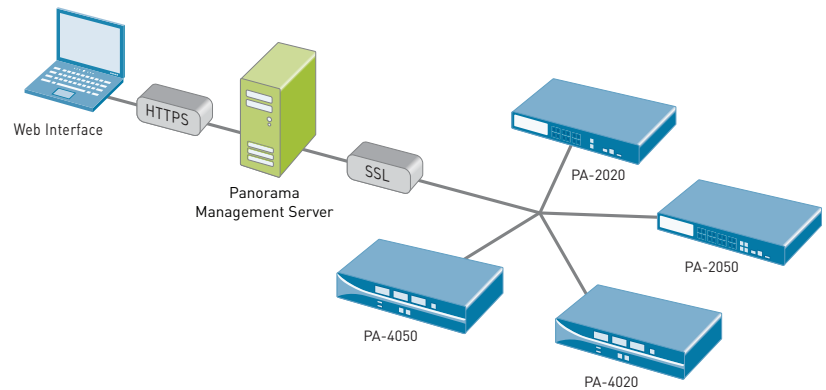


Panorama

Panorama is a centralized security management system that provides global control over multiple Palo Alto Networks' firewalls.

Centralized Visibility, Control and Management:

- Enables simple and intuitive view into applications, users and content flowing across multiple Palo Alto Network's firewalls with a powerful set of visualization tools
- Delivers centralized visibility and control over more than 700 applications
- Facilitates complete device management in a secure manner from a central location



Large enterprises commonly have many firewalls deployed throughout their organization and more often than not, the process of managing and controlling them is cumbersome due to management complexities and inconsistencies between individual device vs centralized management interfaces. The result is an increase in administrative efforts and associated costs.

Panorama provides centralized management of multiple Palo Alto Network's firewalls using an intuitive, easy-to-use web-based interface. With Panorama, administrators can view application and associated user activity, monitor threats, deploy shared or single device policies, filter logs and generate reports for individual firewalls or for a global network of Palo Alto Networks' firewalls.

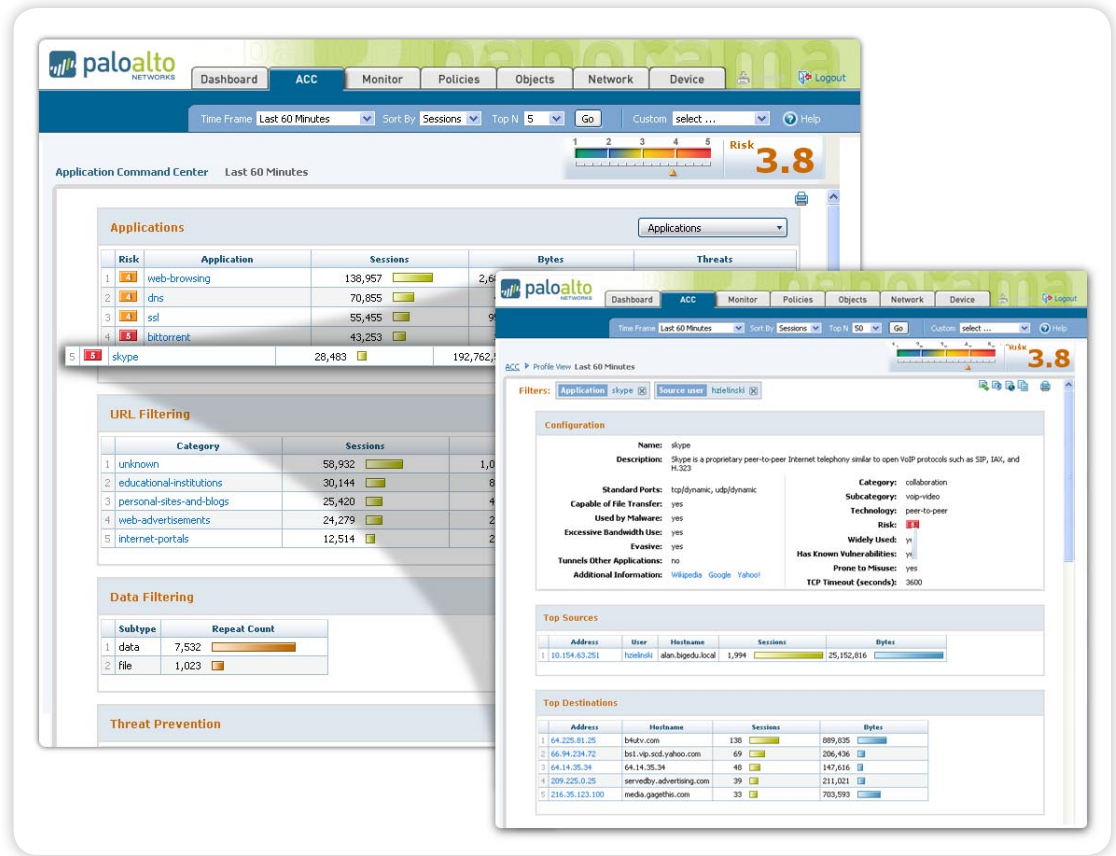
The Panorama web interface achieves two goals. First, it eliminates the need to install a desktop client, enabling access for virtually any browser. Secondly, the web interface carries the exact same look and feel as the individual device management interface which eliminates management inconsistencies that currently plague administrators using other firewall management solutions.

Management Flexibility

To accommodate the dynamic nature of network security and the varied management styles that each administrator may have, the PA-4000 Series and the PA-2000 Series next-generation firewalls can be controlled by a Command Line Interface (CLI), a web-based interface, or a centralized management solution (Panorama) as well as standards-based syslog and SNMP interfaces. Adding Panorama to the IT environment does not preclude administrators from making configuration and management changes using the Command Line Interface (CLI) or the web-based interface. Panorama will always work with the latest configuration, regardless of which management interface was used to make the previous edits.

Application Command Center

View current application, URL, data filtering and threat activity in a clear, easy-to-read format. Add/remove filters to navigate to any depth of data specificity.



Shared Policies

When managing multiple devices with Panorama, a group of devices can now share a set of pre- and post-rules. Device administrators will be able to see these rules, but only a Panorama administrator can modify or remove them. Shared policies enable administrators to establish a baseline policy on top of which the local rules are built with the result being a reduction in administrative efforts and improved policy consistency.

Role-based Administration

For those environments where different staff members require varied levels of access to the management interface, role-based administration allows any of the features in the web interface to be enabled, read-only, or disabled (hidden from view). 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. Some examples:

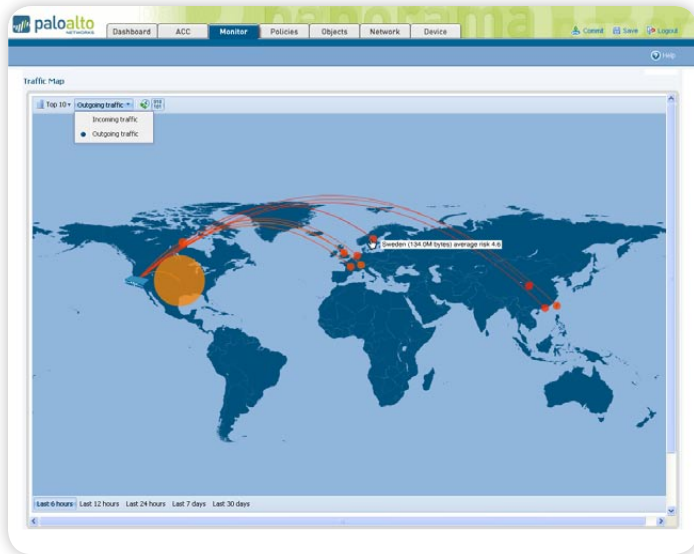
- Executives might be given read-only access to key reporting functions.
- The operations staff may have access to the device and networking configuration.
- Security administrators are given control over security policy definition along with access to the log viewer and reporting.
- Key individuals are given full CLI access while for others, the CLI may be disabled.

All administrative roles and related activities are logged, showing the time of occurrence, the administrator, the management interface used (web UI, CLI, Panorama), the command or action taken along with the result.

Powerful Visualization Tools

The same powerful set of visualization tools that are available in PAN-OS are also available in Panorama, allowing administrators to see the applications traversing the network, who is using them, and assess the potential security impact within a single firewall or across a network of Palo Alto Networks' firewalls.

- **Application Command Center (ACC):** ACC provides a visual display of application, URL, threat and data transfer activity for a single firewall or aggregated across many firewalls. ACC provides administrators with an easy to understand view into current activity that can be tailored to display the data from a variety of different perspectives.
 - ▶ Application data can be viewed by risk level, by category or subcategory or by underlying technology.
 - ▶ Web activity can be displayed based on top URLs visited or blocked or top URL categories visited or blocked.
 - ▶ Data filtering activity can show the sensitive files and data patterns such as SSN and CC # that are being sent across the network.
 - ▶ Threat activity can be viewed based on spyware, application vulnerability exploits, and viruses.



Traffic Map

Geographical map of traffic and threats flowing in and out of the network.

- **Data Mining with ACC:** To learn more about the applications, URLs, data and threats traversing the network, administrators can mine ACC data by adding and removing filters in order to achieve the desired result. For example, selecting a specific application shows the details of what the application is, who is using it and the source / destination countries. Additional filters can be added to learn more about individual user behavior, which security zones are sending/receiving the traffic, the potential threats and what files or data types are being transferred. In the event that ACC displays something that warrants immediate, in depth log analysis, administrators can jump to the appropriate log filter that matches the current ACC context with a click of a mouse.
- **Reporting and Logging:** The log viewer enables forensic investigation into every session traversing the network using real-time filtering. Fully customizable and schedulable reports are available that provide detailed views into applications, users, and threats on the network.

Log Management and Reporting

Leveraging the storage available in each device, detailed logs are collected locally, eliminating the requirement for centralized logging. As ACC, logging and reporting views are used, Panorama dynamically pulls the most current data from all the devices under management or from each individual device as needed.

- **Log storage and archival:** Collect logs with Panorama in a centralized location in order to meet backup or longevity requirements or send them to a syslog server for long term storage and more detailed analysis.
- **Log viewer:** View application, threat and user activity through with dynamic filtering capabilities enabled simply by clicking on a cell value and /or using the expression builder to define the sort criteria.
- **Log exporting:** Export any logs matching the current filter to a CSV file for offline archival or further analysis.
- **Custom reports:** Create custom reports from scratch, pulling data from any of the log databases or modify one of the predefined reports.

The screenshot shows the Palo Alto Networks Security Rules configuration page. The interface includes a navigation bar at the top with tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. Below the navigation bar, there are filter options for Filter Rules (All Rules), Source Zone (Show All), Destination Zone (Show All), and Filter By Zone. The main content area displays a table of Security Rules. On the left side, there is a sidebar for Rulebases, including Security, NAT, SSL Decryption, Application Override, and Captive Portal. The Security Rules table has columns for Name, Source Zone, Destination Zone, Source Address, Source User, Destination Address, Application, Service, Action, Profile, and Options. The table lists 15 rules, including 'No Intra-zone DMZ', 'Monitor ALL', 'Block P2P', 'Webmail - No Attachments', 'CEO YouTube', 'Block High Risk Media', 'Allow IT Remote Access', 'CFO Warcraft', 'Block Remote Access', 'Control Finance Web Posting', 'General Web', 'Inbound SMTP', 'Corp Webserver', 'Deny and Log Outbound', and 'Deny and Log Inbound'. Each rule has a corresponding icon in the Action column, indicating its status (e.g., enabled, disabled, or blocked).

Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1 No Intra-zone DMZ	DMZ	DMZ	any	any	any	any	any	Deny	none	
2 Monitor ALL	tapzone	tapzone	any	any	any	any	any	Log	none	
3 Block P2P	trust	untrust	any	any	any	P2P Filesharing	any	Deny	none	
4 Webmail - No Attachments	trust	untrust	any	any	any	Webmail	any	Deny	none	
5 CEO YouTube	trust	untrust	any	patraining/hzelinski	any	youtube	any	Log	none	
6 Block High Risk Media	trust	untrust	any	any	any	High Risk Media	any	Deny	none	
7 Allow IT Remote Access	trust	untrust	any	patraining/administrators	any	Remote Access	any	Log	none	
8 CFO Warcraft	trust	untrust	any	patraining/stoller	any	worldofwarcraft	any	Log	none	
9 Block Remote Access	trust	untrust	any	any	any	Remote Access	any	Deny	none	
10 Control Finance Web Posting	trust	untrust	any	patraining/finance	any	Web Posting	any	Deny	none	
11 General Web	trust	untrust	any	any	any	web-browsing	any	Log	none	
12 Inbound SMTP	untrust	DMZ	any	any	10.0.0.253	smtp	application-def:aut	Log	none	
13 Corp Webserver	untrust	DMZ	any	any	10.0.0.249	web-browsing	application-def:aut	Log	none	
14 Deny and Log Outbound	trust	untrust	any	any	any	any	any	Deny	none	
15 Deny and Log Inbound	untrust	trust	any	any	any	any	any	Deny	none	

Shared Policies

Panorama enables administrators to deploy shared policies (green) to a global network of Palo Alto Networks firewalls.

- **Report exporting:** Export any of the predefined or custom reports to either CSV or PDF. Any of the PDF reports can be emailed on a scheduled basis.
- **Summary report:** A custom, one-page summary pulls data from any of the predefined or custom reports and can be generated and emailed on a scheduled basis.

Policy Controls

Increased visibility into applications, users and threats traversing the network means the security team can quickly analyze the data and address potential security risks through firewall policies such as:

- Deploy a set of traditional inbound and outbound port-based firewall rules that are shared across all Palo Alto Networks firewalls under management.
- Assign Salesforce.com and Oracle to the sales and marketing groups as defined in Active Directory. Define a group of applications such as SSH, Telnet, MS-RDP and allow only the IT group to use them.
- Define and enforce a corporate policy that dictates which webmail and instant messaging applications should be used and inspect them for viruses, spyware and vulnerability exploits—all in a single policy rule.

- Identify the transfer of sensitive information such as credit card numbers or social security numbers, either in text or file attachments, and block, send alerts on who is transferring the data.
- Implement multi-level URL filtering policies that block access to obvious non-work related sites, monitor questionable sites and “coach” access to others by giving the user the ability to acknowledge the policy and proceed.
- Create traditional inbound and outbound port-based firewall rules mixed with application-based rules to smooth the transition to a Palo Alto Networks next generation firewall.

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. The delivery of Panorama as a virtual appliance on VMware enables installation on the platform of choice, bringing the same characteristics of the Palo Alto Networks’ purpose-built appliances high performance, easy-to-manage, and secure. Installing and managing Panorama can be accomplished through both a web and command-line interface.

Panorama Specifications

SPECIFICATIONS	
Number of Devices Support	Up to 1,000
Administrator Authentication	Local database, RADIUS
Log Storage	Maximum of 2 TB
Command Line Interface	SSHv2, Telnet or Console
Web Interface	HTTPS, HTTP
Device Connection	SSLv2
MINIMUM SYSTEM REQUIREMENTS	
Platform Support	Deployed as a virtual VMware appliance on a wide range of Linux and Microsoft Windows variants: Linux (Red Hat, SuSE, Ubuntu, Mandriva) Windows (Vista, Server 2003, XP, 2000)
Minimum Server Hardware Requirements	80 GB Hard Drive, 2 GHz CPU, 2 GB RAM
VMware Support	VMware ESX 3.5 or later, VMware Server 1.0.5 or later
Browser Support	Internet Explorer 6.0 or later, Firefox 1.5 or later
ORDERING INFORMATION	
Panorama for managing up to 25 devices	PAN-PRA-25
Panorama for managing up to 100 devices	PAN-PRA-100
Panorama for managing up to 1000 devices	PAN-PRA-1000
PART NUMBER	



Palo Alto Networks
 232 E. Java Drive
 Sunnyvale, CA. 94089
 Sales 866.207.0077
www.paloaltonetworks.com

Copyright ©2008, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

840-000006-00A