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.
Panorama Overview

Panorama provides centralized monitoring and management of multiple Palo Alto Networks next-generation firewalls. It provides a single location from which you can oversee all applications, users, and content traversing your network, and then use this knowledge to create application enablement policies that protect and control the network. Using Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

▲ About Panorama
▲ Panorama Platforms
▲ Centralized Configuration and Deployment Management
▲ Centralized Logging and Reporting
▲ Panorama Commit and Validation Operations
▲ Role-Based Access Control
▲ Panorama Recommended Deployments
▲ Plan Your Deployment
▲ Deploy Panorama: Task Overview
About Panorama

Panorama provides centralized management of Palo Alto Networks next-generation firewalls, as the following figure illustrates:

Panorama allows you to effectively configure, manage, and monitor your Palo Alto Networks firewalls using central oversight with local control, as required. The three focal areas in which Panorama adds value are:

- **Centralized configuration and deployment**—To simplify central management and rapid deployment of the firewalls on your network, use Panorama to pre-stage the firewalls for deployment. You can then assemble the firewalls into groups, and create templates to apply a base network and device configuration and use device groups to administer globally shared and local policy rules. See Centralized Configuration and Deployment Management.

- **Aggregated logging with central oversight for analysis and reporting**—Collect information on activity across all the managed firewalls on the network and centrally analyze, investigate and report on the data. This comprehensive view of network traffic, user activity, and the associated risks empowers you to respond to potential threats using the rich set of policies to securely enable applications on your network. See Centralized Logging and Reporting.

- **Distributed administration**—Allows you to delegate or restrict access to global and local firewall configurations and policies. See Role-Based Access Control for delegating appropriate levels of access for distributed administration.

Panorama is available in two appliance types: a virtual appliance and a dedicated hardware appliance. For more information, see Panorama Platforms.
Panorama Platforms

Panorama is available in the following appliances, each of which supports firewall management licenses for managing up to 25, 100, or 1,000 firewalls:

- **Panorama virtual appliance**—You can install the Panorama virtual appliance on a VMware ESXi server or in VMware vCloud Air. The virtual appliance allows for simple installation and facilitates server consolidation for sites that need a virtual management appliance. By default, the Panorama virtual appliance has one disk partition for all data. Approximately 11GB of the partition is allocated to store the logs collected from firewalls and the logs that Panorama and Log Collectors generate. If you need more log storage, you can add a virtual disk of up to 8TB on vCloud Air or ESXi 5.5 and later versions. Earlier ESXi versions support a virtual disk of up to 2TB. If you need more than 8TB, you can mount Panorama to an NFS datastore but only on the ESXi server, not in vCloud Air. The Panorama virtual appliance works best in environments with logging rates of up to 10,000 logs per second. You can forward firewall logs directly to the Panorama virtual appliance (see Deploy Panorama Virtual Appliances with Local Log Collection) or use the Panorama virtual appliance to manage Dedicated Log Collectors that are M-Series appliances (see Deploy Panorama with Dedicated Log Collectors).

- **M-Series appliance**—The M-100 appliance and M-500 appliance are dedicated hardware models intended for large-scale deployments. In environments with high logging rates (over 10,000 logs per second) and log retention requirements, these appliances enables scaling of your log collection infrastructure. Both appliances use RAID drives to store firewall logs and support RAID 1 mirroring to protect against disk failures. Both appliances use an SSD to store the logs that Panorama and Log Collectors generate. Only the M-500 appliance has redundant, hot-swappable power supplies and front-to-back airflow. The M-500 appliance also has faster processors and greater memory for better performance (for example, faster commit times). These attributes make the M-500 appliance more suitable for datacenters than the M-100 appliance. You can deploy the M-Series appliance in the following modes to separate the central management function from the log collection function:
  - **Panorama mode**: The appliance performs both central management and log collection. This is the default mode. For configuration details, see Deploy Panorama with Default Log Collectors.
  - **Log Collector mode**: The appliance functions as a Dedicated Log Collector. If multiple firewalls forward large volumes of log data, the M-Series appliance in Log Collector mode provides increased scale and performance. In this mode, the appliance has no web interface for administrative access, only a command line interface (CLI). However, you can manage the appliance using the web interface of the Panorama management server (M-Series appliance in Panorama mode or a Panorama virtual appliance). CLI access to an M-Series appliance in Log Collector mode is only necessary for initial setup and debugging. For configuration details, see Deploy Panorama with Dedicated Log Collectors.

The log storage capacity and maximum log collection rate varies by appliance and mode, as described in the following table. For more details and specifications, see the M-100 and M-500 Hardware Reference Guides.

The best appliance for your network depends on whether you must deploy within a virtual infrastructure, your bandwidth resources (some networks benefit from deploying Log Collectors close to the firewalls), and your log storage requirements (see Determine Panorama Log Storage Requirements). The following table summarizes the logging capacities of each appliance.

<table>
<thead>
<tr>
<th>Appliance Capacities and Features</th>
<th>M-500 Appliance</th>
<th>M-100 Appliance</th>
<th>Virtual Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Logging Rate for Panorama management server (M-Series appliance in Panorama mode or Panorama virtual appliance)</td>
<td>20,000 logs/second</td>
<td>10,000 logs/second</td>
<td>10,000 logs/second</td>
</tr>
<tr>
<td>Appliance Capacities and Features</td>
<td>M-500 Appliance</td>
<td>M-100 Appliance</td>
<td>Virtual Appliance</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Maximum Logging Rate for Dedicated Log Collector</td>
<td>50,000 logs/second</td>
<td>30,000 logs/second</td>
<td>Not applicable: the Panorama virtual appliance cannot be a Dedicated Log Collector.</td>
</tr>
<tr>
<td>Maximum Log Storage</td>
<td>8TB (16 RAID drives)</td>
<td>4TB (8 RAID drives)</td>
<td>8TB (2TB for ESXi releases before v5.5)</td>
</tr>
<tr>
<td>Default Log Storage</td>
<td>4TB (8 drives)</td>
<td>1TB (2 drives)</td>
<td>~11GB</td>
</tr>
<tr>
<td>SSD Storage (for logs that M-Series appliances generate)</td>
<td>240GB</td>
<td>120GB</td>
<td>Not applicable</td>
</tr>
<tr>
<td>NFS Attached Log Storage</td>
<td>Not available</td>
<td>Not available</td>
<td>ESXi server only</td>
</tr>
</tbody>
</table>
Centralized Configuration and Deployment Management

Panorama uses device groups and templates to group firewalls into logical sets that require similar configuration. You use the device groups and templates to centrally manage all configuration elements, policies, and objects on the managed firewalls. Panorama also enables you to centrally manage licenses, software (PAN-OS software, SSL-VPN client software, GlobalProtect agent/app software), and content updates (Applications, Threats, WildFire, and Antivirus).

- **Context Switch—Firewall or Panorama**
- **Templates and Template Stacks**
- **Device Groups**

**Context Switch—Firewall or Panorama**

The Panorama web interface enables you to toggle between a Panorama-centric view and a firewall-centric view by using the Context drop-down at the top-left of every tab. You can set the Context to Panorama to manage firewalls centrally or switch context to the web interface of a specific firewall to configure it locally. The similarity of the Panorama and firewall web interfaces enables you to seamlessly move between them to administer and monitor firewalls.

The Context drop-down lists only the firewalls that are connected to Panorama. For a Device Group and Template administrator, the drop-down lists only the connected firewalls that are within the Access Domains assigned to that administrator. To search a long list, use the Filters within the drop-down.

For firewalls that have a high availability (HA) configuration, the icons have colored backgrounds to indicate HA state (as follows). Knowing the HA state is useful when selecting a firewall context. For example, you generally make firewall-specific configuration changes on the active firewall.

- Green—Active.
- Yellow—Passive or the firewall is initiating (the initiating state lasts for up to 60 seconds after boot up).
- Red—The firewall is non-functional (error state), suspended (an administrator disabled the firewall), or tentative (for a link or path monitoring event in an active/active HA configuration).

**Templates and Template Stacks**

You use templates to configure the settings that enable firewalls to operate on the network. Templates enable you to define a common base configuration using the Network and Device tabs on Panorama. For example, you can use templates to manage interface and zone configurations, server profiles for logging and syslog access, and network profiles for controlling access to zones and IKE gateways. When defining a template, consider assigning firewalls that are the same hardware model and require access to similar network resources, such as gateways and syslog servers.

If your network has groups of firewalls with some group-specific settings and some settings that are common across groups, you can simplify management by assigning the firewalls to a template stack for each group. A template stack is a combination of templates: the assigned firewalls inherit the settings from every template in the stack. This enables you to avoid the redundancy of adding every setting to every template. The following figure illustrates an example deployment in which you assign data center firewalls in the

© Palo Alto Networks, Inc.  
Panorama Overview  
Centralized Configuration and Deployment Management
Asia-Pacific (APAC) region to a stack that has one template with global settings, one template with APAC-specific settings, and one template with data center-specific settings. To manage firewalls in an APAC branch office, you can then re-use the global and APAC-specific templates by adding them to another stack that includes a template with branch-specific settings. Templates in a stack have a configurable priority order that ensures Panorama pushes only one value for any duplicate setting. Panorama evaluates the templates listed in a stack configuration from top to bottom, with higher templates having priority. The following figure illustrates a data center stack in which the data center template has a higher priority than the global template: Panorama pushes the idle timeout value from the data center template and ignores the value from the global template.

**Figure: Template Stacks**

To accommodate firewalls that have unique settings, you can use templates (single or stacked) to push a limited common base configuration to all firewalls, and in individual firewalls configure firewall-specific settings. Alternatively, you can push a broader common base configuration and in the individual firewalls override certain pushed settings with firewall-specific values. When you override a setting, the firewall saves that setting to its local configuration; Panorama no longer manages the setting. To restore template values after overriding them, you can use Panorama to force the template configuration onto a firewall. For example, after defining a common NTP server in a template and overriding the NTP server configuration on a firewall to accommodate its local time zone, you can later revert to the NTP server defined in the template.

You cannot use templates to set firewall modes: virtual private network (VPN) mode, multiple virtual systems mode (multi-vsys mode), and operational mode (normal, Federal Information Processing Standards [FIPS], or Common Criteria [CC]). For details, see Template Capabilities and Exceptions. However, you can assign firewalls that have non-matching modes to the same template or stack. In such cases, Panorama pushes mode-specific settings only to firewalls that support those modes. As an exception, you can configure Panorama to push the settings of the default vsys in a template to firewalls that don’t support virtual systems or have none configured.

For the relevant procedures, see Manage Templates and Template Stacks.
Device Groups

To use Panorama effectively, you have to group the firewalls in your network into logical units called device groups. A device group enables grouping based on network segmentation, geographic location, organizational function, or any other common aspect of firewalls that require similar policy configurations. Using device groups, you can configure policy rules and the objects they reference. You can organize device group hierarchically, with shared rules and objects at the top, and device group-specific rules and objects at subsequent levels. This enables you to create a hierarchy of rules that enforce how firewalls handle traffic. For example, you can define a set of shared rules as a corporate acceptable use policy. Then, to allow only regional offices to access peer-to-peer traffic such as BitTorrent, you can define a device group rule that Panorama pushes only to the regional offices (or define a shared security rule and target it to the regional offices). For the relevant procedures, see Manage Device Groups. The following topics describe device group concepts and components in more detail:

- Device Group Hierarchy
- Device Group Policies
- Device Group Objects

Device Group Hierarchy

You can Create a Device Group Hierarchy to nest device groups in a tree hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) of higher-level groups. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups (ancestors). At the top level, a device group can have child, grandchild, and great-grandchild device groups (descendants). All device groups inheriting settings from the Shared location—a container at the top of the hierarchy for configurations that are common to all device groups.

Creating a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. For example, you could configure shared settings that are global to all firewalls, configure device groups with function-specific settings at the first level, and configure device groups with location-specific settings at lower levels. Without a hierarchy, you would have to configure both function- and location-specific settings for every device group in a single level under Shared.

Figure: Device Group Hierarchy

For details on the order in which firewalls evaluate policy rules in a device group hierarchy, see Device Group Policies. For details on overriding the values of objects that device groups inherit from ancestor device groups, see Device Group Objects.
Device Group Policies

Device groups provide a way to implement a layered approach for managing policies across a network of managed firewalls. A firewall evaluates policy rules by layer (shared, device group, and local) and by type (pre-rules, post-rules, and default rules) in the following order from top to bottom. When the firewall receives traffic, it performs the action defined in the first evaluated rule that matches the traffic and disregards all subsequent rules. To change the evaluation order for rules within a particular layer, type, and rulebase (for example, shared Security pre-rules), see Manage the Rule Hierarchy.

<table>
<thead>
<tr>
<th>Evaluation Order</th>
<th>Rule Scope and Description</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared pre-rules</td>
<td>Panorama pushes shared pre-rules to all the firewalls in all device groups. Panorama pushes device group-specific pre-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device group hierarchy, it evaluates pre-rules in the order of highest to lowest level. This means the firewall first evaluates shared rules and last evaluates the rules of device groups with no descendants. You can use pre-rules to enforce the acceptable use policy of an organization. For example, a pre-rule might block access to specific URL categories or allow Domain Name System (DNS) traffic for all users.</td>
<td>These rules are visible on firewalls but you can only manage them in Panorama.</td>
</tr>
<tr>
<td>Device group pre-rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local firewall rules</td>
<td>Local rules are specific to a single firewall or virtual system (vsys).</td>
<td>A local firewall administrator, or a Panorama administrator who switches to a local firewall context, can edit local firewall rules.</td>
</tr>
<tr>
<td>Device group post-rules</td>
<td>Panorama pushes shared post-rules to all the firewalls in all device groups. Panorama pushes device group-specific post-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device group hierarchy, it evaluates post-rules in the order of lowest to highest level. This means the firewall first evaluates the rules of device groups with no descendants and last evaluates shared rules. Post-rules typically include rules to deny access to traffic based on the App-ID, User-ID, or service.</td>
<td>These rules are visible on firewalls but you can only manage them in Panorama.</td>
</tr>
<tr>
<td>Shared post-rules</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Centralized Configuration and Deployment Management

<table>
<thead>
<tr>
<th>Evaluation Order</th>
<th>Rule Scope and Description</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>intrazone-default</td>
<td>The default rules apply only to the Security rulebase, and are predefined on Panorama (at the Shared level) and the firewall (in each vsys). These rules specify how PAN-OS handles traffic that doesn’t match any other rule. The intrazone-default rule allows all traffic within a zone. The interzone-default rule denies all traffic between zones. If you override default rules, their order of precedence runs from the lowest context to the highest: overridden settings at the firewall level take precedence over settings at the device group level, which take precedence over settings at the Shared level.</td>
<td>Default rules are initially read-only, either because they are part of the predefined configuration or because Panorama pushed them to firewalls. However, you can override the rule settings for tags, action, logging, and security profiles. The context determines the level at which you can override the rules:  * Panorama—At the Shared or device group level, you can override default rules that are part of the predefined configuration.  * Firewall—You can override default rules that are part of the predefined configuration on the firewall or vsys, or that Panorama pushed from the Shared location or a device group.</td>
</tr>
<tr>
<td>interzone-default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Whether you view rules on a firewall or in Panorama, the web interface displays them in evaluation order. All the shared, device group, and default rules that the firewall inherits from Panorama are shaded orange. Local firewall rules display between the pre-rules and post-rules.

**Figure: Rule Hierarchy**

![Rule Hierarchy Diagram]

**Device Group Objects**

Objects are configuration elements that policy rules reference, for example: IP addresses, URL categories, security profiles, users, services, and applications. Rules of any type (pre-rules, post-rules, default rules, and rules locally defined on a firewall) and any rulebase (Security, NAT, QoS, Policy Based Forwarding, Decryption, Application Override, Captive Portal, and DoS Protection) can reference objects. You can reuse an object in any number of rules that have the same scope as that object in the Device Group Hierarchy. For example, if you add an object to the Shared location, all rules in the hierarchy can reference that shared object because all device groups inherit objects from Shared. If you add an object to a particular device group, only the rules in that device group and its descendant device groups can reference that device group object. If object values in a device group must differ from those inherited from an ancestor device group, you can Override inherited object values. You can also Revert to Inherited Object Values at any time. When you Create Objects for Use in Shared or Device Group Policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.
You can configure how Panorama handles objects system-wide:

- **Pushing unused objects**—By default, Panorama pushes all objects to firewalls regardless of whether any shared or device group policy rules reference the objects. Optionally, you can configure Panorama to push only referenced objects. For details, see Manage Unused Shared Objects.

- **Precedence of ancestor and descendant objects**—By default, when device groups at multiple levels in the 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 object values inherited from ancestor device groups or Shared. Optionally, you can reverse this order of precedence to push values from Shared or the highest ancestor containing the object to all descendant device groups. For details, see Manage Precedence of Inherited Objects.
Centralized Logging and Reporting

Panorama aggregates data from all managed firewalls and provides visibility across all the traffic on the network. It also provides an audit trail for all policy modifications and configuration changes made to the managed firewalls. In addition to aggregating logs, Panorama can aggregate and forward Simple Network Management Protocol (SNMP) traps, email notifications, and syslog messages to an external destination.

The Application Command Center (ACC) on Panorama provides a single pane for unified reporting across all the firewalls. It enables you to centrally Monitor Network Activity, to analyze, investigate, and report on traffic and security incidents. On Panorama, you can view logs and generate reports from logs forwarded to Panorama or to the managed Log Collectors, if configured, or you can query the managed firewalls directly. For example, you can generate reports about traffic, threat, and/or user activity in the managed network based on logs stored on Panorama (and the managed collectors) or by accessing the logs stored locally on the managed firewalls.

If you choose not to Configure Log Forwarding to Panorama, you can schedule reports to run on each managed firewall and forward the results to Panorama for a combined view of user activity and network traffic. Although this view does not provide a granular drill-down on specific data and activities, it still provides a unified reporting approach.

- Logging Options
- Managed Collectors and Collector Groups
- Caveats for a Collector Group with Multiple Log Collectors
- Centralized Reporting

Logging Options

Both the Panorama virtual appliance and M-Series appliance can collect logs that the managed firewalls forward. You can then Configure Log Forwarding from Panorama to External Destinations (syslog server, email server, or Simple Network Management Protocol [SNMP] trap server). The logging options vary on each Panorama appliance.

The PA-7000 Series firewall can’t forward logs to Panorama, only to external services directly. However, when you monitor logs or generate reports for a device group that includes a PA-7000 Series firewall, Panorama queries the firewall in real-time to display its log data.

<table>
<thead>
<tr>
<th>Panorama Appliance</th>
<th>Logging Options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual appliance</td>
<td>Offers three logging options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use the approximately 11GB of internal storage space allocated for logging as soon as you install the virtual appliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add a virtual disk. Panorama running on VMware vCloud Air or ESXi 5.5 and later versions can support a virtual disk of up to 8TB. Earlier versions of the ESXi server support a virtual disk of up to 2TB.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mount a Network File System (NFS) datastore in which you can configure the storage capacity that is allocated for logging.</td>
<td></td>
</tr>
</tbody>
</table>
Managed Collectors and Collector Groups

A Log Collector can be local to an M-Series appliance in Panorama mode (default Log Collector) or can be an M-Series appliance in Log Collector mode (Dedicated Log Collector). Because you use Panorama to configure and manage Log Collectors, they are also known as managed collectors. An M-Series appliance in Panorama mode or a Panorama virtual appliance can manage Dedicated Log Collectors. To administer Dedicated Log Collectors using the Panorama web interface, you must add them as managed collectors. Otherwise, administrative access to a Dedicated Log Collector is only available through its CLI using the default administrative user (admin) account. Dedicated Log Collectors do not support additional administrative user accounts.

A Collector Group is 1 to 16 managed collectors that operate as a single logical log collection unit. If the group contains Dedicated Log Collectors, the logs are uniformly distributed across all the disks in each Log Collector and across all members in the Collector Group. This distribution maximizes the use of the available storage space. To manage a Log Collector, you must add it to a Collector Group. If you assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors.

The Collector Group configuration specifies which managed firewalls can send logs to the Log Collectors in the group. After you configure the Log Collectors and enable the firewalls to forward logs, each firewall forwards its logs to the assigned Log Collector.

Managed collectors and Collector Groups are integral to a distributed log collection deployment on Panorama. A distributed log collection deployment allows for easy scalability and incremental addition of Dedicated Log Collectors as your logging needs grow. The M-Series appliance in Panorama mode can log to its default Collector Group and then be expanded to a distributed log collection deployment with one or more Collector Groups that include Dedicated Log Collectors.

To configure Log Collectors and Collector Groups, see Manage Log Collection.

Caveats for a Collector Group with Multiple Log Collectors

You can Configure a Collector Group with multiple Log Collectors (up to 16) to ensure log redundancy, increase the log retention period, or accommodate logging rates that exceed the capacity of a single Log Collector (see Panorama Platforms for capacity information). All the Log Collectors in any particular Collector...
Group must be the same model, such as all M-500 appliances or all M-100 appliances. For example, if a single managed firewall generates 16TB of logs, the Collector Group that receives those logs will require at least four Log Collectors that are M-100 appliances or two Log Collectors that are M-500 appliances.

A Collector Group with multiple Log Collectors uses the available storage space as one logical unit and uniformly distributes the logs across all its Log Collectors. The log distribution is based on the disk capacity of the Log Collectors (1TB to 8TB, depending on the number of disk pairs and the M-Series appliance) and a hash algorithm that dynamically decides which Log Collector owns the logs and writes to disk. Although Panorama uses a preference list to prioritize the list of Log Collectors to which a managed firewall can forward logs, Panorama does not necessarily write the logs to the first Log Collector specified in the preference list. For example, consider the following preference list:

<table>
<thead>
<tr>
<th>Managed Firewall</th>
<th>Log Forwarding Preference List Defined on a Collector Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW1</td>
<td>L1,L2,L3</td>
</tr>
<tr>
<td>FW2</td>
<td>L4,L5,L6</td>
</tr>
</tbody>
</table>

Using this list, FW1 will forward logs to L1, its primary Log Collector, but the hash algorithm could determine that the logs will be written on L2. If L2 becomes inaccessible or has a chassis failure, FW1 will not know about its failure because it is still able to connect to L1, its primary Log Collector.

In the case where a Collector Group has only one Log Collector and the Log Collector fails, the firewall stores the logs to its HDD/SSD (the available storage space varies by hardware model), and resumes forwarding logs to the Log Collector where it left off before the failure occurred as soon as connectivity is restored.

With multiple Log Collectors in a Collector Group, the firewall does not buffer logs to its local storage when it can connect to its primary Log Collector. Therefore, FW1 will continue sending logs to L1. Because L2 is unavailable, the primary Log Collector L1 buffers the logs to its HDD, which has 10GB of log space. If L2 remains unavailable and the logs pending for L2 exceed 10GB, L1 will overwrite the older log entries to continue logging. In such an event, loss of logs is a risk.
Palo Alto Networks recommends the following mitigations if using multiple Log Collectors in a Collector Group:

- Enable log redundancy when you Configure a Collector Group. This ensures that no logs are lost if any one Log Collector in the Collector Group becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. Log redundancy is available only if each Log Collector in the Collector Group has the same number of logging disks.

  ![Warning] Because enabling redundancy creates more logs, this configuration requires more storage capacity. When a Collector Group runs out of space, it deletes older logs. Enabling redundancy doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives.

- Obtain an On-Site-Spare (OSS) to enable prompt replacement if a Log Collector failure occurs.
- In addition to forwarding logs to Panorama, configure forwarding to an external service as backup storage. The external service can be a syslog server, email server, or Simple Network Management Protocol (SNMP) trap server.

**Centralized Reporting**

Panorama aggregates logs from all managed firewalls and enables reporting on the aggregated data for a global view of application use, user activity, and traffic patterns across the entire network infrastructure. As soon as the firewalls are added to Panorama, the ACC can display all traffic traversing your network. With logging enabled, clicking into a log entry in the ACC provides direct access to granular details about the application.

For generating reports, Panorama uses two sources: the local Panorama database and the remote firewalls that it manages. The Panorama database refers to the local storage on Panorama that is allocated for storing both summarized logs and some detailed logs. If you have a distributed Log Collection deployment, the Panorama database includes the local storage on Panorama and all the managed Log Collectors. Panorama summarizes the information—traffic, application, threat—collected from all managed firewalls at 15-minute intervals. Using the local Panorama database allows for faster response times, however, if you prefer to not forward logs to Panorama, Panorama can directly access the remote firewall and run reports on data that is stored locally on the managed firewalls.

Panorama offers more than 40 predefined reports that can be used as is, or they can be customized by combining elements of other reports to generate custom reports and report groups that can be saved. Reports can be generated on demand, on a recurring schedule, and can be scheduled for email delivery.
These reports provide information on the user and the context so that you correlate events and identify patterns, trends, and potential areas of interest. With the integrated approach to logging and reporting, the ACC enables correlation of entries from multiple logs relating to the same event.

For more information, see Monitor Network Activity.
Panorama Commit and Validation Operations

When you are ready to activate changes that you made to the candidate configuration on Panorama or to push changes to the firewalls and Log Collectors that Panorama manages, you can Preview, Validate, or Commit Configuration Changes. For example, if you add a Log Collector to the Panorama configuration, firewalls cannot send logs to that Log Collector until you commit the change to Panorama and then commit to the Collector Group that contains the Log Collector. Panorama queues commit operations so that you can initiate a new commit while a previous commit is in progress. If the queue already has the maximum of ten administrator-initiated commits, Panorama must process a pending commit before you can initiate a new commit. You can also Use the Panorama Task Manager to cancel pending commits or to see details about commits that are pending, in progress, completed, or failed. To check which changes a commit will activate, you can run a commit preview.

For details on candidate and running configurations, see Manage Panorama and Firewall Configuration Backups. To prevent multiple administrators from making configuration changes during concurrent sessions, see Manage Locks for Restricting Configuration Changes.

When you initiate a commit, Panorama checks the validity of the changes before activating them. The validation output displays conditions that block the commit (errors) or that are important to know even though they don’t block the commit (warnings). For example, validation could indicate an invalid route destination that you need to fix for the commit to succeed. To identify and fix configuration errors before initiating a commit, you can validate changes without committing. A pre-commit validation displays the same errors and warnings as a commit, including reference errors, rule shadowing, and application dependency warnings. Pre-commit validations are useful if your organization allows commits only within certain time windows; you can find and fix errors before commit time to avoid failures that could cause you to miss a window.
Role-Based Access Control

Role-based access control (RBAC) enables you to define the privileges and responsibilities of administrative users (administrators). Every administrator must have a user account that specifies a role and authentication method. Administrative Roles define access to specific configuration settings, logs, and reports within Panorama and firewall contexts. For Device Group and Template administrators, you can map roles to Access Domains, which define access to specific device groups, templates, and firewalls (through context switching). By combining each access domain with a role, you can enforce the separation of information among the functional or regional areas of your organization. For example, you can limit an administrator to monitoring activities for data center firewalls but allow that administrator to set policies for test lab firewalls. By default, every Panorama appliance (virtual appliance or M-Series appliance) has a predefined administrative account (admin) that provides full read-write access (superuser access) to all functional areas and to all device groups, templates, and firewalls. For each administrator, you can define the minimum password complexity, a password profile, and an authentication profile that determines how Panorama verifies user access credentials.

Instead of using the default account for all administrators, it is a best practice to create a separate administrative account for each person who needs access to the administrative or reporting functions on Panorama. This provides better protection against unauthorized configuration changes and enables Panorama to log and identify the actions of each administrator.

- Administrative Roles
- Authentication Profiles and Sequences
- Access Domains
- Administrative Authentication

Administrative Roles

You configure administrator accounts based on the security requirements of your organization, any existing authentication services with which to integrate, and the required administrative roles. A role defines the type of system access that is available to an administrator. You can define and restrict access as broadly or granularly as required, depending on the security requirements of your organization. For example, you might decide that a data center administrator can have access to all device and networking configurations, but a security administrator can control only security policy definitions, while other key individuals can have limited CLI or XML API access. The role types are:

- **Dynamic Roles**—These are built-in roles that provide access to Panorama and managed firewalls. When new features are added, Panorama automatically updates the definitions of dynamic roles; you never need to manually update them. The following table lists the access privileges associated with dynamic roles.

<table>
<thead>
<tr>
<th>Dynamic Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Full read-write access to Panorama</td>
</tr>
<tr>
<td>Superuser (read-only)</td>
<td>Read-only access to Panorama</td>
</tr>
</tbody>
</table>

© Palo Alto Networks, Inc.
### Dynamic Role | Privileges
---|---
Panorama administrator | Full access to Panorama except for the following actions:
- Create, modify, or delete Panorama or firewall administrators and roles.
- Export, validate, revert, save, load, or import a configuration in the **Device > Setup > Operations** page.
- Configure **Scheduled Config Export** functionality in the Panorama tab.

#### Admin Role Profiles
To provide more granular access control over the functional areas of the web interface, CLI, and XML API, you can create custom roles. When new features are added to the product, you must update the roles with corresponding access privileges: Panorama does not automatically add new features to custom role definitions. You select one of the following profile types when you Configure an Admin Role Profile.

<table>
<thead>
<tr>
<th>Admin Role Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama</td>
<td>For these roles, you can assign read-write access, read-only access, or no access to all the Panorama features that are available to the superuser dynamic role except the management of Panorama administrators and Panorama roles. For the latter two features, you can assign read-only access or no access, but you cannot assign read-write access. An example use of a Panorama role would be for security administrators who require access to security policy definitions, logs, and reports on Panorama.</td>
</tr>
</tbody>
</table>
| Device Group and Template | For these roles, you can assign read-write access, read-only access, or no access to specific functional areas within device groups, templates, and firewall contexts. By combining these roles with **Access Domains**, you can enforce the separation of information among the functional or regional areas of your organization. Device Group and Template roles have the following limitations:
- No access to the CLI or XML API
- No access to configuration or system logs
- No access to VM information sources
- In the **Panorama** tab, access is limited to:
  - Device deployment features (read-write, read-only, or no access)
  - The device groups specified in the administrator account (read-write, read-only, or no access)
  - The templates and managed firewalls specified in the administrator account (read-only or no access)
An example use of this role would be for administrators in your operations staff who require access to the device and network configuration areas of the web interface for specific device groups and/or templates. |

### Authentication Profiles and Sequences
An authentication profile specifies the authentication service that validates the credentials of an administrator during login and defines how Panorama accesses the service. If you create a local administrator account on Panorama, you can authenticate the administrator to the local database, use an external service (RADIUS, TACACS+, LDAP, or Kerberos server), or use Kerberos single sign-on (SSO). If you use an external service, you must **configure a server profile** before you **Configure an Admin Role Profile**. If you want to use an external service for both account administration (instead of creating local accounts) and for authentication, you must **Configure RADIUS Vendor-Specific Attributes for Administrator Authentication**.
Some environments have multiple databases for different users and user groups. To authenticate to multiple authentication sources (for example, local database and LDAP), configure an authentication sequence. An authentication sequence is a ranked order of authentication profiles that an administrator is matched against when logging in. Panorama checks against the local database first, and then checks each profile in sequence until the administrator is successfully authenticated. The administrator is denied access to Panorama only if authentication fails for all the profiles defined in the authentication sequence.

Access Domains

Access domains control administrative access to specific device groups (to manage policies and objects) and templates (to manage network and device settings), and also control the ability to switch context to the web interface of managed firewalls. Access domains apply only to administrators with Device Group and Template roles. By combining access domains with Administrative Roles, you can enforce the separation of information among the functional or regional areas of your organization.

You can manage access domains locally or by using RADIUS Vendor-Specific Attributes (VSAs). To use RADIUS VSAs, your network requires an existing RADIUS server and you must configure a RADIUS server profile to define how Panorama accesses the server. On the RADIUS server, you define a VSA attribute number and value for each administrator. The value defined must match the access domain configured on Panorama. When an administrator tries to log in to Panorama, Panorama queries the RADIUS server for the administrator access domain and attribute number. Based on the response from the RADIUS server, the administrator is authorized for access and is restricted to the firewalls, virtual systems, device groups, and templates that are assigned to the access domain.

For the relevant procedures, see:

- Configure an Access Domain.
- Configure RADIUS Vendor-Specific Attributes for Administrator Authentication.

Administrative Authentication

The following methods are available to authenticate Panorama administrators:

- **Local administrator account with local authentication**—Both the administrator account credentials and the authentication mechanisms are local to Panorama. To further secure the local administrator account, create a password profile that defines a validity period for passwords and set Panorama-wide password complexity settings. For details on how to configure this type of administrative access, see Configure an Administrator with Kerberos SSO, External, or Local Authentication.

- **Local administrator account with certificate- or key-based authentication**—With this option, the administrator accounts are local to Panorama, but authentication is based on Secure Shell (SSH) keys (for CLI access) or client certificates/common access cards (for the web interface). For details on how to configure this type of administrative access, see Configure an Administrator with Certificate-Based Authentication for the Web Interface and Configure an Administrator with SSH Key-Based Authentication for the CLI.

- **Local administrator account with external authentication**—The administrator accounts are managed on Panorama, but existing external authentication services (LDAP, Kerberos, TACACS+, or RADIUS) handle the authentication functions. If your network supports Kerberos single sign-on (SSO), you can configure
external authentication as an alternative in case SSO fails. For details on how to configure this type of administrative access, see Configure an Administrator with Kerberos SSO, External, or Local Authentication.

- **External administrator account and authentication**—An external RADIUS server handles account administration and authentication. To use this option, you must define Vendor-Specific Attributes (VSAs) on your RADIUS server that map to the administrator roles and access domains. For a high-level overview of the process, see Configure RADIUS Vendor-Specific Attributes for Administrator Authentication. For details on how to configure this type of administrative access, refer to Radius Vendor-Specific Attributes (VSAs).
Panorama Recommended Deployments

A Panorama deployment comprises the Panorama management server (which has a browser-based interface), optional Log Collectors, and the Palo Alto Networks firewalls that Panorama manages. The recommended deployments are:

- Panorama for Centralized Management and Reporting
- Panorama in a Distributed Log Collection Deployment

For the procedures to configure the most typical log collection deployments, see Log Collection Deployments.

Panorama for Centralized Management and Reporting

The following diagram illustrates how you can deploy the Panorama virtual appliance or M-Series appliance in a redundant configuration for the following benefits:

- **Centralized management**—Centralized policy and firewall management that allows for rapid deployment and management of up to one thousand firewalls.
- **Visibility**—Centralized logging and reporting to analyze and report on user-generated traffic and potential threats.
- **Role-based access control**—Appropriate levels of administrative control at the firewall level or global level for administration and management.
Panorama in a Distributed Log Collection Deployment

You can deploy the hardware-based Panorama—the M-Series appliance—either as a Panorama management server that performs management and log collection functions or as a Dedicated Log Collector that provides a comprehensive log collection solution for the firewalls on your network. Using the M-Series appliance as a Log Collector allows for a more robust environment where the log collection process is offloaded to a dedicated appliance. Using a dedicated appliance in a distributed log collection (DLC) deployment provides redundancy, improved scalability, and capacity for longer term log storage.

In a DLC deployment, the Panorama management server (Panorama virtual appliance or an M-Series appliance in Panorama mode) manages the firewalls and the Log Collectors. Using Panorama, you configure the firewalls to send logs to one or more Log Collectors. You can then use Panorama to query the Log Collectors and provide an aggregated view of network traffic. In a DLC configuration, you can access the logs stored on the Log Collectors from both the primary and secondary Panorama peers in a high availability (HA) pair.

In the following topology, the Panorama peers in an HA configuration manage the deployment and configuration of firewalls. This solution provides the following benefits:

- Enables the Panorama management server to use more resources for management functions.
- Provides high-volume log storage on a dedicated hardware appliance.
- Enables higher logging rates.
- Provides horizontal scalability and redundancy with RAID 1 storage.
- Optimizes bandwidth resources in networks where more bandwidth is available for firewalls to send logs to nearby Log Collectors than to a remote Panorama management server.
- Enables you to meet regional regulatory requirements (for example, regulations might not allow logs to leave a particular region).
Plan Your Deployment

- Determine the management approach. Do you plan to use Panorama to centrally configure and manage the policies, to centrally administer software, content and license updates, and/or centralize logging and reporting across the managed firewalls in the network?

  If you already deployed and configured the Palo Alto Networks firewalls on your network, determine whether to transition the firewalls to centralized management. This process requires a migration of all configuration and policies from your firewalls to Panorama. For details, see Transition a Firewall to Panorama Management.

- Verify the Panorama and firewall software versions. Panorama can manage firewalls running PAN-OS versions that match the Panorama version or are earlier than the Panorama version. The exception is that Panorama 6.1 and later versions cannot push configurations to firewalls running PAN-OS 6.0.0 through 6.0.3. Panorama cannot manage firewalls that run a later PAN-OS version than the Panorama version. For example, Panorama 6.0 cannot manage firewalls running PAN-OS 7.0. For versions within the same feature release, although Panorama can manage firewalls running a later version of PAN-OS, we recommend that Panorama run the same version or a later version. For example, if Panorama runs 7.0.3, it is recommended that all managed firewalls run PAN-OS 7.0.3 or earlier versions.

- Plan to use the same URL filtering database (BrightCloud or PAN-DB) across all managed firewalls. If some firewalls are using the BrightCloud database and others are using PAN-DB, Panorama can only manage security rules for one or the other URL filtering database. URL filtering rules for the other database must be managed locally on the firewalls that use that database.

- Plan to use Panorama in a high availability configuration; set it up as an active/passive high availability pair. See Panorama High Availability.

- Estimate the log storage capacity your network needs to meet security and compliance requirements. Consider such factors as the network topology, number of firewalls sending logs, type of log traffic (for example, URL Filtering and Threat logs versus Traffic logs), the rate at which firewalls generate logs, and the number of days for which you want to store logs on Panorama. For details, see Determine Panorama Log Storage Requirements.

- For meaningful reports on network activity, plan a logging solution:
  - Do you need to forward logs to a syslog server, in addition to Panorama?
  - If you need a long-term storage solution, do you have a Security Information and Event Management (SIEM) solution, such as Splunk or ArcSight, to which you can forward logs?
  - Do you need redundancy in logging?

    With Panorama virtual appliances in HA, each peer can log to its virtual disk. The managed firewalls can send logs to both peers in the HA pair. This option provides redundancy in logging. Panorama running on VMware vCloud Air or ESXi 5.5 and later versions can support a virtual disk of up to 8TB. Earlier versions of the ESXi server support a virtual disk of up to 2TB.

    If you use Dedicated Log Collectors (M-Series appliances in Log Collector mode), you can enable redundancy to ensure that no logs are lost if any one Log Collector in the Collector Group becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector.

    - Will you log to a Network File System (NFS)? Only the Panorama virtual appliance supports NFS. Consider using NFS if Panorama requires more than 8TB of log storage capacity and but doesn’t manage Dedicated Log Collectors. If using NFS, note that the managed firewalls can send logs only to the primary peer in the HA pair, and only the active-primary Panorama is mounted to the NFS and can write to it.

    - If your logging solution includes M-Series appliances, by default they use the management (MGT) interface for configuration, log collection, and Collector Group communication. However, it is a best practice to use the Eth1 or Eth2 interfaces for log collection and Collector Group communication to
improve security, control traffic prioritization, performance, and scalability. Determine whether your solution would benefit from using separate interfaces for these functions. For details, see Set Up the M-Series Appliance.

- Determine what access privileges, roles, and permissions administrators require to access to the managed firewalls and Panorama. See Set Up Administrative Access to Panorama.

- Plan the required Device Groups. Consider whether to group firewalls based on function, security policy, geographic location, or network segmentation. An example of a function-based device group is one that contains all the firewalls that a Research and Development team uses. Consider whether to create smaller device groups based on commonality, larger device groups to scale more easily, or a Device Group Hierarchy to simplify complex layers of administration.

- Plan a layering strategy for administering policies. Consider how firewalls inherit and evaluate policy rules within the Device Group Hierarchy, and how to best implement shared rules, device-group rules, and firewall-specific rules to meet your network needs. For visibility and centralized policy management, consider using Panorama for administering rules even if you need firewall-specific exceptions for shared or device group rules. If necessary, you can Push a Policy Rule to a Subset of Firewalls within a device group.

- Plan the organization of your firewalls based on how they inherit network configuration settings from Templates and Template Stacks. For example, consider assigning firewalls to templates based on hardware models, geographic proximity, and similar network needs for time zones, a DNS server, and interface settings.
## Deploy Panorama: Task Overview

The following task list summarizes the steps to get started with Panorama. For an example of how to use Panorama for central management, see Use Case: Configure Firewalls Using Panorama.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>(M-Series appliance only)</strong> Rack mount the appliance.</td>
</tr>
<tr>
<td>2</td>
<td>Perform initial configuration to enable network access to Panorama. See Set Up the Panorama Virtual Appliance or Set Up the M-Series Appliance.</td>
</tr>
<tr>
<td>3</td>
<td>Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td>4</td>
<td>Install Content and Software Updates for Panorama.</td>
</tr>
<tr>
<td>5</td>
<td><strong>(Optional/recommended)</strong> Set up Panorama in a high availability configuration. See Panorama High Availability.</td>
</tr>
<tr>
<td>6</td>
<td>Add a Firewall as a Managed Device.</td>
</tr>
<tr>
<td>7</td>
<td>Add a Device Group or Create a Device Group Hierarchy, Add a Template, and (if applicable) Configure a Template Stack.</td>
</tr>
<tr>
<td>8</td>
<td><strong>(Optional)</strong> Configure log forwarding to Panorama and/or to external services. See Manage Log Collection.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Monitor Network Activity</strong> using the visibility and reporting tools on Panorama.</td>
</tr>
</tbody>
</table>