG_BranchAndRegional.  
2. Select the **Security > Pre-Rules** rulebase.  
3. Click **Add** and enter a **Name** for the security rule.  
4. In the **Source** tab, **Add** the Source Zone that contains the Marketing group users.  
5. In the **Destination** tab, **Add** the Destination Zone.  
6. In the **User** tab, **Add** the Marketing user group to the Source User list.  
7. In the **Application** tab, click **Add**, type Facebook, and then select it from the drop-down.  
8. In the **Action** tab, set the **Action** to **Allow**.  
9. In the **Target** tab, select the regional office firewalls and click **OK**. |

| 1. Create an address object for the servers/hosts in the data center that need access to the Amazon cloud application.  
  a. Select **Objects > Addresses** and, in the **Device Group** drop-down, select DG_DataCenter.  
  b. Click **Add** and enter a **Name** for the address object.  
  c. Select the **Type**, and specify an IP address and netmask (IP Netmask), range of IP addresses (IP Range), or FQDN.  
  d. Click **OK** to save the object.  
2. Create a security rule that allows access to the Amazon cloud application.  
  a. Select **Policies > Security > Pre-Rules** and, in the **Device Group** drop-down, select DG_DataCenter.  
  b. Click **Add** and enter a **Name** for the security rule.  
  c. Select the **Source** tab, **Add** the Source Zone for the data center, and **Add** the address object (Source Address) you just defined.  
  d. Select the **Destination** tab and **Add** the Destination Zone.  
  e. Select the **Application** tab, click **Add**, type Amazon, and select the Amazon applications from the list.  
  f. Select the **Action** tab and set the **Action** to **Allow**.  
  g. Click **OK** to save the rule.  
3. Select the **Policies** tab and, in the **Device Group** drop-down, select **Shared**.  
4. Select the **Security > Pre-Rules** rulebase.  
5. In the **Source** and **Destination** tabs for the rule, **Add trust_zone** as the Source Zone and **untrust_zone** as the Destination Zone.  
6. In the **Action** tab, set the **Action** to **Deny**, set the **Log Setting to Log at Session end**, and click **OK**. |
Preview the Rules and Commit Changes

The final task in Use Case: Configure Firewalls Using Panorama is to review the rules and commit the changes you have made to Panorama, device groups, and templates.

### Preview the Rules and Commit Changes

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Policies tab, click Preview Rules, and select a Rulebase, Device Group, and Device. This preview enables you to visually evaluate how rules are layered for a particular rulebase. Close the preview dialog when you are done.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Commit, for the Commit Type select Device Group, select the device groups you added, select the Include Device and Network Templates check box, and click Commit again.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Context drop-down, select the firewall to access its web interface and confirm that Panorama applied the template and policy configurations.</td>
</tr>
</tbody>
</table>