Omicron Seit 1995

paloalto NETWORKS®

PANORAMA

Security deployments are complex and can overload IT teams with complex security rules and mountains of data from multiple sources. Panorama™ network security management empowers you with easy-to-implement, consolidated policy creation and centralized management features. Set up and control firewalls centrally with industry-leading functionality and an efficient rule base, and gain insight into network-wide traffic and threats.

Key Security Features

MANAGEMENT

- Deploy corporate policies centrally to be used in conjunction with regional or functional policies for maximum flexibility
- Delegate appropriate levels of administrative control at the regional level or globally with role-based management
- Group devices into logical, hierarchical device groups for greater management flexibility
- Utilize template stacks for easy device and network configuration
- Easily import existing device configurations into Panorama

VISIBILITY AND SECURITY

- Automatically correlate indicators of threats for improved visibility and confirmation of compromised hosts across your network
- Centrally analyze, investigate and report network traffic, security incidents and administrative modifications
- View a highly customizable graphical summary of applications, users, content and security threats
- Generate actionable, customizable reports to view application and threat traffic, SaaS usage, and user behavior across your configuration

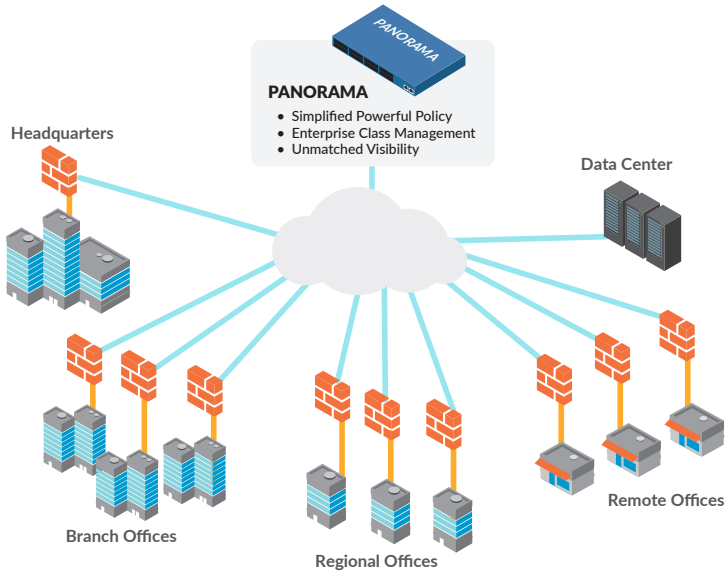

Figure 1: Panorama deployment

Simplified Powerful Policy – Panorama network security management provides static rules in an ever-changing network and threat landscape. Manage your network security with a single security rule base for firewall, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking and data filtering. This crucial simplification, along with dynamic security updates, reduces workload on administrators while improving your overall security posture.

Enterprise Class Management – Panorama keeps the enterprise user in mind. Control your internet and data center edge and your private and public cloud deployments, all from one single console. Panorama can be deployed via virtual appliances, our purpose-built appliances, or a combination of the two. Use appliances as Panorama management units, or as log collectors in hierarchical deployment options. As your network grows, you just need to add the log collectors – we take care of the rest.

Unmatched Automated Visibility and Awareness — Automated threat correlation, with a predefined set of correlation objects, cuts through the clutter of monstrous amounts of data. It identifies compromised hosts and surfaces correlated malicious behavior that would otherwise be buried in the noise of too much information. This reduces the dwell time of critical threats in your network. A clean and fully customizable Application Command Center provides comprehensive insight into current and historical network and threat data.

Figure 1: ACC

Powerful Network Visibility: Application Command Center

Using Application Command Center from Panorama provides you with a highly interactive, graphical view of application, URL, threat and data (files and patterns) traversing your Palo Alto Networks® firewalls. ACC includes a tabbed view of network activity, threat activity, and blocked activity, and each tab includes pertinent widgets for better visualization of traffic patterns on your network. Custom tabs can be created, which include widgets that enable you to drill down into the information that is most important to the administrator. ACC provides a comprehensive, fully customizable view of not only current but also historical data.

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

Reduced Response Times: Automated Correlation Engine

The automated correlation engine built into the next-generation firewall surfaces critical threats that may be hidden in your network. It includes correlation objects that are defined by the Palo Alto Networks threat research team. These objects identify suspicious traffic patterns or a sequence of events that indicates a malicious outcome. Some correlation objects can identify dynamic patterns that have been observed from malware samples in WildFire™ cloud-based threat analysis service.

Simple Policy Control: Safely Enable Applications

Safely enabling applications means allowing access to specific applications and protecting them with specific threat prevention, QoS and file, data or URL filtering policies. Panorama empowers you to set policy with a single security rule base, and simplifies the process of importing, duplicating or modifying rules across your network. The combination of global and regional administrative control over policies and objects lets you strike a balance between consistent security at the global level and flexibility at the regional level.

Enterprise Class Management

Deploying hierarchical device groups ensures that lower-level groups inherit the settings of higher-level groups. This streamlines central management and enables you to organize devices based on function and location without redundant configuration. Template stacking allows for streamlined configuration of networks and devices. Furthermore, a common user interface for both next-generation firewalls and management makes management intuitive. Features such as Global Find and tag-based rule grouping empower your IT administrators to take advantage of all the information in your network with ease.

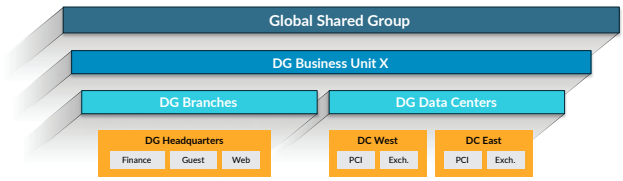

Figure 2: Device Group Hierarchy

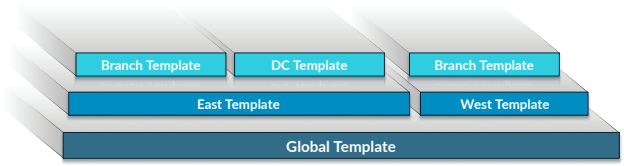

Figure 3: Template Stacking

Traffic Monitoring: Analysis, Reporting and Forensics

Panorama pulls in logs from firewalls, both physical as well as virtual, and from Traps™ advanced endpoint protection and stores them in its own log storage. As you perform log queries and generate reports, Panorama dynamically pulls the relevant logs from its log storage and presents the result to the user.

- **Log viewer:** For an individual device, all devices or Traps, you 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:** A user activity report shows the applications used, URL categories visited, websites visited, and all URLs visited over a specified period of time for individual users. Panorama builds the reports using an aggregate view of users' activity, no matter which firewall they are protected by, or which IP or device they may be using.
- **SaaS reports:** A SaaS usage and threat report provides detailed visibility into all SaaS activity on the firewalls, and related threats.
- **Log forwarding:** Panorama can forward logs collected from all of your Palo Alto Networks firewalls and Traps to remote destinations for purposes such as long-term storage, forensics or compliance reporting. Panorama can forward all or selected logs, SNMP traps, and email notifications to a remote logging destination, such as a syslog server (over UDP, TCP or SSL). Additionally, Panorama can kick off a workflow and send logs to a third-party service that provides an HTTP-based API, for example, a ticketing service or a systems management product.

Panorama Management Architecture

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

- **Templates/Template stacks:** Panorama manages common device and network configuration through templates. Templates can be used to manage configuration centrally and then push the changes to managed firewalls. This approach avoids making the same individual firewall change repeatedly across many devices. To make things even easier, templates can be stacked and used like building blocks during device and network configuration.
- **Hierarchical device groups:** Panorama manages common policies and objects through hierarchical device groups. Multi-level device groups are used to centrally manage the policies across all deployment locations with common requirements. Device group hierarchy may be created geographically (e.g., Europe, North America and Asia), functionally (e.g. data center, main campus and branch offices), a mix of both, or other criteria. This allows for common policy sharing across different virtual systems on a device.

You can use shared policies for global control while still providing your regional firewall administrators with the autonomy to make specific adjustments for their requirements. At the device group level, you 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 they can only be edited from Panorama within the context of the administrative roles that have been defined. The device rules (those between pre- and post-rules) can be edited by either your regional firewall administrator or a Panorama administrator who has switched to a firewall device context. In addition, an organization can use shared objects defined by a Panorama administrator, which can be referenced by regionally managed device rules.

- **Role-based administration:** Role-based administration is used to delegate feature-level administrative access, including the availability of data (enabled, read-only, or disabled and hidden from view) to different members of your staff.

Specific individuals can be given appropriate access to the tasks that are pertinent to their job while making other access either hidden or read-only. Administrators can commit and revert changes that they made in a Panorama configuration independently of changes made by other administrators.

Software, Content and License-Update Management: As your deployment grows in size, you may 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 is 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.

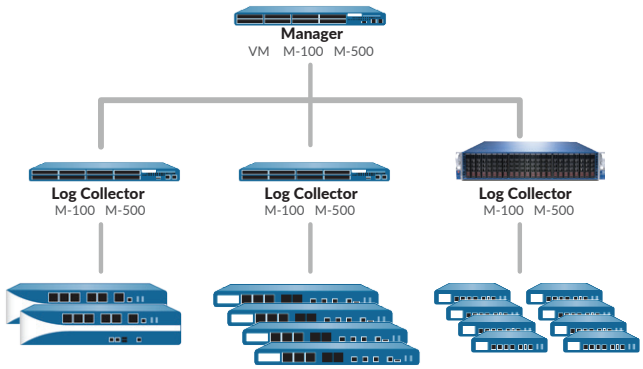

Figure 3: Panorama Architecture

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

Deployment Flexibility

Organizations can deploy Panorama either with hardware appliances or as virtual appliances.

Hardware Appliances

Panorama can be deployed on the M-100 or the M-500 management appliances, and individual management and logging components can be separated in a distributed manner to accommodate large volumes of log data. Panorama, running on these appliances, 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:** You can separate the management and logging functions across multiple devices, splitting the functions 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; instead it 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 you to optimize your Panorama deployment in order to meet scalability, organizational or geographical requirements.

Virtual Appliance

Panorama can also be deployed as a virtual appliance on VMware® ESXi™, allowing organizations to support their virtualization initiatives and consolidate rack space, which is sometimes limited or costly in a data center.

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. It can be deployed in two ways:

- **Centralized:** All Panorama management and logging functions are consolidated into a single virtual appliance (with the option for high availability).
- **Distributed:** Panorama distributed log collection requires a mix of the hardware and virtual appliance.

Note: The virtual appliance may not be used as a Panorama log collector. Panorama log collectors (M-100 or M-500 appliances) are responsible for offloading intensive log collection and processing tasks.

Providing the choice of either a hardware or virtualized appliance, as well as the choice to combine or separate the Panorama functions, provides you 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
Management Tools and APIs
• Graphical User Interface (GUI) • Command Line Interface (CLI) • XML-based REST API

Virtual Appliance Specifications
Minimum Server Requirements
• 81 GB hard drive • 8 CPU cores • 16 GB RAM
VMware Support
• VMware ESX 3.5, 4.0, 4.1, 5.5, 6.5
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: 24 TB maximum

M-100 Panorama Appliance

M-500 Panorama Appliance

M-100 Appliance
I/O
• (4) 10/100/1000, [1] DB9 console serial port, (1) USB
Storage
• Maximum configuration: RAID: 8 x 2 TB RAID Certified HDD for 8 TB of RAID storage
Power Supply/Max Power Consumption
• 500W/500W
Max BTU/hr
• 1,705 BTU/hr
Input Voltage (Input Frequency)
• 100-240 VAC (50-60Hz)
Max Current Consumption
• 10A @ 100 VAC
Mean Time Between Failures (MTBF)
• 14.5 years
Rack Mountable (Dimensions)
• 1U, 19" standard rack (1.75"H x 23"D x 17.2"W)
Weight
• 26.7 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

M-500 Appliance
I/O
• (4) 10/100/1000, (1) DB9 console serial port, (1) USB port, (2) 10 GigE ports
Storage
• Maximum configuration: RAID: 24 x 2 TB RAID Certified HDD for 24 TB of RAID storage • Default Shipping Configuration: 4 TB: 8 x 1TB RAID Certified HDD for 4 TB of RAID storage
Power Supply/Max Power Consumption
• Dual power supplies, hot swap redundant configuration • 1200W/493W (total system)
Max BTU/hr
• 1,681 BTU/hr
Input Voltage (Input Frequency)
• 100-240 VAC (50-60 Hz)
Max Current Consumption
• 4.2A @ 120 VAC
Mean Time Between Failures (MTBF)
• 6 years
Rack Mountable (Dimensions)
• 2 U, 19" standard rack (3.5"H x 21"D x 17.5"W)
Weight
• 42.5 lbs.
Safety
• UL, CUL, CB
EMI
• FCC Class A, CE Class A, VCCI Class A
Environment
• Operating Temperature 50° to 95° F, 10° to 35° C • Non-operating Temperature -40° to 158° F, -40° to 65° C

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

panorama-ds-020817

Omicron AG
Industriestrasse 50b
8304 Wallisellen
+41 44 839 11 11