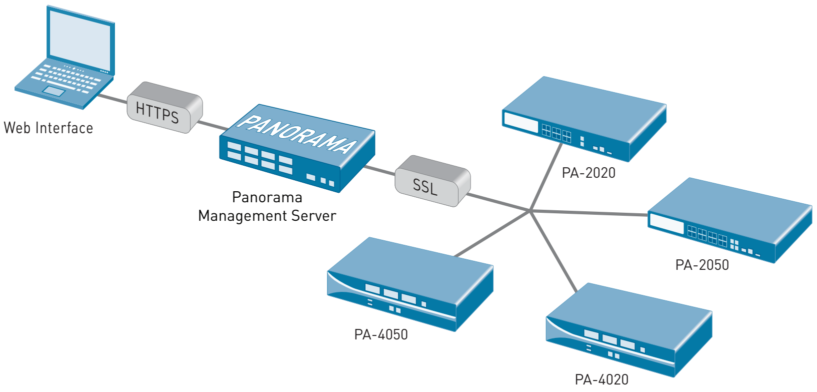
Panorama

Panorama provides centralized policy and device management over a distributed 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 – for individual devices or collectively.
- 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 organization and more often than not, the process of managing and controlling them is cumbersome due to complexities and inconsistencies between individual devices and centralized management interfaces. The result is increased administrative efforts and associated costs.

Panorama provides centralized visibility and management of multiple Palo Alto Networks next-generation firewalls. From a central location, administrators can gain insight into applications, users and content traversing the firewalls controlled by Panorama. The knowledge of what is on the network, at the individual firewall level or collectively, at a global level, can then be translated into secure application enablement policies, thereby maximizing protection and control, while minimizing the administrative efforts. Analysis, reporting and forensics can be performed against the aggregated data over time, or against more recent data delivered in an on-demand manner.

Palo Alto Networks adheres to a management philosophy that emphasizes consistency, no matter which management mechanism is being used: Panorama, the device user interface, or the command line interface (CLI). The management interfaces for both Panorama and the individual devices share the same web-based look and feel, minimizing any learning curve or a delay in executing the task at hand. Management consistency is a significant advantage that Palo Alto Networks has over competitive offerings.

paloalto NETWORKS
the network security company™

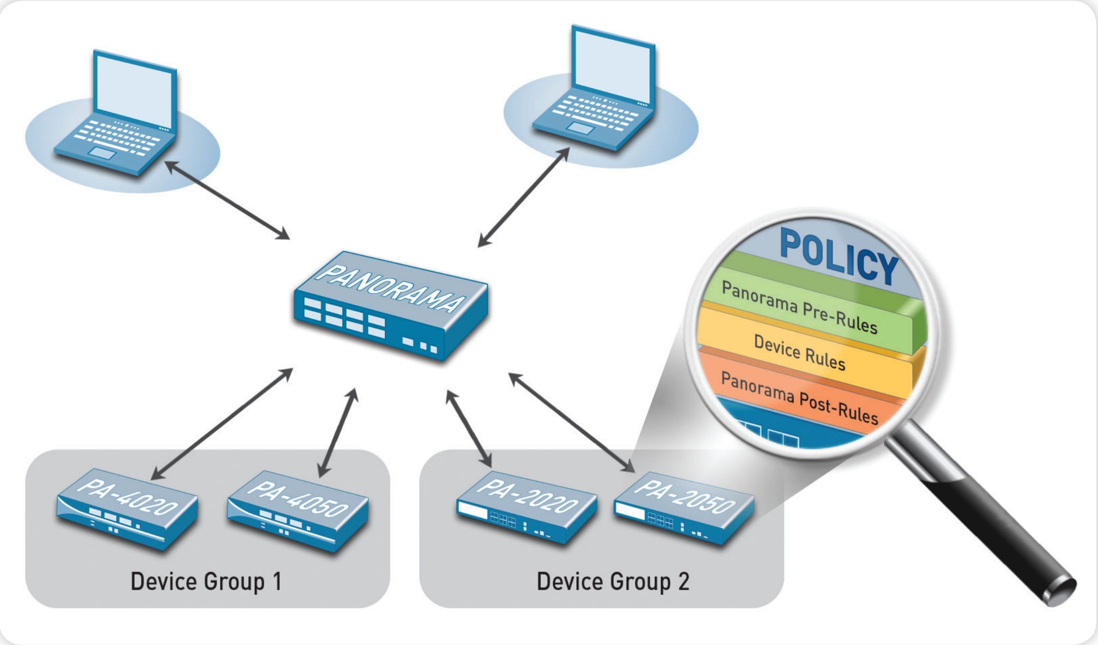
Panorama Management Architecture

A Panorama deployment is comprised of the central Panorama server, a browser-based interface and the network of Palo Alto Networks firewalls to be managed. Panorama enables organizations to distribute the management of their Palo Alto Networks firewalls using a central oversight with local control model. Central oversight is achieved using device groups, shared policies, shared objects, access domains, and role-based administration.

- **Device Groups:** A device group is a means of assembling the firewalls into a smaller, more easily managed group of devices. Within device groups, virtual systems can be treated as an individual device, at the same level as the physical firewalls. Examples of device groups may be geographical (Europe and North America), functional (firewall and IPS) or deployment (perimeter or datacenter) oriented.
- **Shared Policies and Objects:** Administrators can use shared policies and objects to help strike a balance between centralized and local policy control. At the device group level, administrators can create shared policies that are defined as the first set of rules to be executed (pre-rules) and the last set of rules to be executed (post-rules) at the device level. Pre- and post-rules can be viewed on a managed firewall, but can only be edited when inside Panorama. Local device rules (those between pre- and post-rules), can be edited by either the local administrator or a Panorama administrator who has switched to a local firewall context.

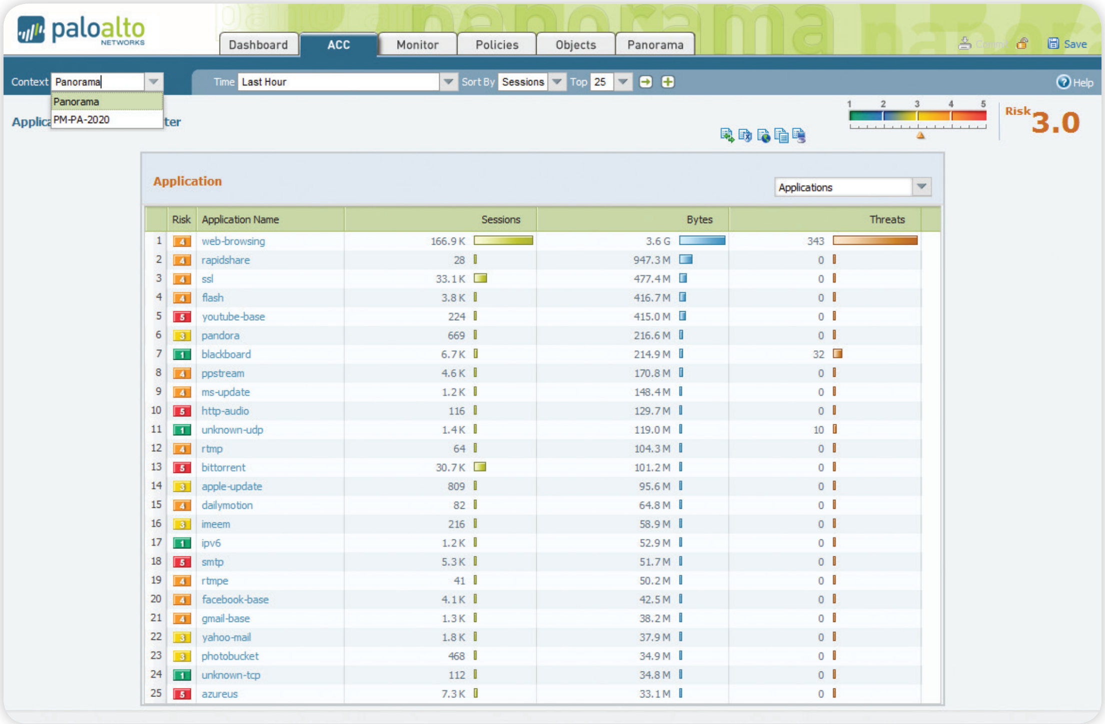
  Shared objects operate in much the same manner as shared policies in that they can only be created and managed by the super administrator. However, shared objects can be used within the locally managed rules, not just the pre- and post-rules. Combining centralized and local administrative control over policies and objects can help strike a balance between consistent security at the global level and flexibility at the local level.
- **Access Domains:** Access domains are the set of firewalls, either physical or virtual, that administrators can manage. Access domains can be comprised of either device groups or individual devices. Within access domains, role-based administration can be used to further control which functions an administrator can use.
- **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. With the most granular role-based administration on the market, specific individuals can be given appropriate access to the tasks that are pertinent to their job. All administrative activities are logged, showing the time of occurrence, the administrator, the management interface used (web UI, CLI, Panorama), the command or action taken.

Using device groups, access domains, and role-based administration, 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 Management Architecture

Panorama allows organizations to balance centralized and local management through device groups, access domains and shared rules/objects.



Context: Panorama (Panorama, PM-PA-2020) · Time: Last Hour · Sort By: Sessions · Top: 25

Application · Applications

	Risk	Application Name	Sessions	Bytes	Threats
1	4	web-browsing	166.9 K	3.6 G	343
2	4	rapidshare	28	947.3 M	0
3	4	ssl	33.1 K	477.4 M	0
4	4	flash	3.8 K	416.7 M	0
5	5	youtube-base	224	415.0 M	0
6	3	pandora	669	216.6 M	0
7	1	blackboard	6.7 K	214.9 M	32
8	4	ppstream	4.6 K	170.8 M	0
9	4	ms-update	1.2 K	148.4 M	0
10	5	http-audio	116	129.7 M	0
11	1	unknown-udp	1.4 K	119.0 M	10
12	4	rtmp	64	104.3 M	0
13	5	bittorrent	30.7 K	101.2 M	0
14	3	apple-update	809	95.6 M	0
15	4	dailymotion	82	64.8 M	0
16	3	imeem	216	58.9 M	0
17	1	ipv6	1.2 K	52.9 M	0
18	5	smtp	5.3 K	51.7 M	0
19	4	rtmpe	41	50.2 M	0
20	4	facebook-base	4.1 K	42.5 M	0
21	4	gmail-base	1.3 K	38.2 M	0
22	3	yahoo-mail	1.8 K	37.9 M	0
23	3	photobucket	468	34.9 M	0
24	1	unknown-tcp	112	34.8 M	0
25	5	azureus	7.3 K	33.1 M	0

Application Command Center
Within Panorama, ACC provides either a global view or a local view of application traffic, complete with drill-down to learn more about current activity.

Application Command Center: Knowledge is Power

Using ACC within 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 every 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. New or unfamiliar applications that are seen in ACC can be quickly investigated with a single click that displays a description of the application, its key features, its behavioral characteristics, and who is using it.

For either an individual firewall or across the entire network of firewalls, an administrator can research an application by applying filters to learn more about individual user behavior, threats and the associated traffic patterns. Additional data on URL categories, threats, and data provides a complete and well-rounded picture of network activity. The visibility that ACC data mining provides allows administrators to make more informed policy decisions or respond more quickly to potential security threats.

Global Policy Control: Securely Enabling Applications

Panorama provides administrators with a global view of network activity and the power to react in an appropriate manner. Pre- and post-rules can help enforce consistent policies to ensure compliance with internal or regulatory requirements while local device rules can be deployed to maintain security and flexibility. Administrators can quickly deploy application, application function, and port-based enablement policies with responses that range from open (allow), to moderate (enabling certain applications or functions, then scan, or shape, schedule, etc.), to closed (deny). The tight integration of application control, based on users and groups, and the ability to scan the allowed traffic for a wide range of threats, allows organizations to dramatically reduce the number of policies they are deploying along with the number of employee adds, moves and changes that may occur on a day-to-day basis.

Securely enabling applications means allowing access to the applications, then applying specific threat prevention and file, data, or web traffic blocking policies. Panorama facilitates secure application enablement across the entire network of firewalls by allowing administrators to manage all of the rulebases from a central location: security, NAT, QoS, policy based forwarding, decryption, application override, captive portal, and DoS protection.

Shared Traffic Monitoring: Analysis, Reporting and Forensics

Leveraging the storage available in each device, detailed logs are collected locally, focusing log forwarding on meeting long term retention requirements Panorama utilizes the same set of powerful monitoring and reporting tools available at the local device management level, and as administrators perform log queries and generate reports, Panorama dynamically pulls the most current data from all the devices under management or from each individual device as needed. Access to the latest information across all devices allows administrators to strike an appropriate balance between being proactive, continually learning and adapting to protect the corporate assets and being reactive, investigating, analyzing and reporting on security incidents.

- **Log viewer:** For either an individual device, or all devices, Panorama administrators can quickly view log activities using the dynamic log filtering enabled simply 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 the specific requirements. All reports can be exported to CSV or PDF format and they can be executed and emailed on a scheduled basis.
- **User Activity Reports:** From Panorama, a user activity report (UAR) that shows the applications used, URL categories visited, web sites visited, and all the URLs visited over a specified period of time can be generated for individual users. When the UAR is generated from Panorama, the data used is an aggregate of all the user activity, no matter which firewall they are being protected by.
- **Log storage and archival:** In order to meet backup or longevity requirements, Panorama can store an unlimited amount of log data using NFS, allowing organizations to use Panorama as the Palo Alto Networks firewall log collection repository. Syslog forwarding is also supported, allowing organizations to easily use 3rd party offerings for long term storage and more detailed analysis.

Deployment Flexibility

Panorama is deployed as a virtual appliance on VMware, providing the flexibility to enable deployment on a wide range of OS and hardware combinations. Installation and management of Panorama can be done through both a web and command-line interface.

Panorama Specifications

SPECIFICATIONS	
Number of Devices Supported	Up to 1,000
Administrator Authentication	Local database, RADIUS
Log Storage Capacity	VMware Virtual Disk: 2TB maximum, NFS: 2TB+
Command Line Interface	SSHv2, Telnet or Console
Web Interface	HTTPS, HTTP
Device Connection	SSLv2
MINIMUM SYSTEM REQUIREMENTS	
Minimum Server Hardware Requirements	80 GB Hard Drive, 2 GHz CPU, 2 GB RAM
Platform Support	Deployed as a virtual appliance on VMware
VMware Support	VMware ESX 3.5 or later, VMware Server 1.0.5 or greater
Browser Support	IE v7 or greater, Firefox v3.6 or greater, Safari v5.0 or greater, Chrome v11.0 or greater

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