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.
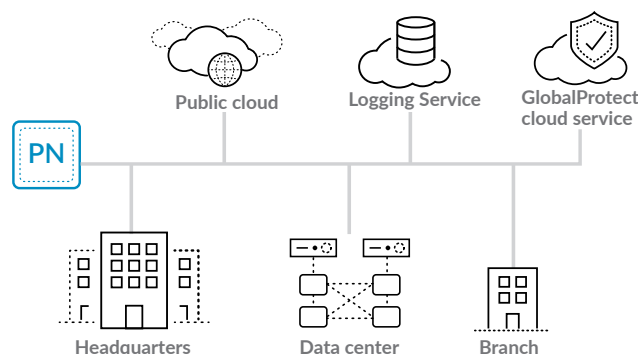

Figure 1: Panorama deployment

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 a 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.
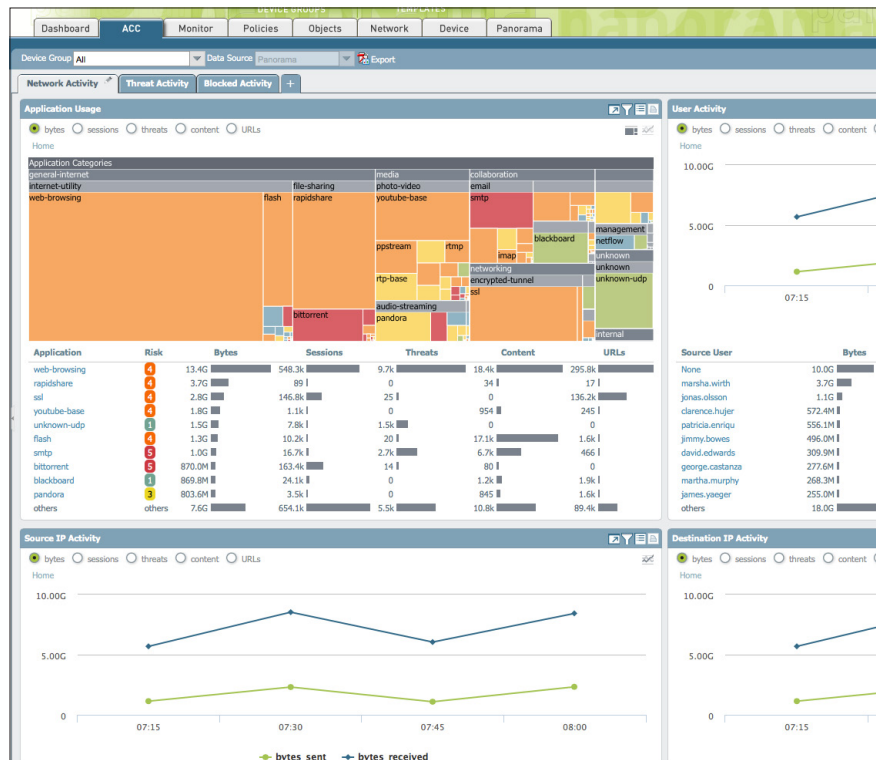
Figure 2: Application Command Center

Powerful Network Visibility: Application Command Center

Using Application Command Center from Panorama provides you with a highly interactive, graphical view of applications, URLs, threats, and data files and patterns traversing your Palo Alto Networks® firewalls. The 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. The ACC provides a comprehensive, fully customizable view of both current and historical data.

Additional data on URL categories and threats provides a complete and well-rounded picture of network activity. The visibility from the 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® malware prevention service.

Simple Policy Control: Safely Enable Applications

Safely enabling applications means allowing access to specific applications and protecting them with specific policies for threat prevention and QoS as well as file, data or URL filtering. 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 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.

Traffic Monitoring: Analysis, Reporting and Forensics

Panorama pulls in logs from firewalls, both physical and virtualized, 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 results to the user.

Figure 3: Device group hierarchy

Figure 4: Template stacking

- **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 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 Traps and all your Palo Alto Networks firewalls 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, such as 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), as a mix of both or based on 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 and the last set of rules – the pre-rules and post-rules, respectively – 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, that is, 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 pertinent to their job while making other access either hidden or read-only. Administrators can commit and revert changes they made in a Panorama configuration independently of changes made by other administrators.
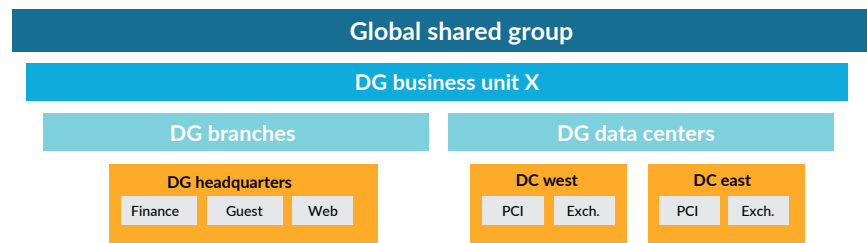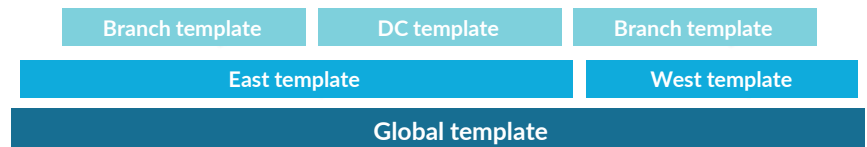
Software, Content and License-Update Management

As your deployment grows in size, you may want to make sure 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.

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 global as well as regional levels.

Deployment Flexibility

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

Hardware Appliances

Panorama can be deployed as the M-100, M-200, M-500 or M-600 management appliance.

Virtual Appliances

Panorama can be deployed as a virtual appliance on VMware® ESXi™ or in public cloud environments, including Amazon® Web Services, or AWS®, and Microsoft® Azure®.
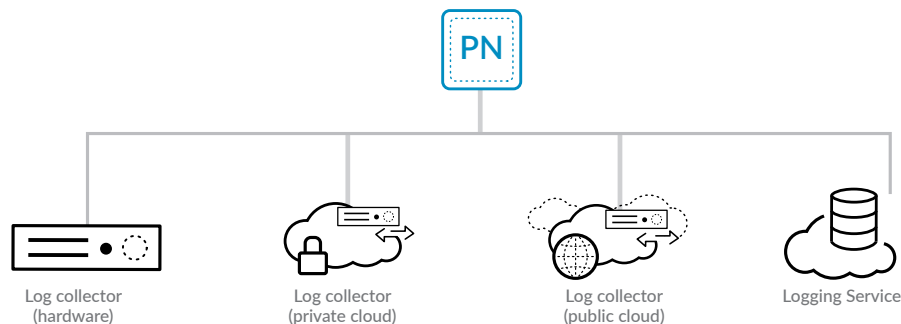

Log collector (hardware)　　Log collector (private cloud)　　Log collector (public cloud)　　Logging Service

Figure 5: Panorama log management

Deployment Modes

You can separate management and logging functions of Panorama using deployment modes. The three supported deployment modes are:

1. **Panorama:** Panorama controls both policy and log management functions for all managed devices.
2. **Management Only:** Panorama manages configurations for the managed devices but does not collect or manage logs.
3. **Log Collector;** Panorama collects and manages logs from managed devices. This assumes another deployment of Panorama is operating in Management Only mode.

The separation of management and log collection enables the Panorama deployment to meet scalability, organizational and geographic requirements. The choice of form factor and deployment mode gives you the maximum flexibility for managing Palo Alto Networks next-generation firewalls in a distributed network.

Deployment Scale

The Panorama Interconnect plugin connects multiple Panorama instances to scale firewall management to tens of thousands of firewalls. By leveraging the plugin, the Panorama Controller allows you to synchronize the configuration, quickly onboard firewalls, and schedule content updates from a central location (see Figure 6). This lets you simplify management by centrally defining security policies and distributing them across all your firewalls regardless of their location – on-premises or in the cloud.

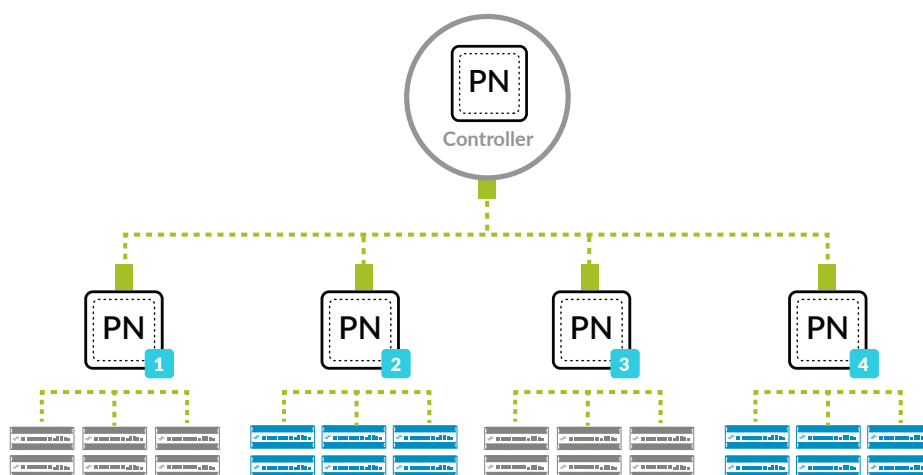*Note: Panorama Interconnect is supported only on Panorama M-600 appliances or similarly resourced VMs.*

Figure 6: Synchronized configuration across all firewalls

Panorama Specifications

Number of Devices Supported
- Up to 1,000

High Availability
- Active/Passive

Administrator Authentication
- Local database
- RADIUS
- SAML
- LDAP
- TACACS+

Management Tools and APIs
- Graphical User Interface (GUI)
- Command Line Interface (CLI)
- XML-based REST API

Public Clouds Supported

Amazon AWS

Microsoft Azure

Private Hypervisor Specifications

	Management Only Mode	Panorama Mode	Log Collector Mode
Cores Supported	4 CPUs	8 CPUs	16 CPUs
Memory (minimum)	8GB	32GB	32GB
Disk Drive	81GB system disk	2TB to 24TB log storage	2TB to 24TB log storage

Public Cloud Instance Types (BYOL License)

	Management Only Mode	Panorama Mode	Log Collector Mode
Amazon AWS	t2.xlarge m4.2xlarge	m4.2xlarge m4.4xlarge	m4.4xlarge c4.8xlarge
Microsoft Azure	D4_V3 Standard D4S_V3 Standard	D16_V3 Standard	D16_V3 Standard D32_V3 Exceeds

M-200 Panorama Appliance

M-200 Appliance

I/O
- (4) 10/100/1000, [1] DB9 console serial port, (1) USB port

Storage
- Maximum configuration: 4 x 8TB RAID Certified HDD for 16TB of RAID storage
- Default shipping configuration: 4 x 8TB RAID Certified HDD for 16TB of RAID storage

Power Supply/Max Power Consumption
- Dual power supplies, hot swap redundant configuration
- 750W/300W

Max BTU/hr
- 1,114 BTU/hr

Input Voltage (Input Frequency)
- 100–240 VAC (50–60Hz)

Max Current Consumption
- 9.5A @ 110 VAC

Mean Time Between Failures (MTBF)
- 10 years

Rack Mount (Dimensions)
- 1U, 19" standard rack (1.7" H x 29" D x 17.2" W)

Weight
- 26 lbs

Safety
- UL, CUL, CB

EMI
- FCC Part 15, EN 55032, CISPR 32

Environment
- Operating temperature: 41° to 104° F, 5° to 40° C
- Non-operating temperature: -40° to 140° F, -40° to 60° C

M-600 Panorama Appliance

M-600 Appliance

I/O
- (4) 10/100/1000, (1) DB9 console serial port, (1) USB port, (2) 10 GigE ports

Storage
- Maximum configuration: 12 x 8TB RAID Certified HDD for 48TB of RAID storage
- Default shipping configuration: 4 x 8TB RAID Certified HDD for 16TB of RAID storage

Power Supply/Max Power Consumption
- Dual power supplies, hot swap redundant configuration
- 750W/486W (total system)

Max BTU/hr
- 1,803 BTU/hr

Input Voltage (Input Frequency)
- 100–240 VAC (50–60 Hz)

Max Current Consumption
- 4.5A @ 220 VAC

Mean Time Between Failures (MTBF)
- 8 years

Rack Mount (Dimensions)
- 2U, 19" standard rack (3.5" H x 28.46" D x 17.2" W)

Weight
- 36 lbs

Safety
- UL, CUL, CB

EMI
- FCC Part 15, EN 55032, CISPR 32

Environment
- Operating temperature: 41° to 104° F, 5° to 40° C
- Non-operating temperature: -40° to 140° F, -40° to 60° C

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: 8 x 2TB RAID Certified HDD for 8TB of RAID storage
- Default shipping configuration: 2 x 1TB RAID Certified HDD for 1TB 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 Mount (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: 24 x 2TB RAID Certified HDD for 24TB of RAID storage
- Default shipping configuration: 4 x 2TB RAID Certified HDD for 4TB 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 (50–60Hz)

Max Current Consumption
- 4.2A @ 120 VAC

Mean Time Between Failures (MTBF)
- 6 years

Rack Mount (Dimensions)
- 2U, 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