

Palo Alto Networks Next-Generation Firewall Overview

The firewall is the most strategic network security infrastructure component, it sees all traffic, and as such, is in the most effective location to enforce security policy. Unfortunately, traditional firewalls rely on port and protocol to classify traffic, allowing tech-savvy applications and users to bypass them with ease; hopping ports, using SSL, sneaking across port 80, or using non-standard ports.

The resulting loss of visibility and control places administrators at a disadvantage and exposes enterprises to network downtime, compliance violations, increased operational expenses, and possible data loss. The historical approach to restoring visibility and control required that additional “firewall helpers” be deployed individually, behind the firewall or in a combined manner through sheet-metal integration. Neither of these approaches solves the visibility and control problem due to limited traffic visibility, cumbersome management, and multiple-latency inducing scanning processes. Restoring visibility and control requires a new, fresh, from-the-ground-up approach. What’s needed is a next-generation firewall.

Key Next-Generation Firewall Requirements:

- **Identify applications, not ports:** Identify exactly what the application is, across all ports, irrespective of protocol, SSL encryption, or evasive tactic. The application identity becomes the basis for all security policies.
- **Identify users, not just IP addresses:** Leverage information stored in enterprise directories for visibility, policy creation, reporting, and forensic investigation.
- **Inspect content in real-time:** Protect the network against attacks and malware embedded in application traffic at low-latency, high throughput speeds.
- **Simplify policy management:** Restore visibility and control with easy-to-use graphical tools and a policy editor that ties applications, users, and content together in a unified manner.
- **Deliver multi-gigabit throughput:** Combine high performance hardware and software in a purpose-built platform to enable low latency, multi-gigabit performance with all services enabled.

Palo Alto Networks was founded by security visionary Nir Zuk, with a mission to re-invent the firewall so it could once again become the most strategically important security device in the network. Palo Alto Networks next-generation firewalls enable unprecedented visibility and control of applications and content – by user, not just IP address – at up to 10Gbps. Based on patent-pending App-ID™ technology, Palo Alto Networks’ next-generation firewalls accurately identify applications – regardless of port, protocol, evasive tactic, or SSL encryption – and scan content to stop threats and prevent data leakage. With Palo Alto Networks, enterprises can, for the first time, embrace and benefit from a new generation of applications while maintaining complete visibility and control.

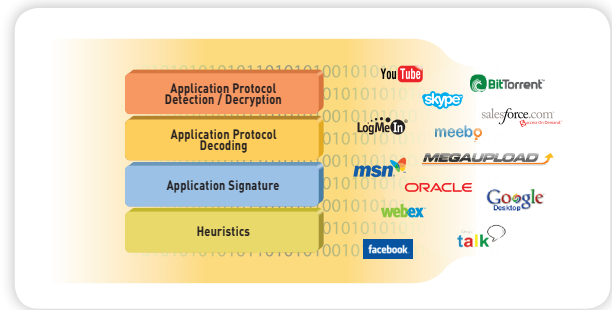


All features are supported by a family of six high performance platforms that fulfill a wide range of customer performance requirements. See www.paloaltonetworks.com for more information on individual platform specifications.

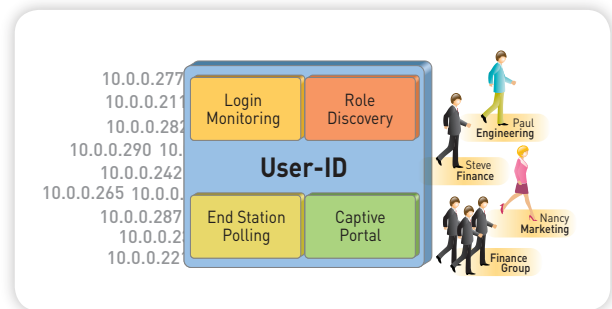
Unique Identification Technologies Enable Palo Alto Networks' Next-Generation Firewall

There are three unique technologies within the Palo Alto Networks' next-generation firewall that enable visibility and control over applications users and content: App-ID™, User-ID, and Content-ID. Each of the three technologies are industry firsts and are delivered in the form of a purpose-built firewall platform that helps administrators restore visibility and control. A complete set of traditional firewall, management, and networking features allows customers to deploy a Palo Alto Networks next-generation firewall into any networking environment.

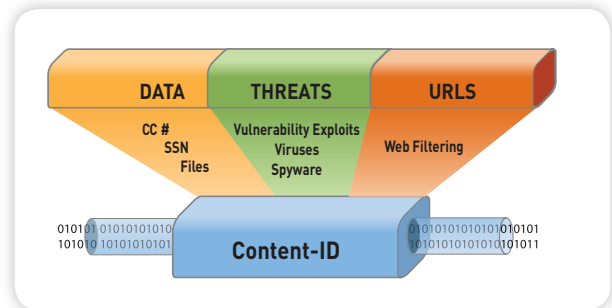
- **App-ID™:** The first firewall traffic classification engine to use as many as four different mechanisms to accurately identify exactly which applications are running on the network, irrespective of port, protocol, SSL encryption, or evasive tactic employed. The determination of the application identity is the first task performed by the firewall and that information is then used as the basis for all firewall policy decisions.



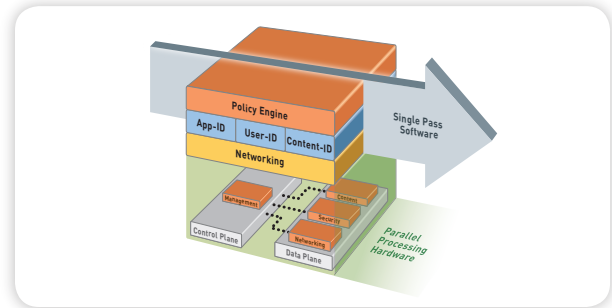
- **User-ID:** Seamless integration with enterprise directory services such as Active Directory, eDirectory, LDAP, and Citrix is unique to Palo Alto Networks and enables administrators to view and control application usage based on individual users and groups of users, as opposed to just IP addresses. User information is pervasive across all features including application and threat visibility, policy creation, forensic investigation, and reporting.



- **Content-ID:** A stream-based scanning engine uses a uniform signature format to block a wide range of threats and limit the transfer of unauthorized files and sensitive data, while a comprehensive URL database controls web surfing. The breadth of threat prevention, done in a single pass, is unique to Palo Alto Networks and when combined with the application visibility and control delivered by App-ID, IT departments regain control over applications and related threats.

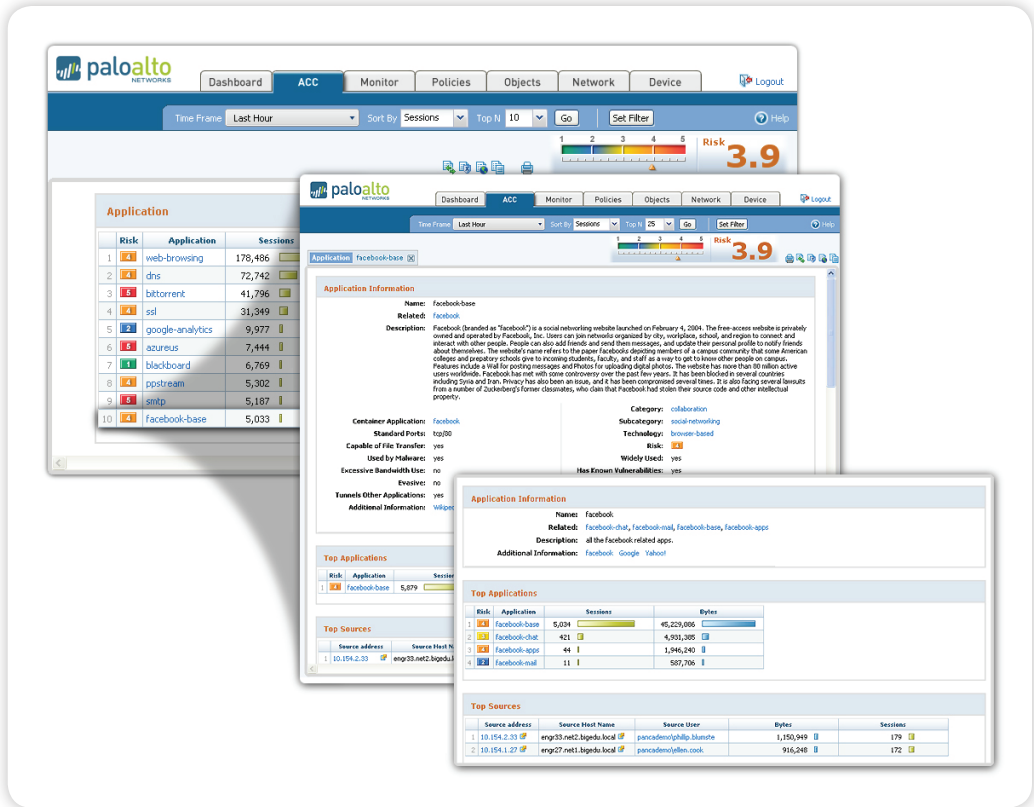


- **Purpose-built Platform:** Multi-Gbps throughput is enabled through function-specific processing for networking, security, threat prevention and management, which are tightly integrated with a single pass software engine to maximize throughput. A 10Gbps data plane smoothes traffic flow between processors while the physical separation of control and data plane ensures that management access is always available, irrespective of traffic load.



Application Visibility

View application activity in a clear, easy-to-read format. Add and remove filters to learn more about the application, its functions and who is using them.



Visibility into Applications, Users and Content

Administrators are in a race to keep up with users that are increasingly tech-savvy and applications that are technically advanced as well as easy to use. Making the race more difficult is the fact that the tools in the administrator’s arsenal are unable to provide them with up-to-date information on network activity. With a Palo Alto Networks next-generation firewall, administrators can use a powerful set of visualization tools to quickly see the applications traversing the network, who is using them, and the potential security impact. The visibility that the Application Command Center (ACC), App-Scope, log viewer, and fully customizable reporting provides can empower administrators to implement more business-relevant security policies.

- **Application Command Center (ACC):** A standard feature that requires no configuration effort, ACC graphically displays a wealth of information on current network activity including applications, URL categories, threats, and data. If a new application appears in ACC, a single click displays a description of the application, its key features, its behavioral characteristics, who is using it, and what security rules allowed it to be used. Additional filters can be added to learn more about application use for individual users along with the threats detected within the application traffic. In the span of just a few minutes, ACC provides administrators with the data they need to make more informed security policy decisions.

- **App-Scope:** Complementing the real-time view of applications and content provided by ACC, App-scope provides a dynamic, user-customizable view of application, traffic and threat activity over time.
- **Management:** To accommodate different management styles, requirements, and staffing, administrators can use the web-based interface, a complete Command Line Interface (CLI), or a centralized management solution (Panorama) to control all aspects of the Palo Alto Networks firewall. For those environments where different staff members require varied levels of access to the management interface, role-based administration across all three management mechanisms enables the delegation of administrative functions to the appropriate individual. Standards-based syslog and SNMP interfaces enable integration with 3rd party management tools.
- **Logging and Reporting:** Real-time filtering facilitates rapid forensic investigation into every session traversing the network. Pre-defined, fully customizable and schedulable reports provide detailed views into applications, users, and threats on the network.

Enabling Appropriate Application Usage Policies

Immediate access to the knowledge of which applications are traversing the network, who is using them, and the potential security risk empowers administrators to quickly and easily determine the appropriate response. Armed with these data points, administrators can apply policies with a range of responses that are more fine-grained than allow or deny. Policy control responses include:

- Allow or Deny
- Allow, but scan for viruses and other threats
- Allow based on schedule, users, or groups
- Decrypt and inspect
- Apply traffic shaping through QoS
- Apply policy-based forwarding
- Allow certain application functions
- Any combination of the above

Using a policy editor that carries a familiar look and feel, experienced firewall administrators can quickly create flexible firewall policies such as:

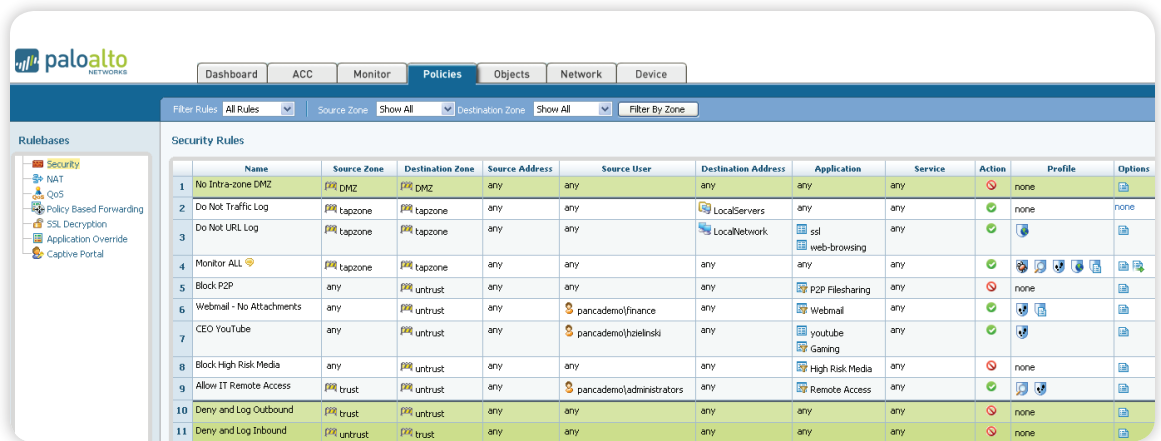
- Assign Salesforce.com and Oracle access to the sales and marketing groups by leveraging Active Directory integration.
- Enable only the IT group to use a fixed set of management applications such as SSH, telnet, and RDP.

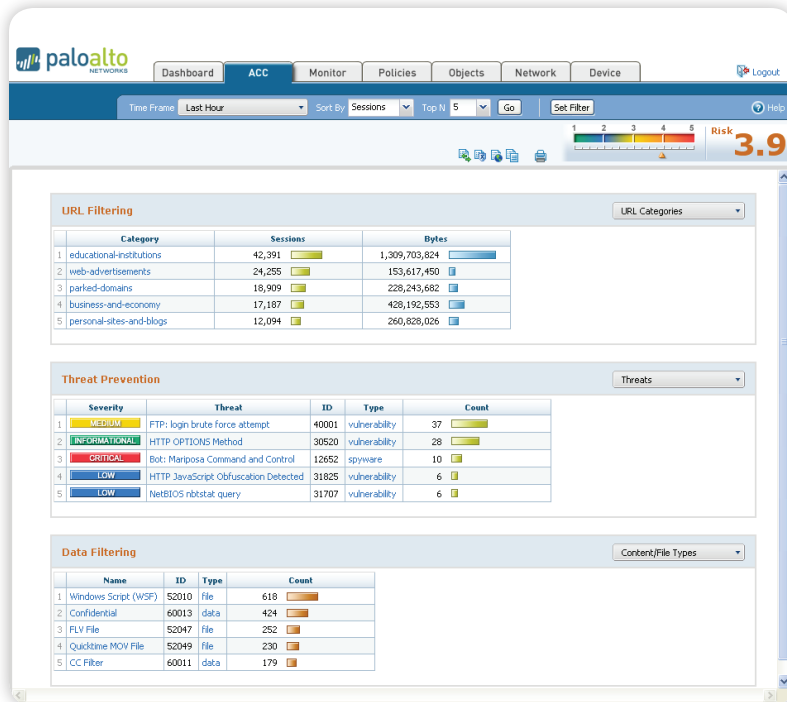
- Block bad applications such as P2P file sharing, circumventors, and external proxies.
- Define and enforce a corporate policy that allows and inspects specific webmail and instant messaging usage.
- Use policy-based forwarding to force Facebook application traffic over a specific route.
- Control the file transfer functionality within an individual application, allowing application use yet preventing file transfer.
- Identify the transfer of sensitive information such as credit card numbers or social security numbers, either in text or file format.
- Deploy URL filtering policies that block access to obvious non-work related sites, monitor questionable sites, and “coach” access to others.
- Implement QoS policies to allow media and other bandwidth intensive applications but limit their impact on business critical applications.

With a Palo Alto Networks next-generation firewall in place, customers can deploy positive enforcement model policies to block bad applications, scan business applications for threats and promote the secure use of end-user applications.

Policy Editor

A familiar look and feel enables the rapid creation and deployment of firewall policies that control applications, users and content.





Content and Threat Visibility

View URL, threat and file/data transfer activity in a clear, easy-to-read format. Add and remove filters to learn more about individual elements.

Protecting the Network from Threats

Regaining visibility and control over application traffic solves only part of the network security 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 a threat prevention engine that is tightly integrated with the firewall, combining a uniform signature format and stream-based scanning to block vulnerability exploits, viruses, and spyware in a single pass.

- **Intrusion Prevention System (IPS):** The vulnerability protection integrates a rich set of intrusion prevention system (IPS) features to block known and unknown network and application-layer vulnerability exploits, buffer overflows, DoS attacks, and port scans from compromising and damaging enterprise information resources. IPS mechanisms include:
 - Protocol decoder analysis
 - Stateful pattern matching
 - Protocol anomaly detection
 - Heuristic-based analysis
 - Statistical anomaly detection
 - IP defragmentation and TCP reassembly
 - Block invalid or malformed packets
 - Custom vulnerability signatures
- **Network Antivirus:** Inline antivirus protection detects and blocks most types of malware at the gateway. Antivirus protection leverages the uniform signature format and stream-based engine to protect

enterprises from millions of malware variants. Stream-based scanning helps protect the network without introducing significant latency – which is the problem with other network AV technologies that rely on proxy-based scanning. Furthermore, the stream-based engine can perform in-line decompression, protecting enterprises from zipped or compressed threats, and because Palo Alto Networks' next-generation firewalls have the ability to decrypt SSL by policy, organizations are further protected from malware moving across SSL encrypted application vectors.

URL Filtering

A fully-integrated, customizable URL filtering database of 20 million URLs across 76 categories allows administrators to apply granular web-browsing policies, complementing application visibility and control policies and safeguarding the enterprise from a full spectrum of legal, regulatory, and productivity risks. Custom categories can be created to complement the on-box URL database and address unique customer requirements. To suit local user community traffic patterns, the on-box database can also be augmented with a separate, dynamic 1 million URL cache database generated from a hosted, 180 million URL database.

Data Filtering

Data filtering features enable administrators to implement policies that will reduce the risks associated with the transfer of unauthorized files based on type (as opposed to looking only at the file extension) and confidential data patterns (credit card and social security numbers).

Network Deployment Flexibility

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

- **Switching and Routing:** L2, L3 and mixed mode support combined with zone-based security enables deployment into a wide range of network environments. Dynamic routing protocols (BGP, OSPF and RIP) and full 802.1Q VLAN support is provided for both L2 and L3.
- **Virtual Wire:** Logically bind two ports together and pass all traffic to the other port without any switching or routing, enabling full inspection and control with no impact on the surrounding devices.
- **Policy-based Forwarding:** Forward traffic based on policy defined by application, source zone/interface, source/destination address, source user/group, and service.
- **Virtual Systems:** Create multiple virtual “firewalls” within a single device as a means of supporting specific departments or customers. Each virtual system can include dedicated administrative accounts, interfaces, networking configuration, security zones, and policies for the associated network traffic.
- **Active/passive High Availability:** Sub-second failover with full support for configuration and session synchronization.
- **IPv6:** Full application visibility, control, inspection, monitoring, and logging for applications using IPv6 is supported (Virtual Wire mode only).
- **Jumbo Frames (PA-4000 Series only):** Jumbo frames (up to 9,216 bytes) are supported.

Secure Connectivity

- **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.
- **Remote Access VPN:** SSL tunnel VPN provides secure network access for remote users and extends policy-based visibility and control over applications, users, and content to those users.

Bandwidth Monitoring and Control

- **Quality of Service (QoS):** Traffic shaping extends the positive enablement policy controls to provide administrators with the ability to allow bandwidth intensive applications such as streaming media, while preserving the performance of business applications. Traffic shaping policies (guaranteed, maximum, and priority) can be enforced based on application, user, schedule, and more. Diffserv marking is also supported, enabling application traffic to be controlled by a downstream or upstream device.
- **Real-time Bandwidth Monitor:** Real-time graphical view of bandwidth and session consumption for applications and users within a selected QoS class.

Reporting and Logging

Powerful reporting and logging enables analysis of security incidents, application usage, and traffic patterns.

- **Reporting:** Predefined reports can be used as-is, customized, or grouped together as one report in order to suit the specific requirements. A detailed activity report shows applications used, URL categories visited, web sites visited, and a detailed report of all URLs visited over a specified period of time for a given user. All reports can be exported to CSV or PDF format and they can be emailed on a scheduled basis.
- **Logging:** Administrators can 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 filter results can be exported to a CSV file or sent to a syslog server for offline archival or additional analysis.
- **Trace Session Tool:** Accelerate forensics or incident investigation with a centralized, correlated view across all of the logs for traffic, threats, URLs, and applications related to an individual session.



Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.320.4788
408.738.7700

www.paloaltonetworks.com

Copyright ©2010, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. 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. PAN-OS 3.1, March 2010.

840-000001-00D