Panorama

Security deployments can be complex, overloading IT teams with myriad 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. You can provision firewalls centrally and use industry-leading functionality to create effective security rules as well as gain insight into network traffic and threats.

Key Features

Management

- Device groups, hierarchies, and tags for organizing policies
- Template stacks for reusable network configuration
- Administrator-specific commits to avoid accidental changes
- Easy software updates and upgrades
- SD-WAN connectivity for branch offices

Visibility

- Centralized visibility across the infrastructure
- Correlated insights that can be acted upon
- Health profiling for improved understanding of device usage

Security

- Easy transformation of legacy rules into application-based rules using intelligence gathered by PAN-OS®
- Rule usage analysis to reduce the attack surface and improve security posture
- Centralized deployment of the latest security content updates

Automation

- Log filtering and automated actions on third-party systems
- Automated policy deployments for dynamic environments
- XML- and JSON-based REST APIs for easy integration

Simplified, Powerful Policy

Panorama network security management provides consistent 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, access control, and data filtering. This crucial simplification, along with App-ID™ technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

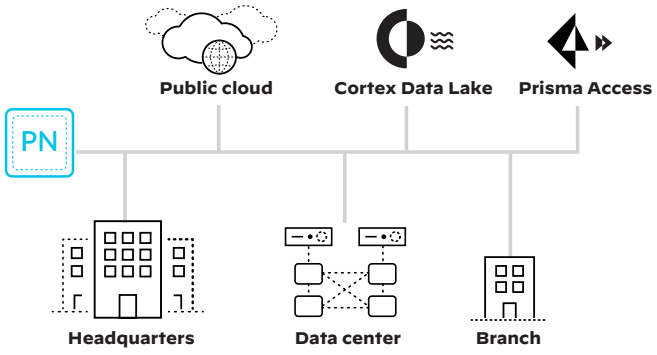

Figure 1: Panorama deployment

Enterprise-Class Management

Panorama keeps enterprise users in mind. You can control your internet edge as well as 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.

Automated, Centralized Visibility

Automated threat correlation, with a predefined set of correlation objects, cuts through the clutter of monstrous amounts of data. It identifies compromised hosts and correlates malicious behavior that would otherwise be lost in the noise. This reduces the dwell time of critical threats in your network. The clean, fully customizable Application Command Center (ACC) provides comprehensive insight into your current as well as historical network and threat data.

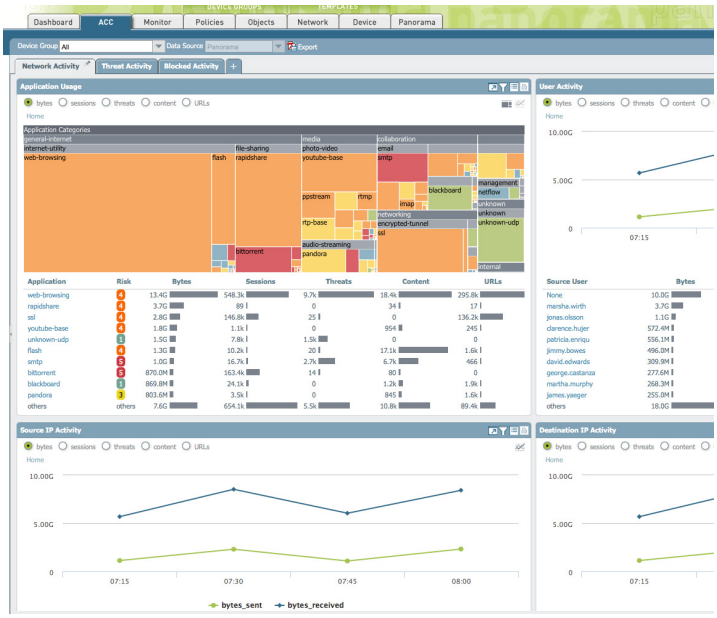

Figure 2: Application Command Center

Unmatched Scale

Use a single highly available pair of Panorama appliances to manage up to 5,000 Next-Generation Firewalls, or use the Panorama Interconnect plugin to centralize configuration management and access control for tens of thousands of devices.

Powerful Network Visibility

The ACC provides you an interactive, graphical view of applications, URLs, threats, 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. You can create custom tabs with widgets that enable you to drill down into the information

most important to the administrator. The ACC provides a comprehensive, fully customizable view of current and historical data.

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

Reduced Response Times

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 identify suspicious traffic patterns or sequences of events that indicate malicious outcomes. Some correlation objects can identify dynamic patterns previously observed from malware samples in WildFire® malware prevention service.

Simple Policy Control

Safely enabling applications means allowing access to specific applications and protecting them with specific policies for Threat Prevention and access control as well as file, data, and URL filtering. You can transform your bulky legacy rule base into an intuitive policy that strengthens security and takes much less time to manage. 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.

Easy-to-Use, Centralized 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 Next-Generation Firewalls makes management intuitive. Features like Global Find, audit comments, universal unique identifier (UUID) for all rules, and tag-based rule grouping empower your IT administrators to take advantage of all the information in your network with ease.

Enhanced Visibility and Troubleshooting for Mobile Workers

GlobalProtect™ network security for endpoints extends Next-Generation Firewall capabilities to mobile workers. By leveraging Panorama, you can get greater visibility into user connection failures at all stages, use authentication logs to help you troubleshoot issues with user accounts, and enforce access control based on specific data in GlobalProtect logs.

Traffic Monitoring: Analysis, Reporting, and Forensics

Panorama pulls and stores logs from physical and virtualized firewalls, Cortex™ Data Lake, and Cortex XDR agents. As you perform log queries and generate reports, Panorama dynamically pulls relevant logs from its storage and presents the results to the user:

- **Log viewer:** For individual devices, all devices, or Cortex XDR agents, you can quickly view log activities with dynamic log filtering by clicking on a cell value and/or using the expression builder to define sort criteria. You can also save results for future queries or export them 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:** These reports show the applications used, URL categories visited, websites visited, and all URLs visited over a specified period for individual users. Panorama builds these reports using an aggregate view of user activity, no matter the user's device or IP, and no matter which firewall is protecting a given user.
- **SaaS reports:** A software-as-a-service (SaaS) usage and threat report provides detailed visibility into all SaaS activity on the firewalls as well as related threats.
- **Log forwarding:** Panorama can forward logs from Cortex XDR agents and your Palo Alto Networks firewalls for storage, forensics, reporting, etc. It can forward all or selected logs, SNMP traps, and email notifications to a remote destination over UDP, TCP, or SSL. Panorama can also send logs to third-party providers of HTTP-based APIs, such as ticketing services or systems management products.

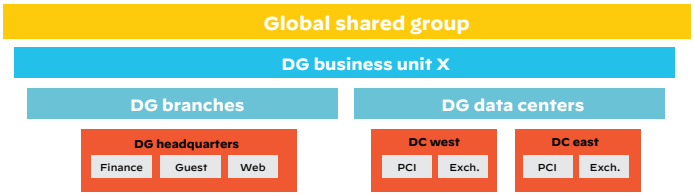

Figure 3: Device group hierarchy

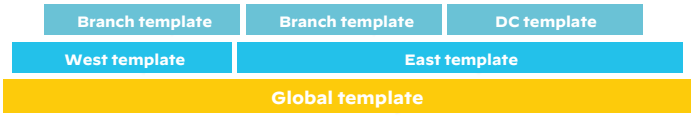

Figure 4: Template stacking

Panorama Management Architecture

Panorama enables you to manage your Palo Alto Networks firewalls using a model that provides both global oversight and regional control. Panorama provides multiple tools for global or centralized administration.

Templates/Template Stacks

Panorama manages common device and network configuration through templates, which can be used to manage configuration centrally and push changes to managed firewalls. This approach avoids the need to make the same individual firewall changes 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. Multilevel 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 allowing your regional firewall administrators 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.

You can give specific individuals appropriate access to the tasks pertinent to their job while making other access either hidden or read-only. Administrators can commit or revert changes they make in a Panorama configuration independently of changes made by other administrators.

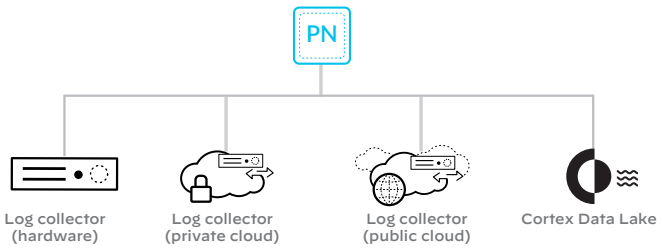

Figure 5: Panorama log management

Software, License Update, and Content Management

As your deployment grows, 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. Panorama lets you centrally manage the update process for software updates, licenses, and content—including application updates, antivirus signatures, threat signatures, URL Filtering database entries, etc.

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-200, M-500, or M-600 management appliance.

Virtual Appliances

Panorama can be deployed as a virtual appliance on VMware ESXi™, KVM, and Microsoft Hyper-V®, or in public cloud environments, including Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure®, and Azure GovCloud.

Deployment Modes

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

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

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), in turn simplifying management of all your firewalls regardless of their location—on-premises or in the cloud.

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

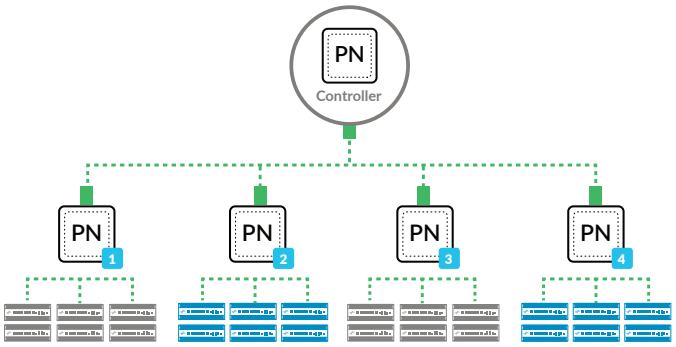

Figure 6: Synchronized configuration across all firewalls

Table 1: Panorama Appliance Hardware Specifications

	M-200	M-500	M-600
I/O	10/100/1000 (4), DB9 console serial port (1), USB port (1)	10/100/1000 (4), DB9 console serial port (1), USB port (1), 10 GigE ports (2)	10/100/1000 (4), DB9 console serial port (1), USB port (1), 10 GigE ports (2)
Storage	Maximum configuration: 8 TB RAID Certified HDD (4) for 16 TB of RAID storage Default shipping configuration: 8 TB RAID Certified HDD (4) for 16 TB of RAID storage	Maximum configuration: 2 TB RAID Certified HDD (24) for 24 TB of RAID storage Default shipping configuration: 2 TB RAID Certified HDD (4) for 4 TB of RAID storage	Maximum configuration: 8 TB RAID Certified HDD (12) for 48 TB of RAID storage Default shipping configuration: 8 TB RAID Certified HDD (4) for 16 TB of RAID storage
Power Supply/ Max Power Consumption	Dual power supplies, hot swap redundant configuration 750 W / 300 W	Dual power supplies, hot swap redundant configuration 1,200 W / 493 W (total system)	Dual power supplies, hot swap redundant configuration 750 W / 486 W (total system)
Max BTU/hr	1,114 BTU/hr	1,681 BTU/hr	1,803 BTU/hr
Input Voltage (Input Frequency)	100–240 VAC (50–60 Hz)	100–240 VAC (50–60 Hz)	100–240 VAC (50–60 Hz)
Max Current Consumption	9.5 A @ 110 VAC	4.2 A @ 120 VAC	4.5 A @ 220 VAC
Mean Time Between Failures (MTBF)	10 years	6 years	8 years
Rack Mount (Dimensions)	1U, 19” standard rack (1.7” H x 29” D x 17.2” W)	2U, 19” standard rack (3.5” H x 21” D x 17.5” W)	2U, 19” standard rack (3.5” H x 28.46” D x 17.2” W)
Weight	26 lbs	42.5 lbs	36 lbs
Safety	UL, CUL, CB	UL, CUL, CB	UL, CUL, CB
EMI	FCC Part 15, EN 55032, CISPR 32	FCC Class A, CE Class A, VCCI Class A	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	Operating temperature: 50° to 95° F, 10° to 35° C Non-operating temperature: -40° to 158° F, -40° to 65° C	Operating temperature: 41° to 104° F, 5° to 40° C Non-operating temperature: -40° to 140° F, -40° to 60° C

Table 2: Other Panorama Specs
Number of Devices Supported
• Up to 5,000
High Availability
• Active/Passive
Administrator Authentication
• Local database • RADIUS • SAML • LDAP • TACACS+
Management Tools and APIs
• Graphical user interface • Command-line interface • XML- and JSON-based REST API

Table 3: Private Hypervisor Specifications			
	Management Only Mode	**Panorama Mode**	**Log Collector Mode**
Cores Supported	4 CPUs	8 CPUs	16 CPUs
Memory (minimum)	8 GB	32 GB	32 GB
Disk Drive	81 GB system disk	2 TB to 24 TB log storage	2 TB to 24 TB log storage

Table 4: Public Clouds Supported
GCP, AWS, AWS GovCloud, Azure, Azure GovCloud

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com