



PA-4000 Series Feature Overview

September, 2007

Palo Alto Networks
2130 Gold Street, Suite 200
Alviso, CA 95002-2130
Main 408.786.0001
Fax 408.786.0006
Sales 866.207.0077
www.paloaltonetworks.com

Table of Contents

Introduction.....	3
A Fresh Approach to Network Security	3
Palo Alto Networks PA-4000 Series.....	4
Application Identification	4
Application Command Center and App-Scope.....	5
User Visibility	7
Policy and Configuration Control	7
FlashMatch Real-Time Threat Prevention.....	8
Networking.....	9
Deployment Options.....	10
High Availability (HA)	10
Management Flexibility	10
Logging and Reporting	11
Device Updates	11
Purpose-Built Platform.....	11
Conclusion.....	12

Introduction

IT administrators today are faced with an application landscape that has evolved in a dramatic fashion. End-user applications that are being installed on the network have been designed specifically to act evasively, avoiding network detection and associated security. Even well-meaning corporate applications utilize similar tactics to accelerate deployment, facilitate wide spread access and minimize disruption.

IT administrators know that there are applications on their network that their network security infrastructure cannot identify, and that without application visibility it is not possible to effectively control traffic on the network. The ramifications resulting from this inability to identify and control the applications traversing the network range from benign to serious. End-user productivity, bandwidth consumption, PC performance degradation due to non-work related processing are just a few of the relatively benign ramifications that administrators face. The more threatening ramifications include regulatory compliance, information leakage, and hackers looking for financial gain through the theft of personal information, passwords and corporate information.

IT administrators are managing as best they can with a patchwork of existing technologies. Conventional approaches to the application visibility and control dilemma include point solution bolt-ons added to an existing technology or deploying a myriad of point solutions that look at only a small portion of the problem; but these approaches simply can't keep pace with today's nimble, network-savvy applications. What's needed is a fresh approach to the firewall, one that takes an application-centric approach to traffic classification and is capable of bringing policy-based application control back to the network security team.

A Fresh Approach to Network Security

In order to keep pace with the evolving application landscape, administrators are coming to the stark realization that only a fresh approach will enable them to accurately identify and therefore control all application traffic flowing in and out of the network. Palo Alto Networks is taking a new approach to build a solution for today's network security needs:

- The solution starts with network traffic classification that identifies the actual application irrespective of port, protocol, or evasive tactic. All traffic on all ports is classified in this way, providing application identification as a comprehensive visibility foundation for all security functions to leverage.
- Policy-based decryption, identification and control of SSL traffic provides visibility into one of the largest blind spots on the network today. The policy controls enable gradual introduction of SSL decryption as well as granular enforcement of corporate policy.
- Graphical visualization and policy control of application usage. Simple and intuitive visualization tools provide visibility into the traffic currently on the network, helping to set appropriate application use policy. Application policy control includes allowing, blocking, controlling file transfers, marking for QoS, and inspecting traffic for viruses, spyware, and vulnerability exploits.
- Real-time protection from threats embedded in applications allows network-based threat prevention without impact to user experience. Rather than using multiple threat prevention devices that often proxy file transfers to look for viruses and spyware, Palo Alto Networks utilizes a single, hardware accelerated prevention engine supported by a common signature format to detect a wide range of malware and threats.
- Rounding out this fresh approach is a purpose-built high speed platform that makes it possible to provide visibility and control for all applications on all ports. The platform

utilizes different processing technologies, applied to specific functions, complemented by large amounts of RAM to maintain multi-gigabit throughput and low latency even under load with all functions turned on.

Palo Alto Networks PA-4000 Series

Palo Alto Networks is taking a fresh approach to deliver a next-generation firewall that classifies traffic from an application-centric perspective, thereby enabling organizations to accurately identify and control applications flowing in and out of the network. The Palo Alto Networks PA-4000 Series brings new levels of application visibility, control and protection to the enterprise firewall market. Based upon a new traffic classification technology called App-ID™, the PA-4000 Series can accurately identify which applications are flowing across the network, irrespective of protocol, port, SSL encryption or evasive tactic employed. Armed with this in-depth knowledge, security administrators can regain control of their networks at the gateway to achieve the following business benefits:

- Mitigate risk through policy-based application usage control and threat detection
- Enable growth by embracing web-based applications in a controlled and secure manner
- Facilitate efficiency by minimizing the amount of manpower associated with monitoring desktops and removing unwanted applications

The PA-4000 Series is a purpose-built, high performance platform with dedicated processing for management, traffic classification and threat mitigation, allowing it to meet the performance demands of protecting a high speed network. The result is a solution that can help mitigate today's emerging security risks through tighter control of the application traffic traversing the network.

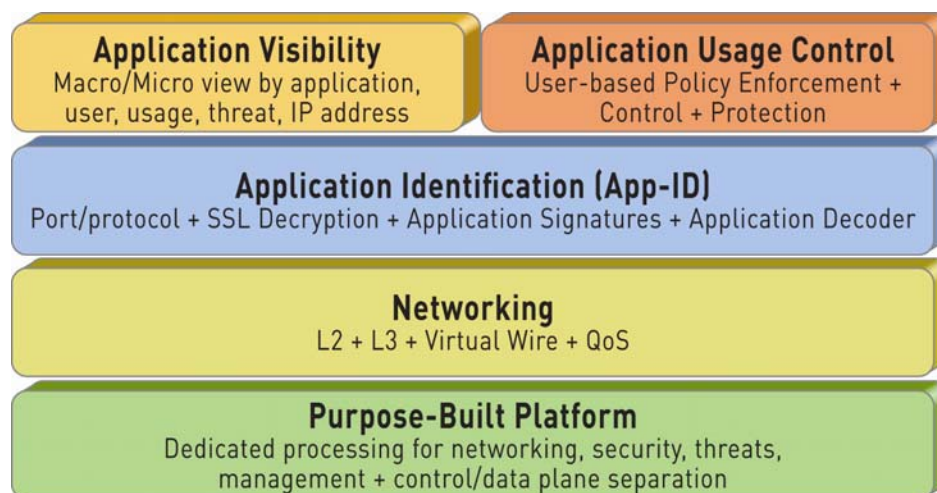


Figure 1: The PA-4000 Series architecture combines a purpose-built platform, a rich networking foundation and a security-specific OS to deliver application visibility control.

Application Identification

At the heart of the PA-4000 Series is an application-centric classification technology called App-ID. Unlike traditional security approaches that rely solely on protocol and port, App-ID is an industry first, using up to four traffic classification techniques to analyze the actual session data and identify the application—even those applications that use random ports, tunnel inside and emulate other applications, or use SSL encryption. With the resultant

visibility into the actual identity of the application, customers can deploy policy-based application usage control for both inbound and outbound network traffic. The four traffic classification mechanisms in App-ID are:

- Application signatures: application context-aware pattern matching designed to look for the unique properties and information exchanges of applications to correctly identify them, regardless of the protocol and port being used.
- Application decoding: a powerful engine that continuously decodes application traffic to identify the more evasive applications as well as create the foundation for accurate threat prevention.
- SSL decryption: decrypts outbound SSL traffic using a forward SSL proxy to identify and control the traffic inside before re-encrypting it to its destination.
- Protocol/port: helps narrow the application identification process, but is primarily used to control which ports applications are allowed to use.

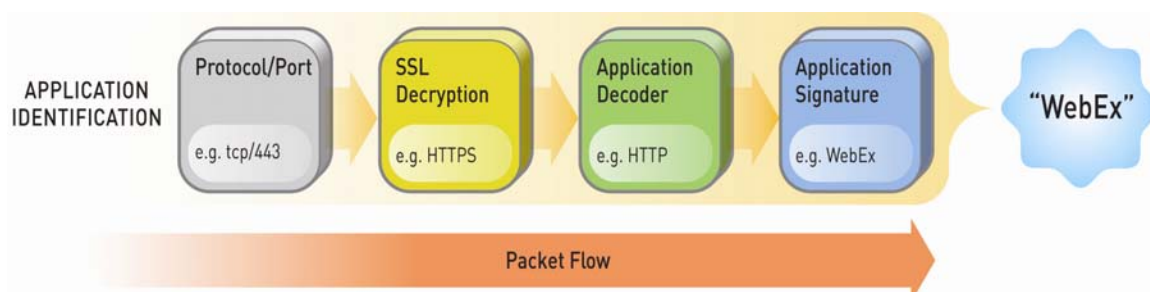


Figure 2: App-ID uses four traffic classification techniques to accurately identify the application, irrespective of port or protocol.

The application-centric nature of App-ID means that it can not only identify and control traditional applications like HTTP, FTP, SNMP, but it can also accurately delineate specific instances of IM (AIM, Yahoo!IM, Meebo, etc), Webmail (Yahoo!Mail, gmail, Hotmail, etc), peer2peer (Bittorrent, emule, Neonet, etc), and other applications commonly found on enterprise networks. Once the application is identified and decoded using App-ID, the traffic can be more tightly controlled through security policies.

Application Command Center and App-Scope

The application visibility that App-ID generates is harnessed by Application Command Center and App-Scope, two powerful visualization tools that present application data in a straightforward, easy to understand manner, using the application names and traditional network security terminology.

- **Application Command Center (ACC):** a visual display of current application traffic flowing across the network. ACC is a simple to use component of the web interface that summarizes current application activity, presenting the data to administrators in a straightforward, easy to understand manner using the application names, categorized by sessions, bytes, threats, source/destination IP addresses, and time. With a click of the mouse, additional information on the application can be viewed as well as usage level, source/destination and threats. A click of the mouse enables visibility into application details such as:
 - Commonly used ports, evasive characteristics, propensity to transmit malware, and risk level.
 - Top threats carried by the application and security rules in use.

- Heaviest users on IP address and their user identity within Active Directory.
- Most common source/destination countries.

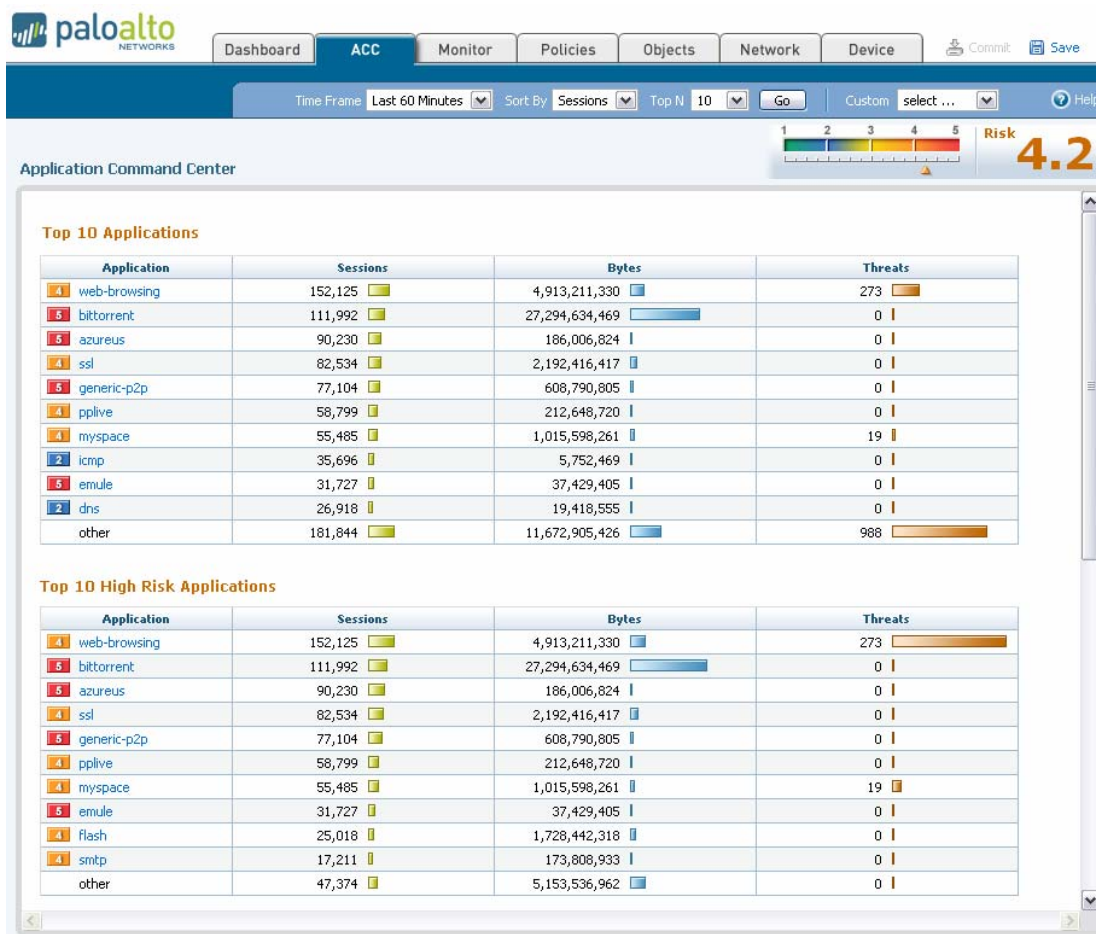


Figure 5: Application Command Center gives administrators a clear, easy-to-understand summary of the application traffic traversing the network.

- **App-Scope:** App-Scope is a set of visualization tools that provides a comparative view of application activity (now vs a past timeframe), that helps IT pinpoint problematic behavior by answering some very common questions:
 - How has application usage and user activity changed on my network?
 - Which users and apps are consuming my bandwidth?
 - Which threats are consistently on my network?

Whereas ACC gives IT a view into current network activity, App-Scope provides a dynamic, user-customizable window into network activity, presenting the information in a comparative manner enabling visibility into unusual or unexpected behavior.

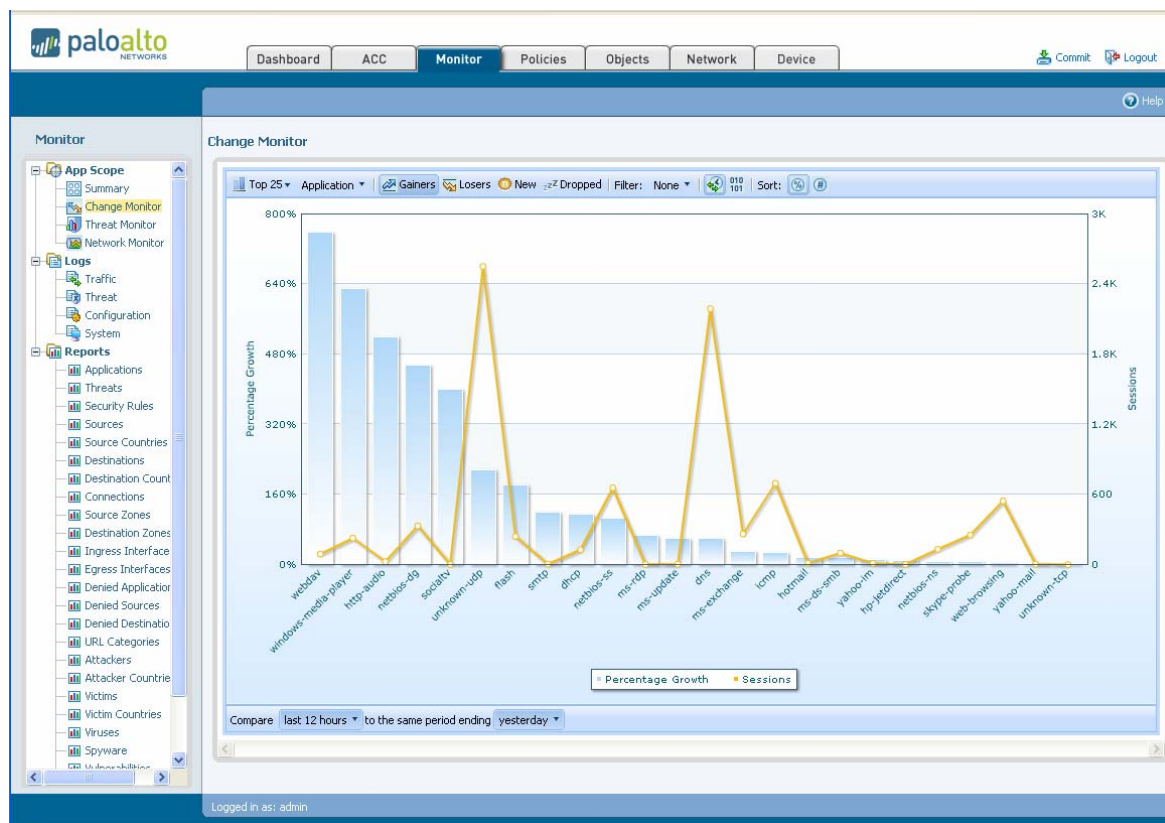


Figure 6: App-Scope shows how traffic has changed by comparing two user defined time-frames.

User Visibility

Through transparent integration with Microsoft's Active Directory (AD), both ACC and App-Scope will display who is using the application based on their identity from Active Directory, as well as their IP address. Positive identification of which actual user is using specific applications is key to providing visibility into application usage on the network and subsequently being able to create an appropriate security policy that is based on actual users and user groups. In addition to being displayed in ACC and App-Scope, user identity is also accessible as part of the policy editor, logging and reporting giving administrators a consistent view of network activity.

Policy and Configuration Control

With increased visibility comes the ability to deploy policies for more granular control over traffic traversing the network. ACC allows a security team to analyze the data collected and make informed, security policy decisions which can then be implemented using the intuitive management interface. From the familiar rule-based editor, an application usage control policy can be created, reviewed and deployed. Administrators can pick and choose from over 450 applications, dynamically updated and listed by their commonly used names. Alternatively, application control can be implemented based on the 16 different application categories, which are dynamically updated as new applications are added the Palo Alto Networks update service. Additional usage control criteria includes:

- By user identity and/or groups via seamless integration with Active Directory.

- By source and destination IP address, source and destination security zones, and time-based schedules.
- Application type or specific application: use application categories to define policy (such as all peer2peer), or select from over 450 applications that are dynamically updated, including traditional enterprise, networking and Internet applications.
- Protocol and port number: restrict and/or enforce applications to use default or specific protocols and port numbers.
- File blocking: block file transfer capabilities within an application as well as block application transfers by file type.

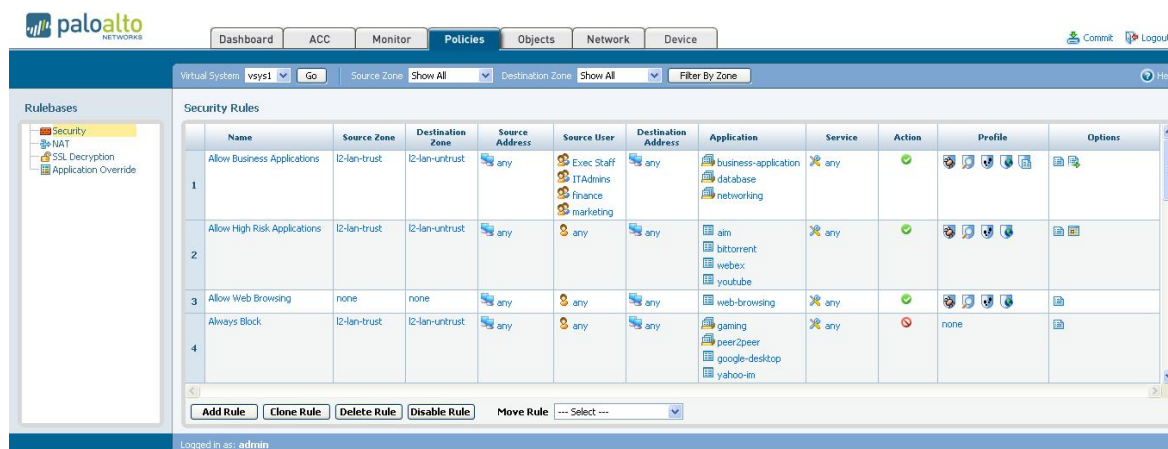


Figure 7: A familiar look and feel takes full advantage of existing firewall policy editing skills, accelerating the deployment of application usage control policies.

FlashMatch Real-Time Threat Prevention

Just as App-ID has taken a fresh approach to classifying traffic more accurately, Palo Alto Networks has applied the same innovative thinking to detecting and blocking threats. The result is FlashMatch™ Real-Time Threat Prevention. FlashMatch applies a uniform signature format to identify and block viruses, spyware, Trojans, worms, and vulnerability exploits in a single pass, as opposed to traditional, multiple pass offerings. The three key elements within FlashMatch include:

- **Uniform signature format:** The Palo Alto Networks development team has developed a uniform signature format that supports virus, spyware, botnet, and vulnerability exploit threat detection. By using a uniform signature format, the FlashMatch engine is able to detect multiple types of threats in a single pass, thereby accelerating performance and accuracy.
- **Real-time scanning:** The FlashMatch scanning engine is designed to look at reassembled streams of information to find unique threat identifiers. By avoiding the traditional file-based proxy method, the PA-4000 Series is able to scan multiple gigabits per second of traffic for a wide range of threats with very low latency. The net result: real-time applications can be inspected for threats without impacting the user experience.
- **Hardware enabled:** FlashMatch is accelerated in hardware to multi-gigabit speeds, even while scanning all traffic for all threats, yet is flexible enough to support dynamic updates for new threats

- Application decoding:** While part of App-ID, application decoding plays a critical role in the FlashMatch threat prevention engine. App-ID reassembles and parses application traffic to know exactly where to look for different types of threats, and when combined with FlashMatch, improves the accuracy of the threat prevention function.

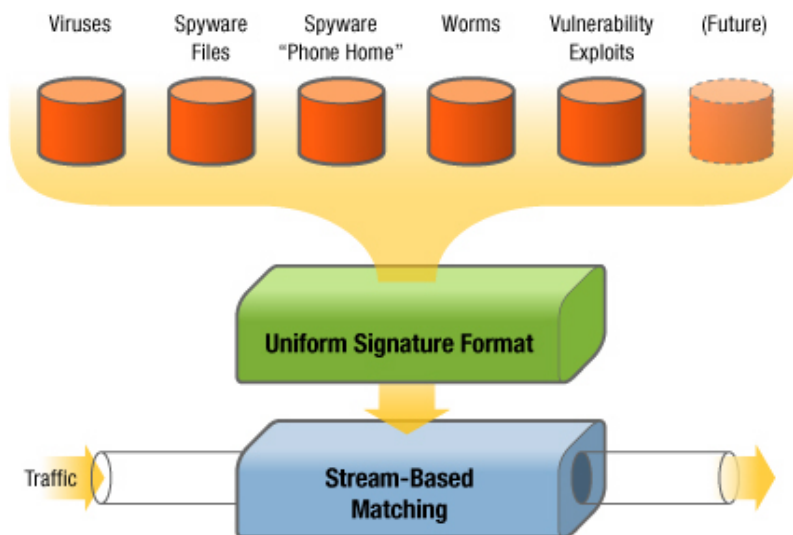


Figure 3: FlashMatch real-time, streaming threat prevention engine that blocks viruses, spyware, worms and application vulnerabilities in a single pass.

Networking

The PA-4000 Series is built from the ground up with a flexible networking architecture to ensure deployment in nearly any environment. From the high density physical interfaces running in virtual wire mode (completely transparent to surrounding devices), layer 2 or layer 3 modes to high availability options, the PA-4000 Series can be deployed along side almost any other network device in enterprise networking environments.

Just as App-ID makes it possible to implement a security policy that matches your corporate policy, the networking capabilities of the PA-4000 Series make it possible to configure the device fit cleanly into the network instead without IP address reconfiguration.

- Connectivity:** The PA-4000 Series has 16 10/100/1000 copper Ethernet ports and 8 SFP ports for data traffic. In addition, dedicated management and HA ports are provided.
- Virtual Wire:** In many scenarios, it is desirable to be able to deploy a firewall between two existing, functioning networking devices. With the virtual wire option in the PA-4000 Series, two ports can be paired so that all traffic coming in one port will, if allowed by policy, be sent out the other. No switching or routing is performed and the adjacent devices will not be aware of the existence of the PA-4000 Series.
- Switching and Routing:** The PA-4000 Series can be placed into layer 2 and layer 3 networks. Full 802.1Q VLAN support is provided so that all services can be provided without interfering with the existing VLAN architecture. 802.3ad is also supported to connect multiple ports to adjacent switches using link aggregation.

The PA-4000 Series networking foundation is very similar to common L2/L3 architectures but with zone-based security enforcement.

- **Network Address Translation (NAT):** The PA-4000 Series provides address and port translation for many different scenarios. Whether translating many internal addresses to one external address, providing one-to-one mapping of external addresses to internal addresses or simply mapping specific ports to various destinations, the NAT rulebase provides flexibility for even the most complex translation requirements.
- **Virtual Systems:** Architected from the ground up for virtualization, the PA-4000 Series provides a scalable method for segmenting services without sacrificing usability for administrators not requiring virtualization.

Deployment Options

With full support for traditional firewall applications and protocols, a rich networking foundation and a familiar policy editor, the Palo Alto Networks PA-4000 Series can be deployed as a complement to, or as replacement for, an existing firewall implementation.

- **Tap Mode:** By connecting the PA-4000 to the network via a span port, IT can monitor traffic in real-time, providing the IT department with exactly which applications are traversing the network without disrupting the existing infrastructure.
- **Inline Transparent Mode:** Using Virtual Wire, the PA-4000 Series is deployed inline, complementing yet completely transparent to the existing security infrastructure, allowing IT to begin controlling applications as needed.
- **Firewall Replacement:** The PA-4000 Series can perform all of the same allow/deny functionality that existing firewalls can, and IT may find that there is no need for two firewalls, allowing the PA-4000 Series to become the primary firewall.

High Availability (HA)

Network reliability is crucial in all enterprise environments. The PA-4000 Series provides configuration synchronization as well as full session synchronization so that if one device becomes inoperable—either through device failure or network connectivity failure—the backup firewall will be able to continue seamlessly, without impacting the applications currently passing through the firewall.

Each PA-4000 Series includes dedicated ports for HA traffic so that configuration synchronization is not adversely affected by session synchronization and normal data traffic is uninterrupted by the synchronization process. The high availability pair can either be connected directly or over a switched or routed network.

Management Flexibility

To accommodate the dynamic nature of network security and the varied management styles that each administrator may have, the PA-4000 Series can be controlled by a Command Line Interface (CLI), a web-based interface, or a centralized management solution (Panorama). Moving from one management interface to another does not hinder administrative efforts – the most current configuration is always used, thereby eliminating possible security holes. Both Panorama and the web-based interface have the exact same look and feel thereby minimizing the learning curve often associated with swapping between an individual device management interface and a centralized interface. No matter which management interface is preferred, administrators can quickly implement application

visibility and control policies. Rounding out the management interfaces are standards-based syslog and SNMP interfaces.

Logging and Reporting

The PA-4000 Series provides powerful, on-box logging and reporting tools that allow administrators to perform extensive data analysis. Logs are collected in real time and can be filtered on 17 different categories, including source/destination, user/group, application, and usage. Logs can be sent to a syslog server for more detailed analysis. Reporting is enabled through more than 25 pre-defined reports including Top Applications, Threats, Source and Destination, User/Group and Policy Rules.

Device Updates

To ensure that the PA-4000 Series is kept up-to-date, available software, threat, and application updates are shown in the web interface, with options for downloading, installing them. Updates to the documentation such as release notes are also displayed in the web interface.

Purpose-Built Platform

Architected for enterprise networks, the PA-4000 Series utilizes a combination of purpose-built hardware and PAN-OS, a security-specific operating system, to maximize security and performance. The PA-4000 Series is built to manage multi-Gbps traffic flows using a high speed network processor, a multi-core security processor and a dedicated threat prevention processor, all of which are connected by a 10 Gbps data plane. To ensure that management access is always available, irrespective of the traffic load, the control plane has been separated from the data plane with its' own dedicated processing, an industry first for the firewall market. The controlling element for the PA-4000 Series is PAN-OS, a modular operating system that delivers the reliability and flexibility needed for today's complex, high performance, and ever-changing networks.

- **Control plane processing:** Dual-Core CPU and dedicated memory enables highly available management under load and accelerates logging, route updates, and device management.
- **Data plane processing:** Multiple processing technologies are used to maximize throughput.
 - A 10 Gbps front-end network processor offloads security processors and delivers hardware accelerated QoS, route lookup, MAC lookup and NAT.
 - A multi-core security processor delivers high density processing and hardware-acceleration of standardized, complex security functions (IPSec, SSL, decompression, etc).
 - Dedicated processing and multiple memory banks are used to accelerate the FlashMatch engine to deliver high performance threat mitigation.

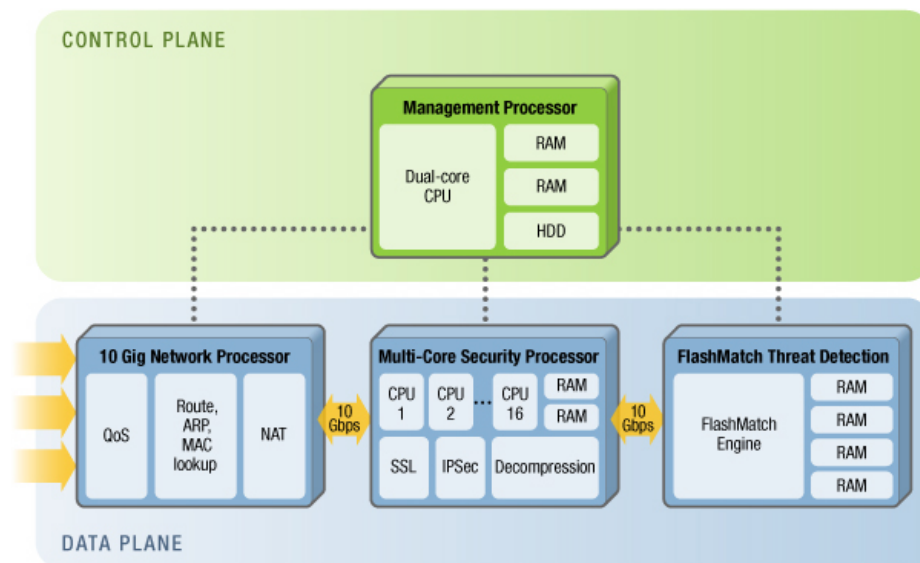


Figure 4: The PA-4000 Series is a purpose-built with dedicated processing for networking, security, threat prevention and management.

Conclusion

The Palo Alto Networks PA-4000 Series brings welcome relief to security teams struggling to gain control of, and protect the network from new threats borne by the next-generation of applications, both personal and business, that are specifically designed to evade today's port-based security offerings. With its' fresh from-the-ground-up approach, the Palo Alto Networks PA-4000 Series accurately identifies applications irrespective of the protocol or port that they may use for communications. Once accurately identified, appropriate security policies can be implemented to enforce application usage rights and any traffic that is ultimately allowed onto the network can be inspected more completely for all manner of malware.