

PA-4000 Series

The PA-4000 Series is a next-generation firewall that delivers unprecedented visibility and control of the applications flowing in and out of the enterprise network.

APPLICATION VISIBILITY:

- Uniquely identifies over 400 applications by application content irrespective of port, protocol, or SSL encryption
- Graphical visibility tools enable simple and intuitive view into application traffic

APPLICATION CONTROL:

- Allow or block by application, source/destination, URL category, or schedule
- Scan for threats, including viruses, spyware, and vulnerability exploits
- Mark traffic for QoS enforcement

THE PA-4000 SERIES INCLUDES:

- The PA-4020: capable of 2 Gbps firewall throughput and 2 Gbps full threat prevention
- The PA-4050: capable of 10 Gbps firewall throughput and 5 Gbps full threat prevention

Both models are equipped with 24 interfaces—16 10/100/1000 GigE and 8 SFP.



IT departments today face the common and growing problem of end-users downloading and installing a new generation of applications, both personal and business oriented, that are capable of evading detection on the network. At the same time, well-meaning corporate applications are utilizing similar tactics to accelerate deployment, facilitate wide spread access and minimize disruption.

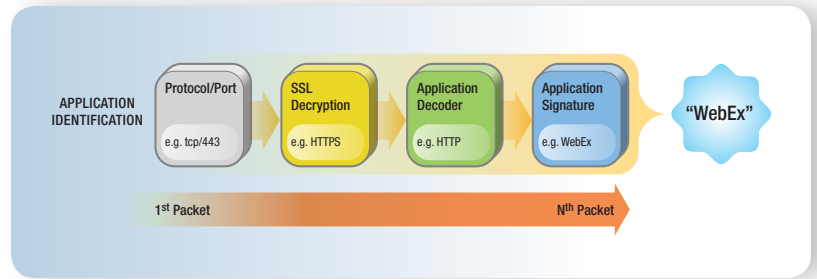
The result is a loss of visibility and control over the applications traversing the network which negatively impacts the business in several ways:

- **Business liability:** Regulatory and internal policy compliance, unseen data leakage
- **Operational expenses:** Rising bandwidth consumption, added IT operational expenses, lost user productivity from personal application usage
- **Increased propagation of threats:** Viruses, spyware, worms and application vulnerabilities can quickly spread across the network

Most network administrators are aware that these applications exist and are managing as best they can with a patchwork of existing technologies. The key challenge they face is that their firewalls use port and protocol to identify and control what gets in and out of the network. This port-centric design is at a disadvantage when facing new applications that have increasingly sophisticated security evasion techniques such as random port numbers, application emulation and SSL encryption. What's needed is an application-centric approach to traffic classification that can bring policy-based application control back to the network security team.

App-ID

A combination of four traffic classification techniques accurately identifies applications traversing the network.



Introducing the PA-4000 Series

The Palo Alto Networks PA-4000 Series is 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. Based upon a new traffic classification technology called App-ID™, the PA-4000 Series can accurately determine which applications are flowing across the network, irrespective of port, protocol, SSL encryption or evasive characteristic. Armed with this in-depth knowledge, security administrators can implement policy-based controls over the applications on their network 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 operational efficiency by controlling application usage at the firewall gateway

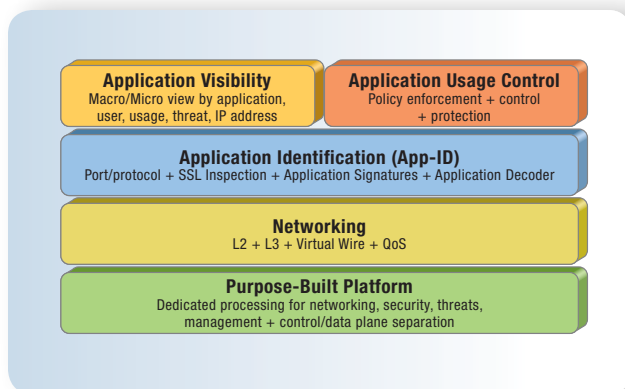
The PA-4000 Series consists of two models, the PA-4020 and PA-4050, both of which are targeted at high speed Internet gateway deployments.

Application Identification

Designed to help IT regain application visibility and control, App-ID is the cornerstone of the PA-4000 Series. App-ID’s application-centric approach to traffic classification addresses security evasion tactics commonly used in many of today’s new applications. App-ID uses four traffic identification mechanisms that operate in concert to determine exactly what application is running on the network.

- **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 continuous application decoding engine identifies the more evasive applications and creates 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. SSL decryption can be enabled or disabled per policy based on source, destination, and URL category.
- **Protocol/port:** helps narrow the application identification process, but is primarily used to enable policy control over which ports applications are allowed to use.

With App-ID identifying exactly which applications are traversing the network, administrators are empowered with newfound visibility and control over their application traffic.

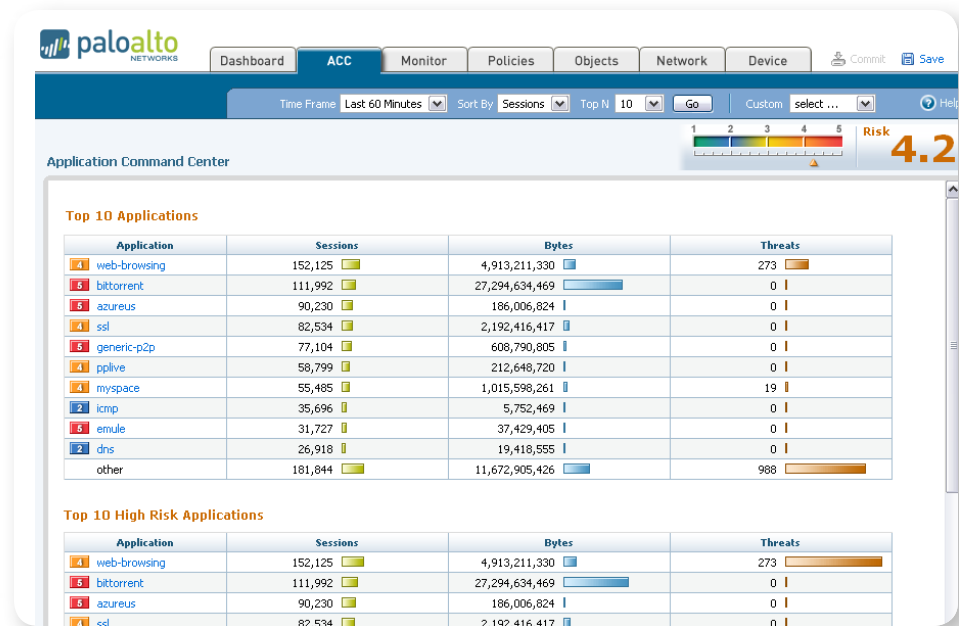


PA-4000 Series Architecture

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

Application Command Center

Application Command Center presents data in a clear, easy-to-read format with drill down into specific details.



Application Visibility and Policy Creation

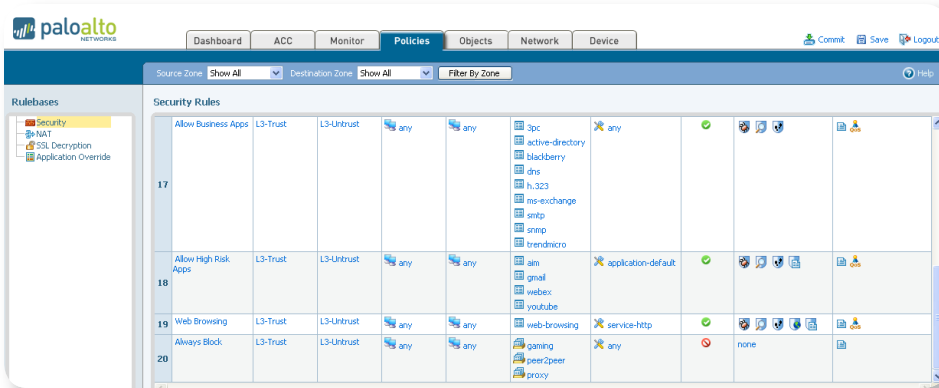
The application visibility that the PA-4000 Series and App-ID provides is harnessed by the Application Command Center (ACC), a simple to use, web-based interface that presents the data in a straightforward, easy to understand manner using the application names and traditional network security terminology. Armed with this newfound visibility into their applications traffic, administrators can quickly deploy security policies using the intuitive and familiar interface. Additional details on the visibility and policy creation features include:

- **Application visibility:** ACC summarizes the application activity collected by the PA-4000 Series, allowing administrators to view application traffic sorted by usage (sessions and bytes), by threat and by category. A click of the mouse enables drill down into additional information on the application as well as more details on usage, specific users, source/destination and threats.
- **Policy-based application usage control:** Increased visibility means that the security team can quickly analyze the data and make informed network security decisions that can easily be translated into application usage control policies. The policy editor carries a familiar look and feel to take full advantage of existing firewall knowledge, easing the implementation and transition processes. Application usage control policies can be enforced using a combination of the following parameters:

- 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 400 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

URL Filtering

Four base URL filtering categories are available as a standard feature, with an optional upgrade for a fully integrated URL database of over 20 million URLs across 54 categories for comprehensive web browsing control. This database enables control of web browsing by URL category as well as facilitating SSL decryption policies such as “don’t decrypt web browsing to finance sites” but “decrypt web browsing to online shopping sites”.



Policy Editor

A familiar look and feel takes full advantage of existing firewall knowledge to ease transition and implementation.

Real-Time Threat Prevention

Once identified, application traffic can be protected from a wide range of threats with FlashMatch™, a real-time, single-pass threat prevention engine. FlashMatch leverages the application visibility generated by App-ID and blocks viruses, spyware, worms, and vulnerability exploits in a single pass. Because traffic is inspected only once by FlashMatch—as opposed to the traditional method of passing traffic through multiple scan engines for each threat type—the PA-4000 Series is capable of scanning traffic at speeds of up to 5 Gbps.

Network Deployment Flexibility

A flexible networking architecture that includes Virtual Wire mode, layer 2 or layer 3 modes and high availability enables deployment of the PA-4000 Series into nearly any networking environment.

- **Virtual Wire:** Virtual Wire enables a truly transparent implementation where it is desired that the device be deployed without reconfiguring the existing infrastructure. Virtual Wire logically binds two ports together and passes all traffic to the other port without any switching or routing. Multiple virtual wire pairs can be configured to support multiple network segments. In all deployment options, interfaces are mapped to security zones which are in turn used to define security policy.

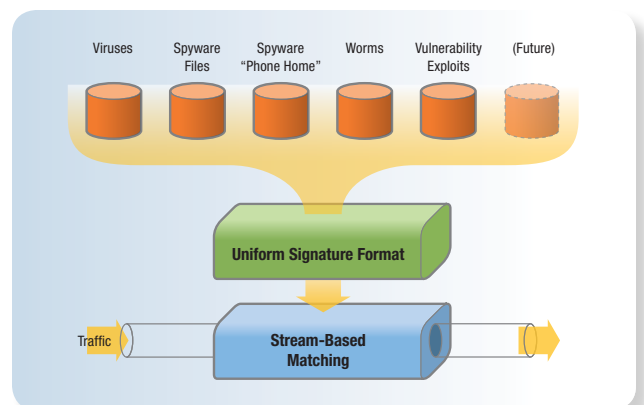
- **Switching and Routing:** The PA-4000 Series can be placed into layer 2 and layer 3 networks. The PA-4000 Series networking foundation is very similar to common L2/L3 architectures but with zone-based security enforcement. Full 802.1q VLAN support is provided for both layer 2 and layer 3, so that all services can be provided without interfering with the existing VLAN architecture.
- **Deployment Options:** With full support for traditional firewall applications and protocols, a rich networking foundation and a familiar policy management editor, the Palo Alto Networks PA-4000 Series can be deployed as a complement to, or as replacement for, an existing firewall implementation.

Logging and Reporting

The PA-4000 Series includes 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 14 different categories, including source, destination, application, and usage. Logs can be exported 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 and Policy Rules.

FlashMatch

FlashMatch real-time threat prevention protects traffic against viruses, spyware, worms, and vulnerability exploits in a single pass.

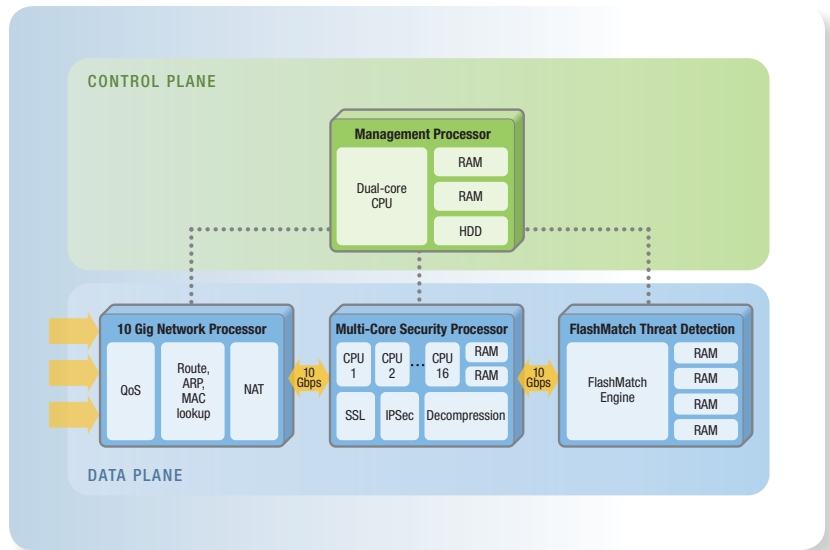


PA-4000 Specifications

	PA-4020	PA-4050
PERFORMANCE		
Firewall throughput	2 Gbps	10 Gbps
Threat prevention throughput	2 Gbps	5 Gbps
New sessions per second	60,000	60,000
Max sessions	500,000	2,000,000
APP-ID		
Applications identified	400+	400+
Application categories	14 categories: Business, Database, Email, Encrypted-tunnel, File Sharing, Gaming, General Internet, Instant Messaging, Media, Networking, Peer2Peer, Proxy, Remote Access, and Webmail	
File blocking by type	PPT, DOC, XLS, BAT, CAB, Zip, TAR, HTA, GZ, Z, PIF, REG, WSF, RAR, PL, SH	
Application packet capture	Yes	Yes
Zero-downtime App-ID updates	Yes	Yes
SSL decryption (forward proxy)	Yes	Yes
APPLICATION POLICY		
Policy control by application or category	Yes	Yes
URL filtering	Yes	Yes
Diffserv marking	Yes	Yes
Scheduled policies	Yes	Yes
FLASHMATCH REAL-TIME THREAT PREVENTION		
Antivirus	Yes	Yes
Anti-spyware	Yes	Yes
Network worm and vulnerability exploit protection	Yes	Yes
Default action designed for zero-tuning	Yes	Yes
Zero-downtime FlashMatch updates	Yes	Yes
NETWORKING		
Virtual wire, Layer 2, and Layer 3	Yes	Yes
802.1Q VLAN tagging (layer 2, layer 3)	Yes	Yes
Virtual routers (static routes)	10	25
Virtual systems	10	25
Network Address Translation (NAT)	Yes	Yes
HIGH AVAILABILITY		
Active/Passive	Yes	Yes
Configuration synchronization	Yes	Yes
Session synchronization	Yes	Yes
Interface and IP tracking	Yes	Yes
MANAGEMENT		
Command Line Interface (CLI)	Yes	Yes
Integrated web interface	Yes	Yes
Syslog	Yes	Yes
SNMPv2	Yes	Yes
HARDWARE SPECIFICATIONS		
I/O	16 10/100/1000 copper gigabit 8 SFP optical gigabit	
Management I/O	2 10/100/1000 high availability 1 10/100 out of band management 1 DB9 console port	
Power supply	Redundant 400W AC power	
Rack mountable	2U, 19" standard rack	
Safety	UL, CUL, CB	
EMI	FCC class A, CE class A, VCCI Class A, TUV	
ENVIRONMENT		
Operating temperature	32° to 122° F, 0° to 50° C	
Non-operating temperature	-4° to 158° F, -20° to 70° C	
ORDERING INFORMATION		
Palo Alto Networks PA-4050	PAN-PA-4050	
Palo Alto Networks PA-4020	PAN-PA-4020	
1 year threat prevention updates (PA-4050)	PAN-PA-4050-TP	
1 year threat prevention updates (PA-4020)	PAN-PA-4020-TP	
1 year URL filtering updates (PA-4050)	PAN-PA-4050-URL	
1 year URL filtering updates (PA-4020)	PAN-PA-4020-URL	
PART NUMBER		

Purpose-Built Platform

The PA-4000 Series is a purpose-built platform with dedicated processing for control and data plane enabling reliable, high performance throughput.

**Purpose-Built Platform**

Architected for enterprise networks, the PA-4000 Series utilizes a combination of custom-built hardware, function-specific processing with dedicated memory and PAN-OS, a security specific operating system. 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.



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

Copyright ©2007, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, FlashMatch and App-ID are trademarks of Palo Alto Networks, Inc. in the United States. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.