

PAN-OS

Palo Alto Networks' family of next generation firewalls delivers unprecedented visibility and control of applications flowing in and out of the enterprise network.

APPLICATION VISIBILITY:

- Identifies more than 700 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, application characteristics, user/group with Active Directory integration, source/destination, URL category, or schedule
- Scan for threats, including viruses, spyware, and vulnerability exploits

PLATFORM SUPPORT AND FIREWALL THROUGHPUT:

- PA-4060 - 10 Gbp
- PA-4050 - 10 Gbps
- PA-4020 - 2 Gbps
- PA-2050 - 1 Gbps
- PA-2020 - 500 Mbps



PA-4060



PA-4020



PA-4050



PA-2020



PA-2050

IT departments today face a growing problem of employees using a new generation of applications that are capable of evading detection on the network. Some may hop from port to port, others may sneak across port 80 or use SSL. At the same time, well-meaning corporate applications are utilizing similar tactics to accelerate deployment, facilitate wide spread access and minimize disruption.

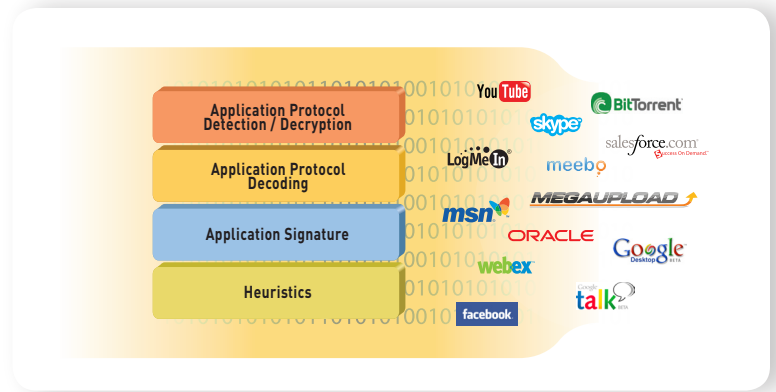
The result is a loss of visibility and control over the applications traversing the network, which introduces the following business risks:

- Business continuity risks brought on by propagation of malware and/or application vulnerability exploits
- Loss of data through unmonitored and/or unauthorized file transfer
- Internal and regulatory compliance risks through the lack of visibility into application usage
- Operational cost increases from higher bandwidth consumption, added IT expenses, and lost user productivity from personal application usage

IT 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, placing them at a disadvantage when facing new applications that use increasingly sophisticated security evasion techniques. What's needed is an application-centric approach to traffic classification that brings policy-based application control back to the network security team.

App-ID

Multiple traffic classification engines accurately identifies applications traversing the network.



Palo Alto Networks™ Next Generation Firewall

Palo Alto Networks brings visibility and control back to the security team with a family of next-generation firewalls that identify which applications are flowing across the network, irrespective of port, protocol, SSL encryption or evasive characteristic. The controlling element of the Palo Alto Networks family of firewalls is PAN-OS™, a security-specific

operating system that tightly integrates networking, IPsec VPN connectivity, threat prevention, and management features with unmatched application visibility and control capabilities. PAN-OS is married to a family of custom hardware platforms that have been built to manage enterprise network traffic flows using function specific processing for networking, security, threat prevention and management.

App-ID Traffic Classification Technology

At the heart of PAN-OS is App-ID, a patent-pending traffic classification technology that uses four different techniques to identify and classify applications, going well beyond any other network security technology available. App-ID inspects all of the traffic passing through the firewall, one or more of these techniques – including application protocol detection and decryption, application decoding, application signatures, and heuristic analysis – to quickly identify the specific application associated with each packet stream.

- **Application Protocol Detection and Decryption:** With its deep knowledge of application protocols, App-ID identifies which protocol is being used and whether or not it is encrypted with SSL. If App-ID determines that the protocol is encrypted, it decrypts, then passes the traffic to other elements of App-ID. Once the application is identified, and deemed acceptable by policy threat prevention profiles are applied, ensuring no threats sneak through over SSL. App-ID then re-encrypts the protocol and the traffic and sends it on its way.
- **Application Protocol Decoding:** The application protocol decoding in App-ID serves two purposes - first, it enables App-ID to significantly narrow the

range of possible applications providing valuable context when applying signatures. Second, it strips away protocols that might be used for tunneling purposes. App-ID’s protocol decoders determine if the application is using a protocol as a normal application transport (such as HTTP for web browsing applications), or if it is only using the apparent protocol to hide the real application protocol (for example, Yahoo Instant Messenger might hide inside HTTP).

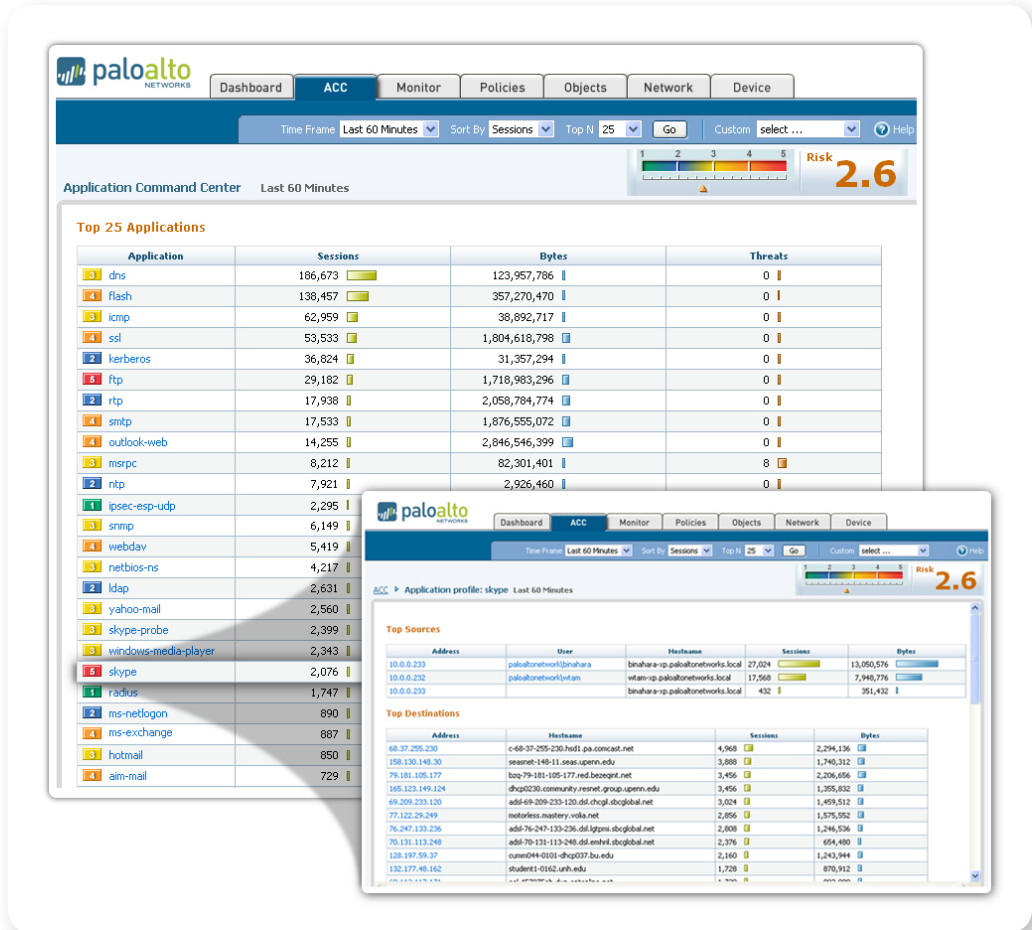
- **Application Signatures:** Context-based signatures look for unique application properties and related transaction characteristics to correctly identify the application regardless of the protocol and port being used.
- **Heuristics:** Applies additional heuristic or behavioral analysis to identify certain evasive applications - such as peer-to-peer or VoIP applications that use proprietary encryption. Heuristic analysis is used as needed in conjunction with the other App-ID identification techniques.



The identity of the application generated by App-ID is used as the basis for all visualization, reporting, policy control and threat prevention functions. Complementing the application identity is a rich set of data on each of the applications bringing a better understanding of the applications’ capabilities and potential risks resulting in more effective policy creation and enforcement.

Application Command Center

View current application activity in a clear, easy-to-read format with drill down for additional details including who is using it.



Application Visualization Tools

A powerful set of visualization tools presents administrators with a wealth of knowledge on which applications are traversing the network in a clear and concise manner for rapid interpretation. Armed with this information, administrators are enabled to make a more informed decision on how to treat the application. Application Command Center, App-Scope, customizable reporting, and the log viewer provide administrators with a wide range of data points on application traffic including what it is, who is using it, and the potential security impact.

- **Application Command Center (ACC):** ACC is a simple to use component of the web interface that provides a visual display of application traffic flowing across the network. Unlike other solutions that may present the data in cryptic port and protocol format, ACC provides administrators with an in-depth view into current application activity in a straightforward, easy to understand manner using the application names and standard security terminology.

- ▶ **Application usage:** ACC presents a high level summary of the top applications traversing the network. Drilling into a specific application shows the details of who is using the application, where the traffic is going, who is using it and the source / destination countries. Additional details about the application such as whether or not it has known vulnerabilities, can transfer files, or is known to be evasive is accessed with a click of the mouse.
- ▶ **User activity:** Clicking on any user or IP address in ACC provides a detailed view of a specific user's application activity, as well as information about any threats coming to or from the user or host. Knowledge of who is using the application is a critical element in the quest to learn more about the applications traversing the network and whether or not they require policy controls.
- ▶ **Threat activity:** A list of the threats traversing the network is shown in ACC, enabling an immediate view into the spyware, viruses, or vulnerability exploits traversing the network. Like the applications, a mouse click enables drill down into more detail.

- **App-Scope:** App-Scope complements the current view of traffic presented by ACC with a dynamic, user-customizable window into network activity that enables administrators to pinpoint problematic or erratic behavior with a view of what has transpired over time. For example, the traffic map provides administrators with a worldwide view of application traffic and threats traversing the network.
- **Reporting and Logging:** In addition to ACC and App-Scope, fully customizable and schedulable reports are available that provide detailed views into applications, users, and threats on the network. The log viewer enables forensic investigation into every session traversing the network using real-time filtering and regular expressions.

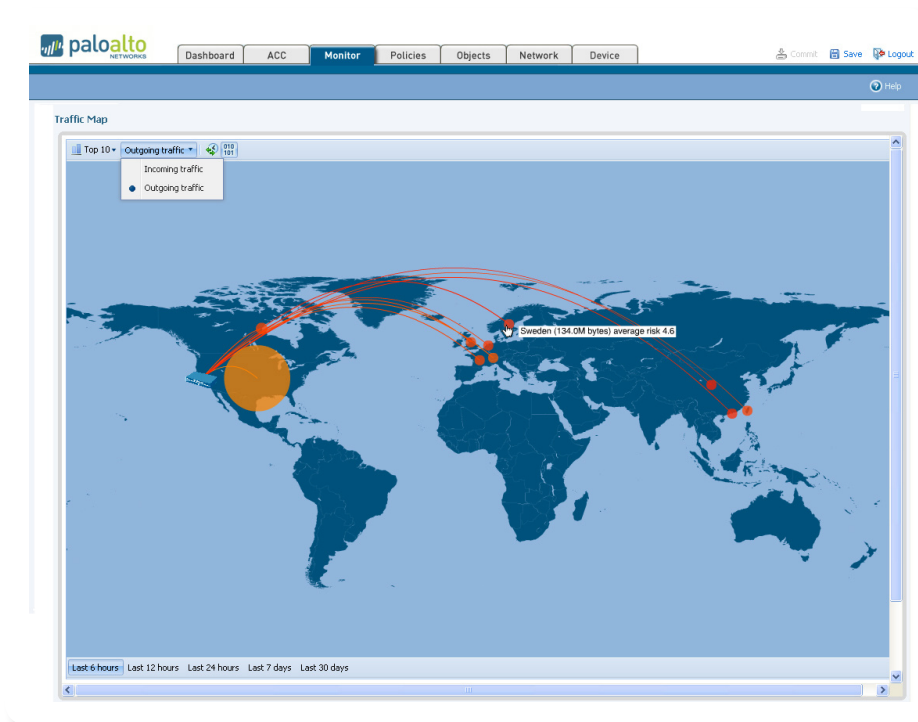
Management Flexibility

To accommodate the dynamic nature of network security and the varied management styles that each administrator may have, all Palo Alto Networks firewalls 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 as the most current configuration is always used, thereby eliminating possible out-of-sync configurations. Both Panorama and the web-based interface have the same look and feel, thereby minimizing the learning curve often associated with moving between an individual device management interface and a centralized interface. Rounding out the management interfaces are standards-based syslog and SNMP interfaces.

Networking Flexibility

A flexible networking architecture that includes dynamic routing, switching, high availability and IPSec VPN support enables deployment into nearly any networking environment.

- **Virtual Wire:** Virtual Wire logically binds two ports together and passes all traffic to the other port without any switching or routing, enabling a truly transparent implementation. 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:** A networking foundation that is very similar to common L2/L3 architectures but with zone-based security enforcement, enables deployment into L2/L3 networks. Dynamic routing protocols (OSPF and RIPv2) combined with full 802.1q VLAN support is provided for both L2/L3, so that all services can be provided without interfering with the existing routing or VLAN architecture.
- **High Availability:** Active/passive high availability is supported where the active device continuously synchronizes its configuration and session information with the passive device over two dedicated interfaces.
- **Site-to-Site VPN:** Standards-based IPSec VPN functionality provides secure site-to-site connectivity between headquarters and branch offices, business partners or customers. IPSec VPN connectivity combined with application visibility and control enables protected communications between two or more Palo Alto Networks devices or another vendor's IPSec VPN device.

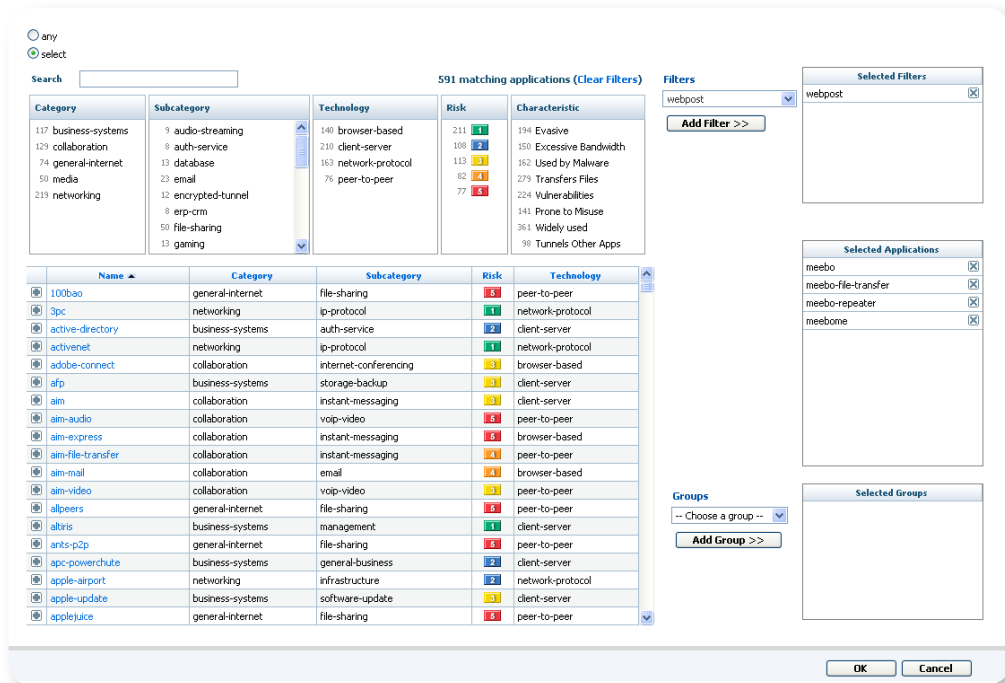


Traffic Map

Geographical view of application traffic and threats flowing in and out of the network.

Application Browser

Learn more about the applications traversing the network and immediately translate the results into application usage control policies.



Policy-based Application Usage Controls

Increased visibility means the security team can quickly analyze which applications are traversing the network, who is using them and then easily translate that data into application usage control policies. The policy editor carries a familiar look and feel, enabling experienced firewall administrators to quickly create firewall policies using standard parameters such as source and destination, security zone and time-based schedule. Where Palo Alto Networks differentiates itself from other solutions is in the ability to create and enforce effective application usage control policies based on applications, application characteristics, specific users or groups of users.

- **Application-based controls:** Policy controls based on applications are enabled using the application browser, an integral component of the policy editor that presents administrators with a wealth of information relevant to deciding how to treat an application. The application browser is unmatched by any solution on the market, allowing administrators to view the application, which category and subcategory it belongs in, its underlying technology and what the application characteristics are. The application characteristics tell administrators about the application file transfer capabilities, whether it has had any known vulnerabilities, its ability to evade network security detection, the propensity to consume bandwidth, and capacity to transmit/propagate malware. Using the application browser, administrators can quickly research an application and immediately translate the results into a security policy.

- **User-based controls:** Transparent integration with Microsoft’s Active Directory (AD) enables administrator to create a security policy that is based on a specific user, set of users or a group. In the event that the IP address changes as the user moves from place to place, the Palo Alto Networks user ID agent continually checks to make sure that the user and user location is up to date.

URL Filtering

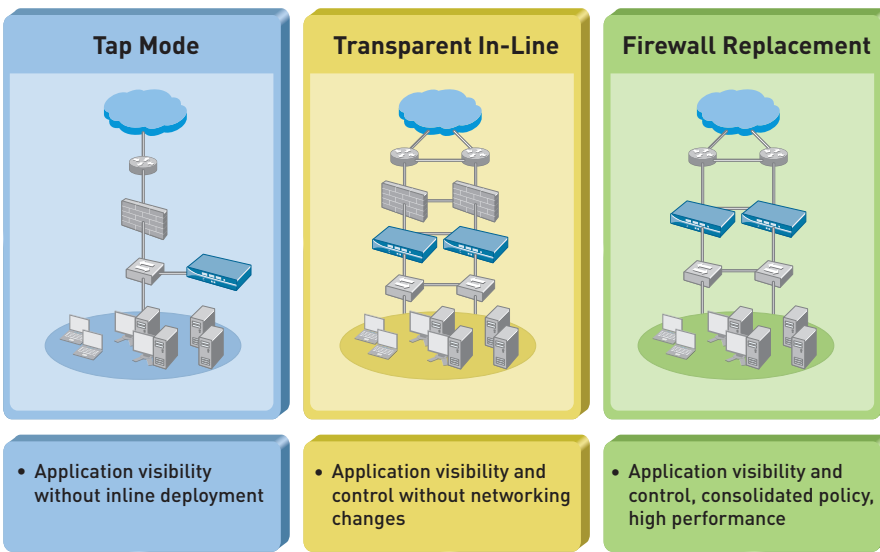
A fully integrated URL filtering database of over 20 million URLs across 54 categories allows administrators to apply granular web browsing policies, complementing the application visibility and control policies and safeguarding the enterprise from a full spectrum of legal, regulatory, productivity and resource risks. The URL filtering database also facilitates SSL decryption policies such as “don’t decrypt traffic to finance sites” but “decrypt traffic to web-based email sites”.

Real-Time Threat Prevention

Application traffic is protected from a wide range of threats with FlashMatch, a real-time, stream-based threat prevention engine that leverages the application visibility generated by App-ID to block viruses, spyware, worms, and vulnerability exploits. Traffic and files are inspected in a single pass as they stream through the Palo Alto Networks firewall eliminating the need to buffer or proxy them which results in improved throughput and minimal latency.

Flexible Deployment Options

A rich networking foundation enables deployment as a complement to, or as a replacement for, an existing firewall.



Reporting and Logging

Fingertip access to powerful reporting and logging enables analysis of security incidents, application usage and traffic patterns.

- **Custom reports:** Create custom reports either from scratch or based on one of the predefined reports. Custom reports can pull data from any of the log databases and can be configured to run on a regular basis.
- **Report Exporting:** Any of the reports – predefined or custom – can be exported to either CSV or PDF. In addition, the system can be configured to email a set of PDF reports on a daily basis.
- **Summary Report:** A custom, one-page summary report that pulls data from any of the predefined or custom reports or to provide a holistic view of application, threat, and user activity in the network. The summary report can be configured to be automatically distributed via email.
- **Log Viewer:** The log viewer provides a view into application and threat activity with flexible filtering capabilities. Clicking on a cell value immediately creates

a filter that can be narrowed down further by combining multiple criteria using an expression builder and additional log fields, even if they are not visible in the log viewer. The log viewer leverages the integration with Active Directory, complementing application and threat views with user and group visibility.

- **Log Exporting:** An export button is available to export any logs matching the current filter to a CSV file for offline archival or further analysis.

Additional Information (www.paloaltonetworks.com/literature)

- PA-4000 Series Hardware specifications datasheet
- PA-2000 Series Hardware specifications datasheet
- App-ID datasheet
- URL Filtering datasheet
- FlashMatch Real-Time Threat Prevention Whitepaper
- Panorama Centralized Management datasheet
- Support services datasheet



Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.207.0077
www.paloaltonetworks.com

Copyright ©2008, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, and Panorama 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.