Firewall Feature Overview

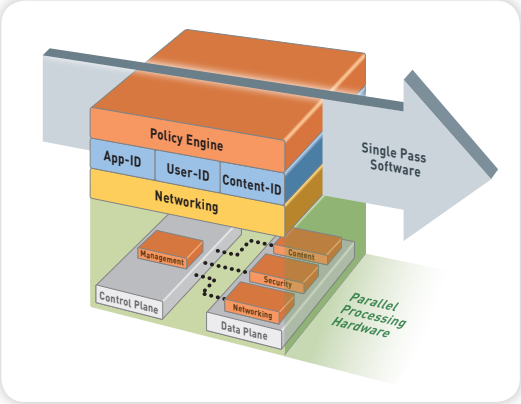
A next-generation firewall restores application visibility and control for today's enterprises while scanning application content for threats, enabling organizations to manage risk more effectively. Key requirements for next-generation firewalls include the ability to:

- Identify applications across all ports, irrespective of protocol, SSL encryption or evasive tactic.
- Enable policy control based on user identity and/or group membership, not just the IP address.
- Protect in real-time against attacks and malware embedded in application traffic.
- Simplify policy management with powerful visualization tools and a unified policy editor.
- Deliver multi-gigabit throughput with no performance degradation when deployed in-line.

The firewall is the most strategic security infrastructure component, it sees all traffic, and as such, is the ideal 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 resultant loss of visibility and control exposes enterprises to network downtime, compliance violations, increased operational expenses, and possible data loss. The traditional approach to solving the problem required that additional "firewall helpers" be deployed behind the firewall. This costly approach does not solve the problem due to limited traffic visibility, cumbersome management, latency inducing multi-scan software design and poor throughput.

Palo Alto Networks™ next-generation firewalls bring high performance, policy-based visibility and control over applications, users and content back to the firewall, where it belongs.



Single Pass Parallel Processing Architecture

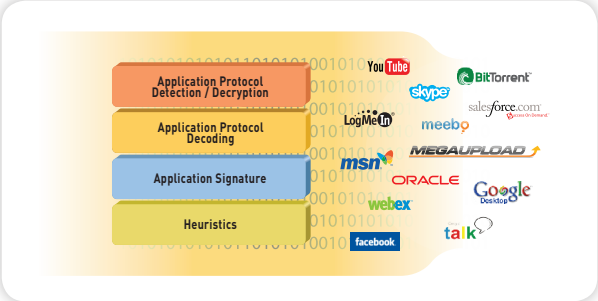
The foundation of the Palo Alto Networks next-generation firewall is a single pass parallel processing architecture, a unique approach to integrating software and hardware that simplifies management, streamlines processing and maximizes performance. The single pass software performs policy lookup, application identification and decoding, Active Directory user mapping, and content scanning (viruses, spyware, IPS) once on a given set of traffic. The software is tied directly to a parallel processing hardware platform that uses function specific processors for networking, security, threat prevention and management to maximize throughput and minimize latency.

paloalto NETWORKS

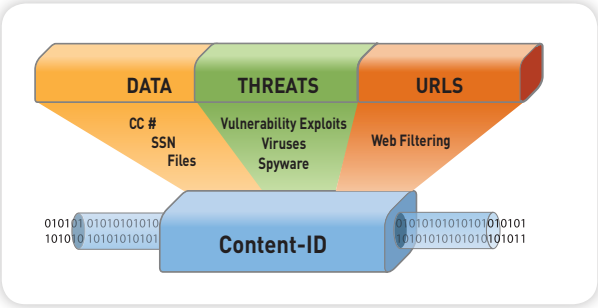
Unique Identification Technologies Enable Visibility and Control

The three key elements of the single pass parallel processing architecture that enable visibility and control over applications users and content are App-ID, User-ID and Content-ID. These unique identification technologies help IT managers accurately determine what is on their network and in so doing, allows them to make more informed policy decisions and improve their security posture.

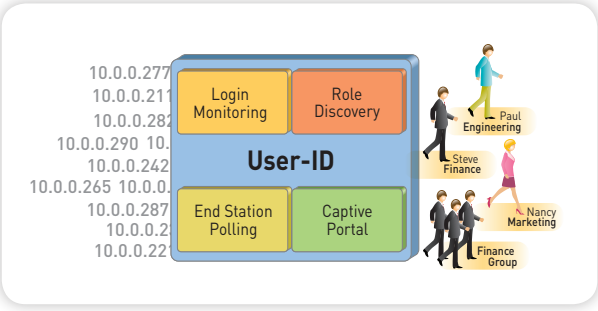
- **App-ID:** Using as many as four different traffic classification mechanisms, App-ID™ accurately identifies exactly which applications are running on the network, irrespective of port, protocol, SSL encryption or evasive tactic employed. App-ID gives administrators increased visibility into the actual identity of the application, allowing them to deploy comprehensive application usage control policies for both inbound and outbound traffic.



- **Content-ID:** A stream-based scanning engine that uses a uniform threat signature format detects and blocks a wide range of threats and limits unauthorized transfer of files and sensitive data while a comprehensive URL database controls non-work related web surfing. User-ID also provides visibility into Citrix and terminal services environments, enabling full application visibility, policy creation, logging and reporting.



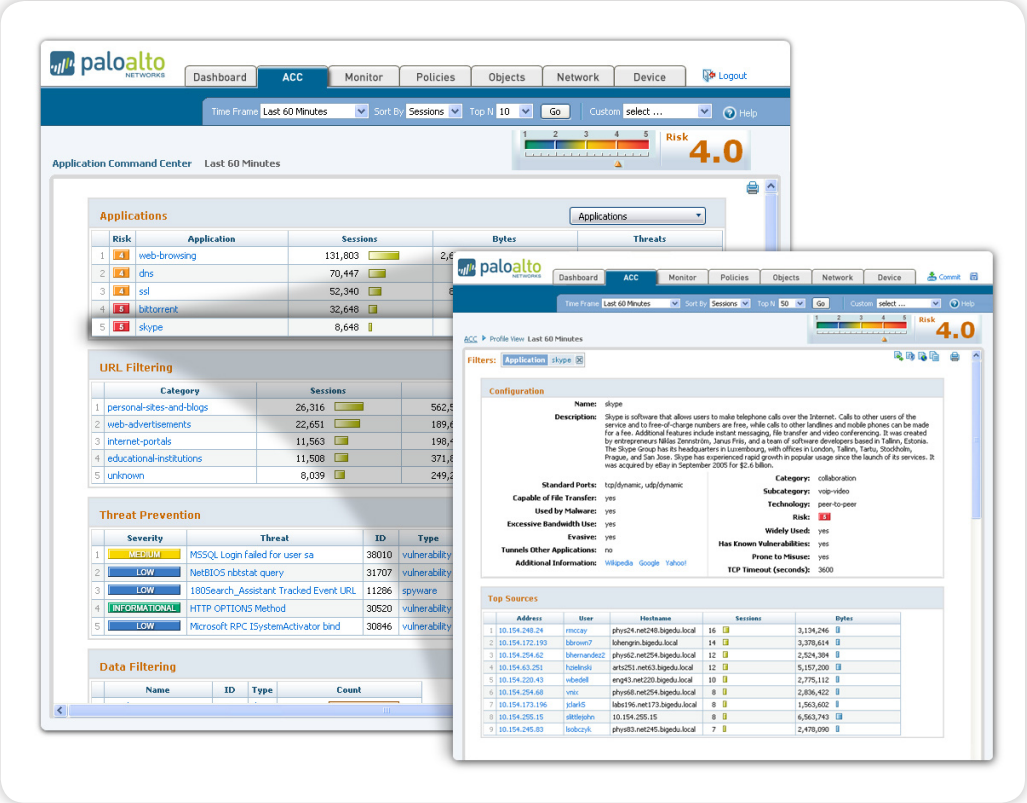
- **User-ID:** Seamless integration with Microsoft Active Directory links the IP address to specific user and group information enabling IT organizations to monitor applications and content based on the employee information stored within Active Directory. User-ID allows administrators to leverage user and group data for application visibility, policy creation, logging and reporting.



Rounding out the capabilities of PAN-OS, the security-specific operating system that controls the Palo Alto Networks next-generation firewalls is a rich set of traditional firewall, management and networking features.

Additional information on Palo Alto Networks' identification technologies can be found at http://www.paloaltonetworks.com/technology/index.html

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



Powerful Visualization and Management Tools

A powerful set of visualization tools including Application Command Center (ACC), App-Scope, the log viewer and fully customizable reporting provides security administrators with a wide range of data points on the applications traversing the network, who is using them, and the potential security impact.

- **Application Command Center (ACC):** ACC graphically displays a current view of application, URL, threat and data (files and patterns) traversing the network. An administrator can research an application by applying filters to see which employees are using the application and the threats that they may introduce to the network. Additional filters can be added to learn more about individual user behavior, threats and the associated traffic patterns. The visibility that ACC data mining provides allows administrators to make more informed policy decisions or respond more quickly to potential security threats.
- **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.
- **Logging and reporting:** The log viewer enables forensic investigation into every session traversing the network using real-time filtering and regular expressions. Pre-defined, fully customizable and schedulable reports provide detailed views into applications, users, and threats on the network.
- **Management:** Managing the Palo Alto Networks firewall is enabled using a Command Line Interface (CLI), a web-based interface, or a centralized management solution (Panorama). 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. Rounding out the management interfaces are standards-based syslog and SNMP interfaces.

Policy-based Controls Enable Appropriate Application Usage

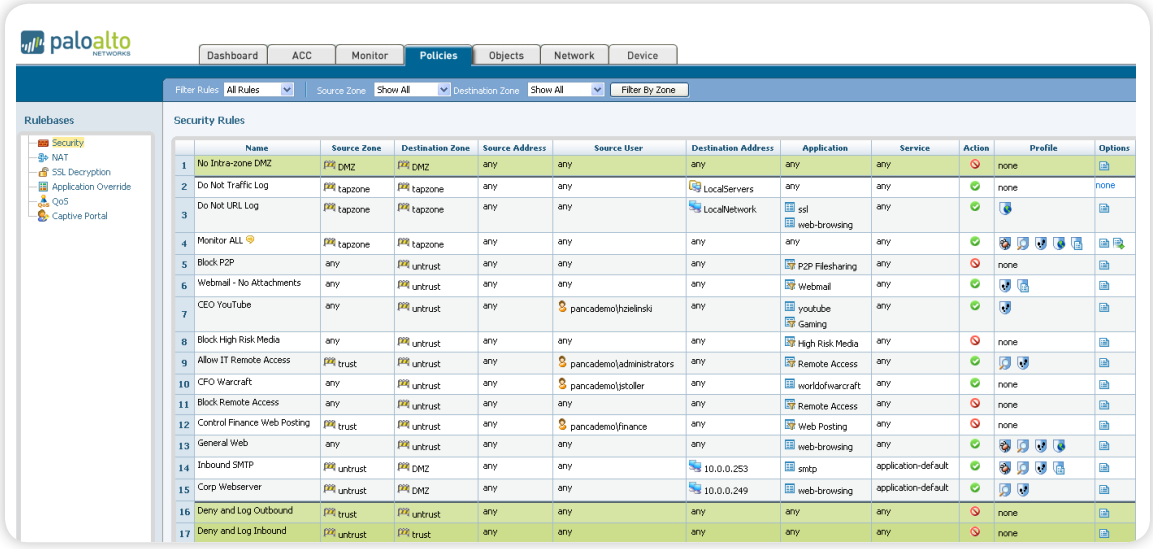
The increased visibility into network activity generated by App-ID, User-ID and Content-ID can help simplify the task of determining which applications are traversing the network, who is using them, the potential security risk and then easily determine the appropriate response. Armed with these data 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
- Allow based on schedule
- Decrypt and inspect
- Apply traffic shaping
- Any combination
- Allow certain application functions
- Allow for certain users or groups

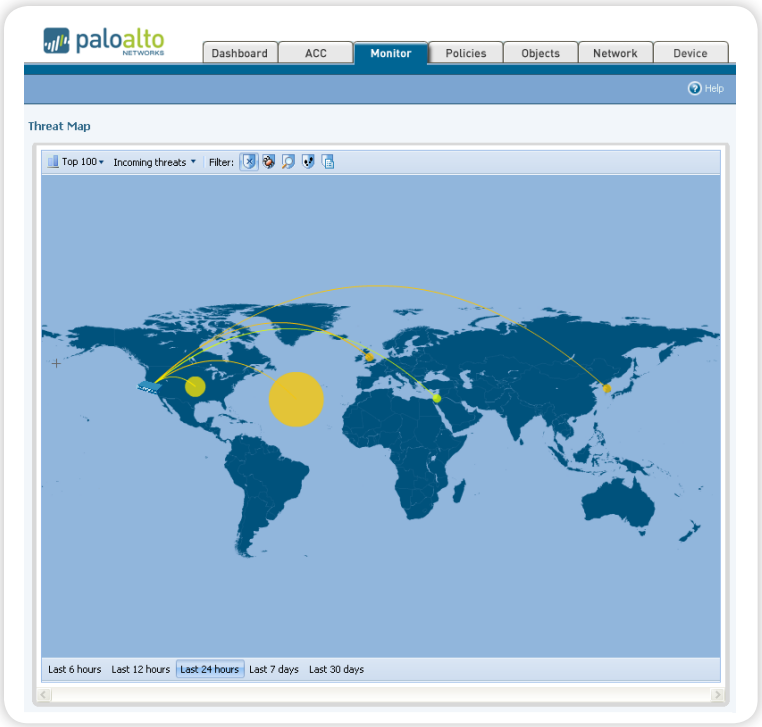
Using a policy editor that carries a familiar look and feel, experienced firewall administrators can quickly create flexible firewall policies such as:

- Assign Saleforce.com and Oracle 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.
- 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 multi-level 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, protect the business applications and promote the secure use of end-user applications resulting in a more positive employee environment.



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



Threat Map
Geographical representation of the threats traversing the network.

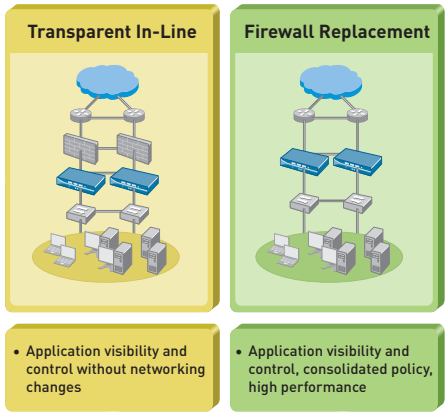
Identify the Application, Inspect the Content

The accurate identification of, and control over 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.

- **Threat prevention:** The threat prevention engine combines a uniform signature format and stream-based scanning to simultaneously detect and block viruses, spyware and application vulnerabilities in a single pass. The application vulnerability prevention integrates a 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 anomaly detection
  - Stateful pattern matching
  - Statistical anomaly detection
  - Heuristic-based analysis
  - Block invalid or malformed packets
  - IP defragmentation and TCP reassembly

  The threat prevention engine is stream-based which means that the scanning process begins as soon as the traffic hits the device, eliminating the need to buffer or proxy the files for threat inspection. The result is a dramatic reduction in latency and improved throughput.
- **URL filtering:** A fully-integrated, customizable URL filtering database of over 20M 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, productivity and resource risks. The on-box URL database can be augmented to suit the traffic patterns of the local user community. If a URL is detected that is not categorized by the local URL database, the firewall can request the category from a hosted URL database which has over 180M URLs. The URL is then stored locally in a separate, dynamic 1M URL database.
- **File and data filtering:** Taking full advantage of the in-depth analysis performed by App-ID, the Content-ID engine enables administrators to implement data filtering policies to reduce the risks associated with unauthorized file and data transfer. Files based on type (as opposed to looking only at the file extension) and confidential data patterns (credit card and social security numbers) can be detected and blocked based on policy.

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



Networking

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

- **Virtual wire:** Logically bind 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.
- **IPv6:** Full application visibility, control, inspection, monitoring and logging for applications using IPv6 is supported (virtual wire mode only).
- **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 (OSPF and RIP) and full 802.1Q VLAN support is provided for both L2/L3.
- **Active/passive high availability:** Hardware redundancy with full support for configuration and session synchronization.
- **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.
- **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.

Reporting and Logging

Fingertip access to 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.

paloalto NETWORKS

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

840-000001-00B