Firewall Feature Overview

Palo Alto Networks' family of next generation firewalls delivers unprecedented visibility and control of applications, users and content flowing across the enterprise network.

APPLICATION IDENTIFICATION :

- Identifies more than 700 applications irrespective of port, protocol, SSL encryption or evasive tactic employed
- Graphical visibility tools enable simple and intuitive view into application traffic
- Policy controls block bad applications and control good applications

USER IDENTIFICATION:

- Policy-based visibility and control over who is using the applications through seamless integration with Active Directory
- Control non-Windows hosts via web-based authentication

CONTENT IDENTIFICATION:

- Block viruses, spyware, and vulnerability exploits, limit unauthorized transfer of files and sensitive data such as CC# or SSN, and control non-work related web surfing
- Single pass architecture enables multi-gigabit throughput with low latency while scanning content

PLATFORM SUPPORT AND FIREWALL THROUGHPUT:

- PA-4060 - 10 Gbps
- 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

As the center of enterprise network security, the firewall is the ideal location to enforce security policy. But because traditional firewalls rely on port and protocol to classify traffic, today's Internet applications can bypass them with ease; hopping ports, using SSL, sneaking across port 80 or using non-standard ports that are generally left open. The resultant loss of application control exposes enterprises to business risks including network downtime, increased operational expenses, data loss through unauthorized data transfer.

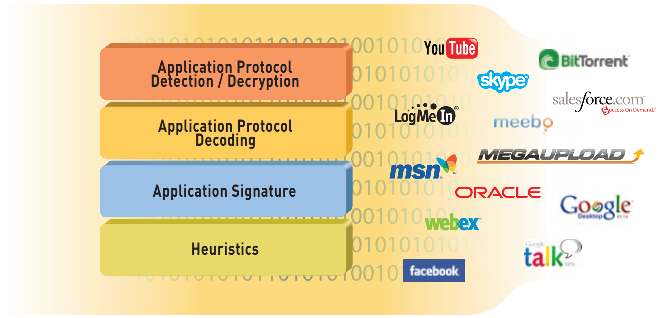
A next generation firewall restores application visibility and control for today's enterprises while scanning application content for threats, enabling organizations to manage risk more effectively. Enterprises need a next generation firewall that fulfills these key requirements:

- Identifies applications across all ports, irrespective of protocol, SSL encryption or evasive tactic.
- Protects in real time against attacks and malware embedded in application traffic.
- Simplifies policy management with powerful visualization tools and a unified policy editor.
- Delivers multi-gigabit throughput with no performance degradation when deployed in-line.

The Palo Alto Networks™ next generation firewall addresses key shortcomings that plague traditional stateful inspection-based firewalls and brings policy-based visibility and control over applications, users and content back to the IT department where it belongs.

Identification Technologies: The Power Behind Palo Alto Networks Next Generation Firewall

Palo Alto Networks' family of next generation firewalls provides policy-based visibility and control over applications, users and content with three unique identification technologies: App-ID, User-ID and Content-ID.



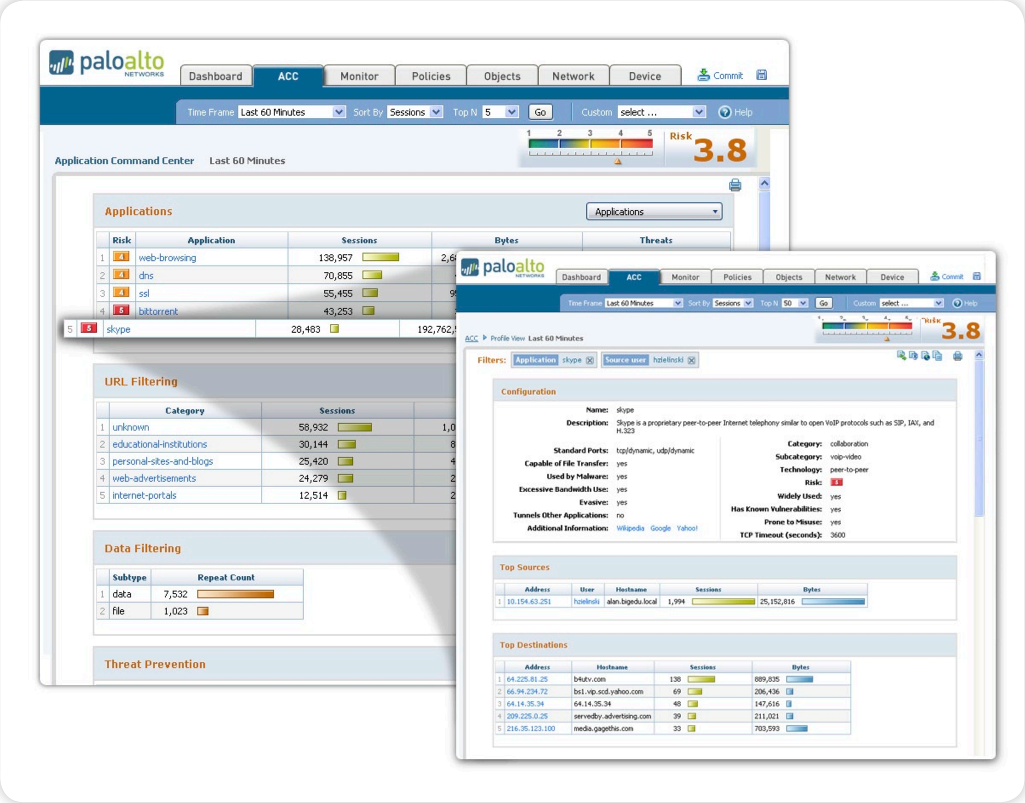
App-ID

Multiple traffic classification engines accurately identify applications traversing the network.

- **App-ID** is a patent-pending traffic classification technology that determines exactly which applications are traversing the network using up to four different identification techniques. The application identity is then used as the basis for all policy decisions including appropriate usage and content inspection.
    - **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. Encrypted traffic is decrypted, inspected based on policy, re-encrypted and sent on its way.
    - **Application Protocol Decoding:** Protocol decoders determine whether the application is using a protocol as a normal application transport or as an obfuscation technique and they help narrow the range of possible applications, providing valuable context when applying signatures. The decoders also identify files and other content that should be scanned for threats or sensitive data.
    - **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:** Heuristic or behavioral analysis is combined with other App-ID identification techniques as needed to identify certain evasive applications, particularly those that use proprietary encryption.
- **User-ID** seamlessly integrates Palo Alto Networks next generation firewalls with Active Directory to dynamically link an IP address to user and group information. With visibility into user activity, enterprises can monitor and control applications and content traversing the network based on the user and group information stored within the user repository.
- **Content-ID** combines a real-time threat prevention engine with a comprehensive URL database and elements of application identification to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing. A single pass architecture inspects traffic using a combination of stream-based scanning and a uniform signature format. Content-ID works in concert with App-ID, leveraging the application identity which makes the content inspection process more efficient.

A rich set of networking, IPSec VPN and management features join App-ID, User-ID and Content-ID as the key features of PAN-OS, the security-specific operating system that controls the Palo Alto Networks next generation firewalls. PAN-OS is married to a family of custom hardware platforms that are designed to manage enterprise network traffic flows using function specific processing for networking, security, threat prevention and management.

Application Command Center
View current application, URL, data filtering and threat activity in a clear, easy-to-read format. Add/remove filters to navigate to any depth of data specificity.



Time Frame: Last 60 Minutes · Sort By: Sessions · Top N: 5 · Custom: select ...

Application Command Center Last 60 Minutes

Applications

	Risk	Application	Sessions	Bytes	Threats
1	4	web-browsing	138,957	2,6	
2	4	dns	70,855		
3	4	ssl	55,455	9	
4	5	bittorrent	43,253		
5	5	skype	28,483	192,762,	

URL Filtering

	Category	Sessions	
1	unknown	58,932	1,0
2	educational-institutions	30,144	8
3	personal-sites-and-blogs	25,420	4
4	web-advertisements	24,279	2
5	internet-portals	12,514	2

Data Filtering

	Subtype	Repeat Count
1	data	7,532
2	file	1,023

Threat Prevention

Time Frame: Last 60 Minutes · Sort By: Sessions · Top N: 50 · Custom: select ...

ACC ▸ Profile View Last 60 Minutes

Filters: Application skype ☒ Source user hzielinski ☒

Configuration

Name: skype
Description: Skype is a proprietary peer-to-peer Internet telephony similar to open VoIP protocols such as SIP, IAX, and H.323

Standard Ports: tcp/dynamic, udp/dynamic
Capable of File Transfer: yes
Used by Malware: yes
Excessive Bandwidth Use: yes
Evasive: yes
Tunnels Other Applications: no
Additional Information: Wikipedia Google Yahoo!

Category: collaboration
Subcategory: voip-video
Technology: peer-to-peer
Risk: 5
Widely Used: yes
Has Known Vulnerabilities: yes
Prone to Misuse: yes
TCP Timeout (seconds): 3600

Top Sources

	Address	User	Hostname	Sessions	Bytes
1	10.154.63.251	hzielinski	alan.bigedu.local	1,994	25,152,816

Top Destinations

	Address	Hostname	Sessions	Bytes
1	64.225.81.25	b4utv.com	138	889,835
2	66.94.234.72	bs1.vip.scd.yahoo.com	69	206,436
3	64.14.35.34	64.14.35.34	48	147,616
4	209.225.0.25	servedby.advertising.com	39	211,021
5	216.35.123.100	media.gagethis.com	33	703,593

Powerful Visualization Tools

A powerful set of visualization tools presents administrators with a wide range of data points on applications traversing the network, who is using them, and the potential security impact. The Application Command Center, log viewer and fully customizable reporting are the primary components of the web interface that provide administrators with unmatched visibility into the applications, users and content traversing the network.

- **Application Command Center (ACC):** ACC graphically displays the applications, URLs, threats and data (files and patterns) traversing the network. Unlike other solutions that may present the data in a cryptic, hard-to-interpret format, ACC provides administrators with a view into current activity that can be tailored in several ways.
    - Application data can be viewed by risk, category, subcategory, or underlying technology.
    - Web activity can be displayed based on top URLs visited or blocked or top URL categories visited or blocked.
    - Data filtering shows files and sensitive data patterns (CC # and SSN) that are traversing the network.
    - Threat activity can be viewed based on spyware, vulnerability exploits, and viruses.

To learn more about the applications, URLs, data and threats traversing the network, administrators can mine ACC data by adding and removing filters in order to achieve the desired result. For example, selecting a specific application shows the details of what the application is, who is using it, where the traffic is going, and the source/destination countries. Additional filters can be added to learn more about individual user behavior, which security zones are sending/receiving the traffic, the potential threats and what files or data types are being transferred. The visibility that data mining ACC provides allows administrators to learn more about the network activity to make more informed policy decisions or respond more quickly to potential threats. In the event that ACC displays something that warrants immediate, in depth analysis, administrators can jump to the corresponding logs that match the current ACC context with a click of a mouse.

- **Reporting and logging:** The log viewer enables forensic investigation into every session traversing the network using real-time filtering and regular expressions. Fully customizable and schedulable reports are available that provide detailed views into applications, users, and threats on the network.

Content Inspection

The accurate identification of applications by App-ID solves only part of the visibility and control challenge that IT departments face with today's Internet-centric environment. Inspecting permitted application traffic becomes the next significant challenge and one that is addressed by the threat prevention, URL filtering and data filtering elements within Content-ID.

- **URL filtering:** A fully integrated URL filtering database of over 20 million URLs across 76 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. In addition to black list/white list options, administrators can use customizable block pages, password enabled access and user override to enable flexible yet enforceable web activity policies.

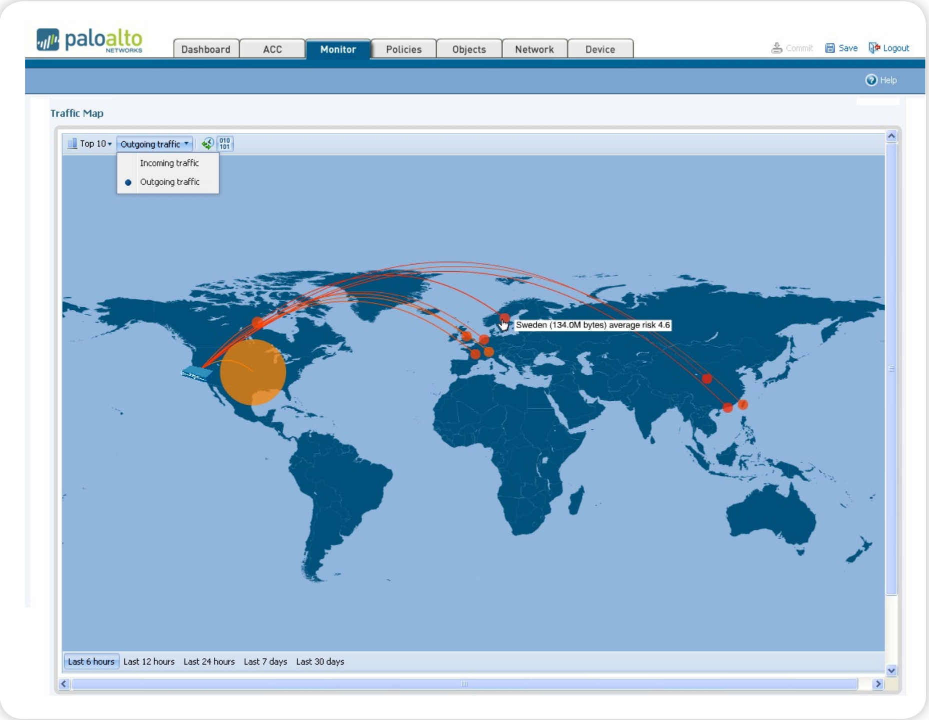
- **Threat prevention:** Detect and block a broad range of threats including viruses, spyware, application vulnerability exploits is performed by a threat prevention engine that delivers real-time performance through Palo Alto Networks' single pass architecture. The threat prevention engine combines a uniform signature format and stream-based scanning to inspect the traffic only once, simultaneously detecting and blocking all manner of malware in a single pass. The single pass architecture eliminates the need to buffer or proxy the files prior to threat inspection, resulting in improved throughput and reduced latency.

- **File and data filtering:** Taking full advantage of the in-depth application inspection being performed by App-ID and the single pass architecture, administrators can implement several different types of policies that reduce the risk associated with unauthorized file and data transfer.

    - **File blocking by type:** Controls the flow of a wide range of file types by looking deep within the payload to identify the file type (as opposed to looking only at the file extension).

    - **Data filtering:** Identify and control the transfer of sensitive data patterns such as credit card and social security numbers in application content or attachments.

    - **File transfer function control:** Control the file transfer functionality within an individual application, allowing application use yet preventing undesired inbound or outbound filr transfer.

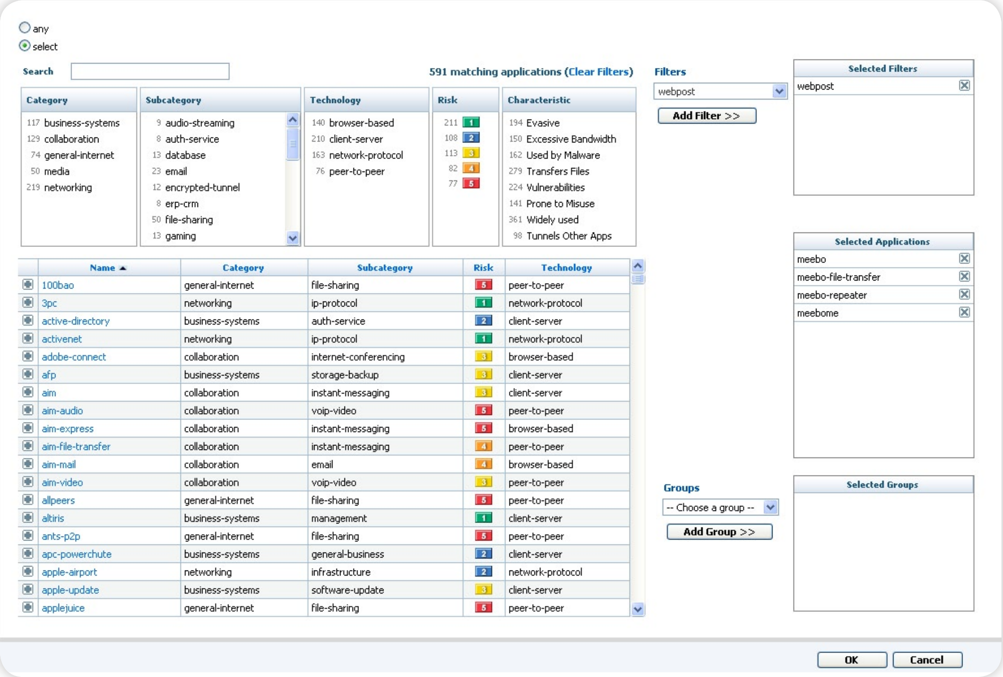


Sweden (134.0M bytes) average risk 4.6

Traffic Map

Geographical map of 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 security policies.



○ any
● select

Search

591 matching applications (Clear Filters)

Category	Subcategory	Technology	Risk	Characteristic
117 business-systems	9 audio-streaming	140 browser-based	211 1	194 Evasive
129 collaboration	8 auth-service	210 client-server	108 2	150 Excessive Bandwidth
74 general-internet	13 database	163 network-protocol	113 3	162 Used by Malware
50 media	23 email	76 peer-to-peer	82 4	279 Transfers Files
219 networking	12 encrypted-tunnel		77 5	224 Vulnerabilities
	8 erp-crm			141 Prone to Misuse
	50 file-sharing			361 Widely used
	13 gaming			98 Tunnels Other Apps

Name ▲	Category	Subcategory	Risk	Technology
100bao	general-internet	file-sharing	5	peer-to-peer
3pc	networking	ip-protocol	1	network-protocol
active-directory	business-systems	auth-service	2	client-server
activenet	networking	ip-protocol	1	network-protocol
adobe-connect	collaboration	internet-conferencing	3	browser-based
afp	business-systems	storage-backup	3	client-server
aim	collaboration	instant-messaging	3	client-server
aim-audio	collaboration	voip-video	5	peer-to-peer
aim-express	collaboration	instant-messaging	5	browser-based
aim-file-transfer	collaboration	instant-messaging	4	peer-to-peer
aim-mail	collaboration	email	4	browser-based
aim-video	collaboration	voip-video	3	peer-to-peer
allpeers	general-internet	file-sharing	5	peer-to-peer
altiris	business-systems	management	1	client-server
ants-p2p	general-internet	file-sharing	5	peer-to-peer
apc-powerchute	business-systems	general-business	2	client-server
apple-airport	networking	infrastructure	2	network-protocol
apple-update	business-systems	software-update	3	client-server
applejuice	general-internet	file-sharing	5	peer-to-peer

Filters
webpost
Add Filter >>

Selected Filters
webpost ☒

Selected Applications
meebo ☒
meebo-file-transfer ☒
meebo-repeater ☒
meebome ☒

Groups
-- Choose a group --
Add Group >>

Selected Groups

OK Cancel

Policy-based Controls

The Increased visibility into network activity generated by App-ID, User-ID and Content-ID means the security team can quickly analyze which applications are traversing the network, who is using them, the potential security risk and then easily translate that into firewall policies. 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 policy editor carries a familiar look and feel, enabling experienced firewall administrators to quickly create firewall policies such as:

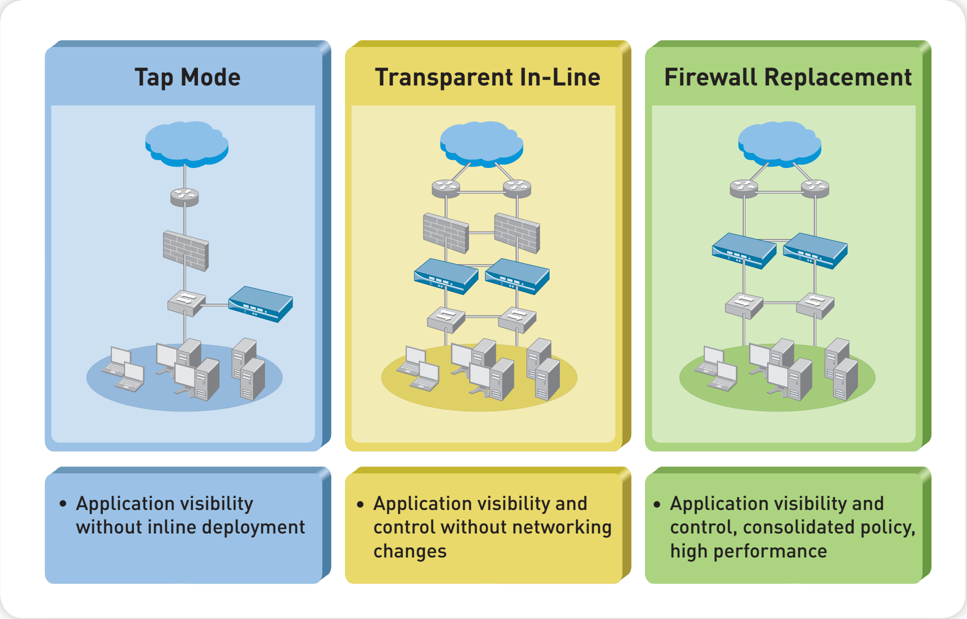
- Deny network access for certain types of applications such as peer-to-peer or circumventors and proxy services.
- Assign Saleforce.com and Oracle to the sales and marketing groups as defined in Active Directory. Define a group of applications such as SSH, Telnet, MS-RDP and allow only the IT group to use them.
- Define and enforce a corporate policy that dictates which webmail and instant messaging applications should be used, inspecting them for viruses, spyware and vulnerability exploits—all in a single policy rule.
- Identify the transfer of sensitive information such as credit card numbers or social security numbers, either in text or file format, and block, allow or send alerts on who is transferring the data .
- Define multi-level URL filtering policies that block access to obvious non-work related sites, monitor questionable sites and "coach" access to others by giving the user the ability proceed after an initial warning.
- Create traditional inbound and outbound port-based firewall rules mixed with application-based rules to smooth the transition to a Palo Alto Networks next generation firewall.

Networking

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 full inspection and control with no impact on the surrounding devices. Multiple Virtual Wire pairs can be configured to support multiple network segments.
- **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 RIP) combined with full 802.1Q VLAN support is provided for both L2/L3, so that all services can be enabled without interfering with the existing routing or VLAN architecture.

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



Tap Mode
- Application visibility without inline deployment

Transparent In-Line
- Application visibility and control without networking changes

Firewall Replacement
- Application visibility and control, consolidated policy, high performance

- **High Availability:** Active/passive high availability is supported where the active device continuously synchronizes its configuration and session information with the passive device.
- **Site-to-Site VPN:** Standards-based 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.

Management

To accommodate the dynamic nature of network security and the varied management styles and roles 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) with tailored roles providing access to only the necessary administrative functions for each administrator. 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.

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 from scratch, pulling data from any of the log databases or modify one of the predefined reports.
- **Report Exporting:** Export any of the predefined or custom reports to either CSV or PDF. Any of the PDF reports can be emailed on a scheduled basis.
- **Summary Report:** A custom, one-page summary pulls data from any of the predefined or custom reports and can be generated and emailed on a scheduled basis.
- **Log Viewer:** View application, threat and user activity through dynamic filtering capabilities enabled simply by clicking on a cell value and /or using the expression builder to define the filter criteria.
- **Log Exporting:** Export any logs matching the current filter to a CSV file for offline archival or additional analysis.

paloalto NETWORKS

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