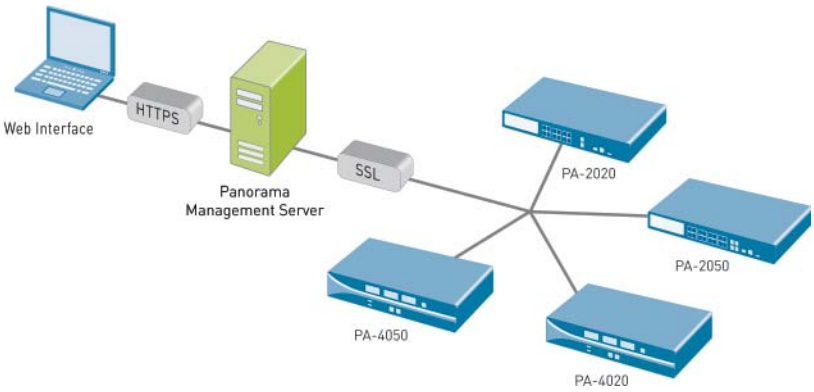
Panorama

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

Centralized Visibility, Control and Management:

- Perform centralized device and policy management of multiple Palo Alto Network's firewalls.
- 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.
- 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 and centralized management interfaces. The result is an increase in administrative efforts and associated costs.

Panorama provides centralized management of multiple Palo Alto Network's next-generation firewalls, enabling administrators to view applications, who is using them, any associated threats and respond by deploying shared or single device policies. Logs can be consolidated and filtered to gain an aggregate view of network activity while reports can be generated for an individual or multiple firewalls.

The management interfaces for both Panorama and the individual devices share the exact same web-based look and feel which achieves two goals. First, it eliminates the need to install a desktop client, enabling access for virtually any browser. Second, the consistent look and feel eliminates management inconsistencies that currently plague administrators using other firewall management solutions.

Management Flexibility

All of the Palo Alto Networks next-generation firewalls can be controlled by a Command Line Interface (CLI), a web-based interface, or Panorama as well as monitored with standards-based syslog, SNMP interfaces and a REST API. 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 for a global network of, or an individual instance of Palo Alto Networks firewalls.

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 graphically displays a current view of application, URL, threat and data (files and patterns) traversing all Palo Alto Networks devices under management. An administrator can research an application by applying filters to see which employees are using the application and the threats that they may introduce to the network. Additional filters can be added to learn more about individual user behavior, threats and the associated traffic patterns. The visibility that ACC data mining provides allows administrators to make more informed policy decisions or respond more quickly to potential security threats.
- **App-Scope:** App-Scope complements the current view of traffic presented by ACC with a dynamic, user-customizable window into network activity that enables administrators to pinpoint problematic or erratic behavior with a view of what has transpired over time.
- **Logging and reporting:** The log viewer enables forensic investigation into every session traversing the network using real-time filtering and regular expressions. Pre-defined, fully customizable and schedulable reports provide detailed views into applications, users, and threats on the network.

Policy-based Controls Enable Appropriate Application Usage

The increased visibility into network activity generated by App-ID, User-ID and Content-ID can help simplify the task of determining which applications are traversing the network, who is using them, the potential security risk and then easily determine the appropriate response. Armed with these data points, administrators use Panorama to apply policies on a single, or multiple device using a range of responses that are more fine-grained than allow or deny. Policy control responses include:

- Allow based on schedule
- Allow but scan
- Apply traffic shaping
- Decrypt and inspect
- Allow certain application functions
- Allow for certain users or groups

Expanding on the response options, experienced firewall administrators can use the intuitive policy-editor to quickly create firewall policies such as:

- Allow Saleforce.com and Oracle for the sales and marketing groups by leveraging Active Directory integration.
- Enable only the IT group to use a fixed set of management applications such as SSH, telnet and RDP.
- Block dangerous or risky applications such as P2P file sharing, circumventors and external proxies.
- Enforce a corporate policy that allows specific webmail and instant messaging usage and inspects for threats.
- Control the file transfer functionality within an individual application, allowing application use yet preventing file transfer.
- Identify the transfer of sensitive information such as credit card numbers or social security numbers.
- Multi-level URL filtering policies that block access to obvious non-work related sites, monitor questionable sites and "coach" access to others.
- Implement QoS policies to allow media and other bandwidth intensive applications but limit their impact on business critical applications.

With Panorama and a network of Palo Alto Networks next-generation firewalls in place, customers can deploy global or local policies to block bad applications, protect the business applications and promote the secure use of end-user applications resulting in a more positive employee environment.

Shared Policies

Panorama enables enterprises to distribute the management of their Palo Alto Networks firewalls using a central oversight with local control model. Central oversight can be achieved by deploying a set of pre- and post-rules to all devices. Local administrators will be able to see these rules, but only a Panorama administrator can modify or remove them. Shared policies enable central 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. Shared policies are complemented by the granular role-based administration capabilities

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 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.

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

Log Management and Reporting

Leveraging the storage available in each device, detailed logs are collected locally, eliminating the requirement for centralized logging. 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.

- **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:** Modify one of the predefined reports or create a custom reports from scratch.
- **Report exporting:** Reports can be exported to CSV or PDF and they 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.
- **User activity reports:** Individual user activity report shows applications used, URL categories visited, web sites visited, and a detailed report of all URLs visited over a specified period of time.

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 is 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	Maximum of 2 Terabytes (TB)
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 later
Browser Support	Internet Explorer 6.0 or later, Firefox 2.0 or later

ORDERING INFORMATION	PART NUMBER
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

paloalto NETWORKS

For additional Information, please visit www.paloaltonetworks.com.