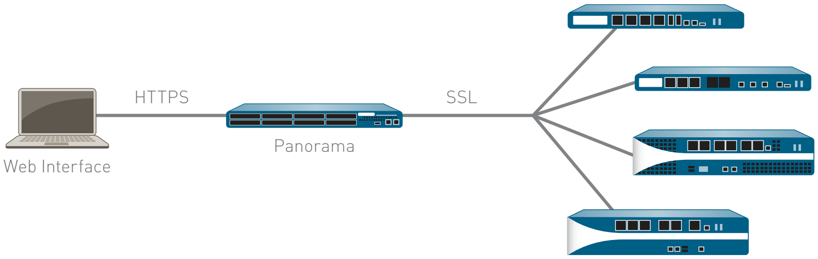
PANORAMA

Panorama provides centralized policy and device management over a network of Palo Alto Networks™ next-generation firewalls.

- View a graphical summary of the applications on the network, the respective users, and the potential security impact.
- Deploy corporate policies centrally to be used in conjunction with local policies for maximum flexibility.
- Delegate appropriate levels of administrative control at the device level or globally with role-based management.
- Centrally analyze, investigate and report on network traffic, security incidents and administrative modifications.



Large organizations commonly have many firewalls deployed throughout their network and more often than not, the process of managing and controlling them is cumbersome due to complexities and inconsistencies between individual devices. The result is an increase in administrative efforts and associated costs.

Panorama provides centralized management and visibility of Palo Alto Networks next-generation firewalls. From a central location, administrators can gain insight into applications, users and content traversing the firewalls. The knowledge of what is on the network, in conjunction with safe application enablement policies, maximizes protection and control while minimizing administrative effort. Administrators can centrally perform analysis, reporting and forensics with the aggregated data over time, or on data stored on the local firewall.

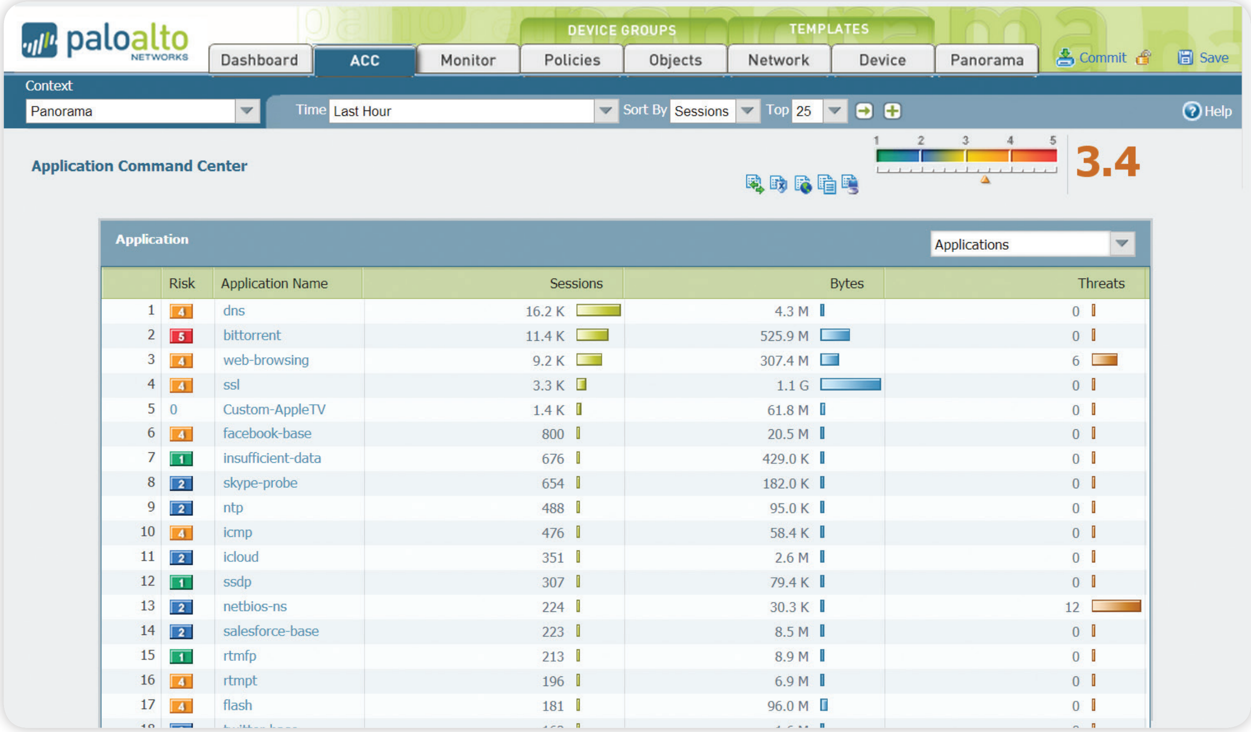
Both Panorama and the individual devices share the same web-based look and feel, minimizing any learning curve or delay in executing the task at hand. Palo Alto Networks adheres to a management philosophy that emphasizes consistency, providing a significant advantage over competitive offerings.

Central Visibility: Application Command Center

Using Application Command and Control (ACC) from Panorama provides an administrator with a graphical view of application, URL, threat and data (files and patterns) traversing all Palo Alto Networks devices under management. ACC dynamically fetches data from each device to ensure that administrators have an up-to-date view of the applications on the network, who is using them, and the potential threats they may pose. Administrators can investigate new or unfamiliar applications with a single click that displays a description of the application, its key features, its behavioral characteristics, and who is using it.

Additional data on URL categories and threats provides a complete and well-rounded picture of network activity. The visibility from ACC allows administrators to make informed policy decisions and to respond quickly to potential security threats.

paloalto NETWORKS
the network security company™



Context: Panorama

Time: Last Hour

Sort By: Sessions

Top: 25

Application Command Center

Application: Applications

	Risk	Application Name	Sessions	Bytes	Threats
1	4	dns	16.2 K	4.3 M	0
2	5	bittorrent	11.4 K	525.9 M	0
3	4	web-browsing	9.2 K	307.4 M	6
4	4	ssl	3.3 K	1.1 G	0
5	0	Custom-AppleTV	1.4 K	61.8 M	0
6	4	facebook-base	800	20.5 M	0
7	1	insufficient-data	676	429.0 K	0
8	2	skype-probe	654	182.0 K	0
9	2	ntp	488	95.0 K	0
10	4	icmp	476	58.4 K	0
11	2	icloud	351	2.6 M	0
12	1	ssdp	307	79.4 K	0
13	2	netbios-ns	224	30.3 K	12
14	2	salesforce-base	223	8.5 M	0
15	1	rtmfp	213	8.9 M	0
16	4	rtmpt	196	6.9 M	0
17	4	flash	181	96.0 M	0

Application Command Center provides global and local views of application traffic, complete with drill-down to learn more about current activity.

Global Policy Control: Safely Enabling Applications

Safely enabling applications means allowing access to specific applications with specific threat prevention and file, data, or URL filtering policies applied. Panorama facilitates safe application enablement across the entire network of firewalls by allowing administrators to manage rules from a central location.

Panorama-based shared policies help ensure compliance with internal or regulatory requirements while local device rules maintain both security and flexibility. Combining centralized and local administrative control over policies and objects can help strike a balance between consistent security at the global level and flexibility at the local level.

Administrators can deploy policies that safely enable applications or application functions based on users via directory services integration while application-specific threat prevention protects the contents and the network. The ability to set a single policy that safely enables applications based on user—not IP addresses—allows organizations to dramatically reduce the number of policies required. An added benefit of directory services integration is a dramatic reduction in administrative overhead associated with employee adds, moves and changes that may occur on a day-to-day basis – security policies remain stable while the employees are moved from one group to another.

Traffic Monitoring: Analysis, Reporting and Forensics

Panorama utilizes the same set of powerful monitoring and reporting tools available at the local device management level and adds visibility by providing an aggregate view of activities. As administrators perform log queries and generate reports, Panorama dynamically pulls the most current data directly from firewalls under management or from logs forwarded to Panorama. Access to the latest information across all devices allows administrators to address security incidents as well as take a proactive position to protect corporate assets.

- **Log Viewer:** For either an individual device, or all devices, Panorama administrators can quickly view log activities using dynamic log filtering by clicking on a cell value and/or using the expression builder to define the sort criteria. Results can be saved for future queries or exported for further analysis.
- **Custom Reporting:** Predefined reports can be used as-is, customized, or grouped together as one report in order to suit specific requirements.
- **User Activity Reports:** From Panorama, a user activity report shows the applications used, URL categories visited, web sites visited, and all URLs visited over a specified period of time for individual users. Panorama builds the reports using an aggregate view of user's activity, no matter which firewall they are protected by, or which IP or device they may be using.

Panorama Management Architecture

Panorama enables organizations to manage their Palo Alto Networks firewalls using a model that provides both central oversight and local control. Panorama provides a number of tools for centralized administration:

- **Templates:** Panorama manages common device and network configuration through templates. Templates can be used to manage configuration centrally and then push the changes to all managed firewalls. This approach avoids making the same individual firewall change repeatedly across many devices. One example of such use is to push common DNS and NTP server settings across hundreds of firewalls, rather than performing the same change on a device by device basis.

- **Device Groups:** Panorama manages common policy and objects through device groups. Device groups are used to centrally manage the rulebases of many devices with common requirements. Examples of ways to group devices in device groups may be geographically (e.g., Europe and North America) or functionally (e.g., perimeter or datacenter) oriented. Within device groups, virtual systems are treated as individual devices, at the same level as physical firewalls. This allows common rulebase sharing across different virtual systems on a device.

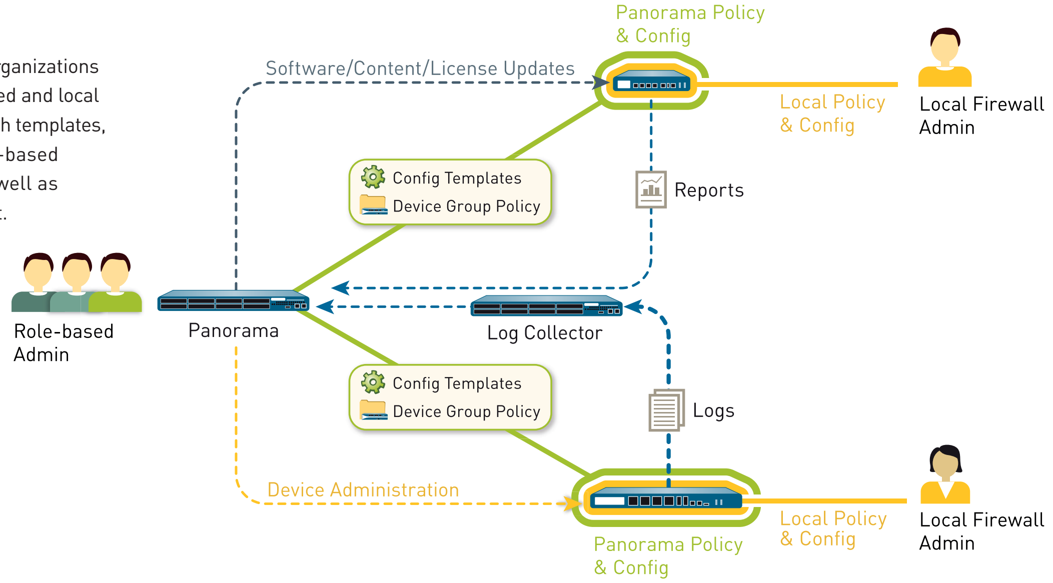
  Organizations can use shared policies for central control while still providing the firewall administrator with the autonomy to make specific adjustments for local requirements. At the device group level, administrators can create shared policies that are defined as the first set of rules (pre-rules) and the last set of rules (post-rules) to be evaluated against match criteria. Pre- and post-rules can be viewed on a managed firewall, but can only be edited from Panorama within the context of the administrative roles that have been defined. Local device rules (those between pre- and post-rules), can be edited by either the local administrator, or by a Panorama administrator who has switched to a local firewall context. In addition, an organization can use shared objects defined by a Panorama administrator, which can be referenced by locally managed device rules.

- **Role-based Administration:** Organizations can use role-based administration to delegate feature level administrative access (enabled, read-only, or disabled and hidden from view) to different staff members. Specific administrators can be given appropriate access to the tasks that are pertinent to their job while making other access either hidden or read-only. An example of how this type of access control could be used is to define different roles for personnel responsible for different tasks across the enterprise, such as the security admins versus network admins. All changes made by an administrator are logged, showing the time of occurrence, the administrator, the management interface used (Web UI, CLI, Panorama), the command or action taken.

- **Software, Content and License Update Management:** As a deployment grows in size, many organizations want to make sure that updates are sent to downstream boxes in an organized manner. For instance, security teams may prefer to centrally qualify a software update before it's delivered via Panorama to all production firewalls at once. Using Panorama, the update process can be centrally managed for software updates, content (application updates, antivirus signatures, threat signatures, URL filtering database, etc) and licenses.

Using templates, device groups, role-based administration, and update management, organizations can delegate appropriate access to all management functions; visualization tools, policy creation, reporting and logging at both a global level as well as a local level.

Panorama allows organizations to balance centralized and local management through templates, device groups, role-based administration, as well as update management.



Deployment Flexibility

Organizations can deploy Panorama either as a hardware appliance or as a virtual appliance.

Hardware Appliance

Organizations which prefer to deploy Panorama on high performance dedicated hardware, or would like to separate the Panorama management and logging functions for large volumes of log data, can use the M-100 hardware appliance to meet their needs. Panorama running on the M-100 can be deployed in the following ways:

- **Centralized:** In this scenario, all Panorama management and logging functions are consolidated into a single device (with the option for high availability).
- **Distributed:** An organization may prefer to separate the management and logging functions across multiple devices. Under this configuration, the functions are split between managers and log collectors.
  - **Panorama Manager:** The Panorama manager is responsible for handling the tasks associated with policy and device configuration across all managed devices. The manager does not store log data locally, but rather uses separate log collectors for handling log data. The manager analyzes the data stored in the log collectors for centralized reporting.
  - **Panorama Log Collector:** Organizations with high logging volume and retention requirements can deploy dedicated Panorama log collector devices that will aggregate log information from multiple managed firewalls.

The separation of management and log collection enables organizations to optimize their deployment in order to meet scalability, organizational or geographical requirements.

Virtual Appliance

Panorama can be deployed as a virtual appliance on VMware ESX(i), allowing organizations to support their virtualization initiatives and consolidate the rack space which is sometimes limited or costly in a data center. The virtual appliance can be deployed in two ways:

- **Centralized:** All Panorama management and logging are consolidated into a single virtual appliance (with the option for high availability).
- **Distributed:** Panorama distributed log collection supports a mix of the hardware and virtual appliance.
  - **Panorama Manager:** The virtual appliance can serve as a Panorama manager, and is responsible for handling the tasks associated with policy and device configuration across all managed devices.
  - **Panorama Log Collector:** Panorama log collectors are responsible for offloading intensive log collection and processing tasks, and may be deployed using the M-100. The virtual appliance may not be used as a Panorama log collector.

Providing the choice of either a hardware or virtualized platform, as well as the choice to combine or separate the Panorama functions, provides organizations with the maximum flexibility for managing multiple Palo Alto Networks firewalls in a distributed network environment.

PANORAMA SPECIFICATIONS

Number of devices supported	Up to 1,000
High Availability	Active/Passive
Administrator authentication	Local database RADIUS

M-100 MANAGEMENT APPLIANCE SPECIFICATIONS

I/O

- (1) 10/100/1000, (3) 10/100/1000 (for future use), (1) DB9 Console serial port

STORAGE

- M-100 1TB RAID: 2 x 1TB RAID Certified HDD for 1TB of RAID Storage
- M-100 4TB RAID: 8 x 1TB RAID Certified HDD for 4TB of RAID Storage

POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- 500W/500W

MAX BTU/HR

- 1,705

INPUT VOLTAGE (INPUT FREQUENCY)

- 100-240VAC (50-60Hz

MAX CURRENT CONSUMPTION

- 10A@100VAC

MEAN TIME BETWEEN FAILURE (MTBF)

14.5 Years

RACK MOUNTABLE (DIMENSIONS)

- 1U, 19” standard rack (1.75”H x 23”D x 17.2”W)

WEIGHT (STANDALONE DEVICE/AS SHIPPED)

- 26.7lbs/35 lbs

SAFETY

- UL, CUL, CB

EMI

- FCC Class A, CE Class A, VCCI Class A

ENVIRONMENT

- Operating temperature: 40 to 104 F, 5 to 40 C
- Non-operating temperature: -40 to 149 F, -40 to 65 C

VIRTUAL APPLIANCE SPECIFICATIONS

MINIMUM SERVER REQUIREMENTS

- 80 GB Hard Drive
- 2 GHz CPU
- 2 GB RAM

VMWARE SUPPORT

- VMware ESX 3.5, 4.0, 4.1, 5.0

BROWSER SUPPORT

- IE v7 or greater
- Firefox v3.6 or greater
- Safari v5.0 or greater
- Chrome v11.0 or greater

LOG STORAGE

- VMware Virtual Disk: 2TB maximum
- NFS

paloalto NETWORKS

the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

PAN_SS_P_103112