

Comparing Palo Alto Networks with Proxy-based Products

OVERVIEW

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. The ability to control applications leads to logical comparisons of Palo Alto Networks and proxies. The key differences between Palo Alto Networks and proxy-based solutions can be summarized as follows:

- **Breadth of Application Support:** Palo Alto Networks identifies and controls more than 800 applications flowing across all ports while proxy solutions look only at a limited number of ports and protocols.
- **Simplified Policy Management:** Palo Alto Networks delivers policy-based visibility and control over applications, users and content using a single, centralized policy table as opposed to proxy solutions whose management is known to be complex and cumbersome.
- **High Performance:** Palo Alto Networks next-generation firewalls are architected to deliver inline application visibility and control performance of up to 10 Gbps. The processing intensive nature of a proxy dictates that it be optimized for small subset of traffic, otherwise overall network performance will suffer.

	Palo Alto Networks	Proxies
Application support	More than 900	~20
Control over application functions	Yes	No
Apply threat inspection to each application	Yes	No
Application vulnerability exploit protection	Yes	No
Spyware protection	Yes	No
Anti-virus protection	Yes	Web* 1.0 only
Act as primary firewall	Yes	No
WAN Optimization(Caching, Compression, etc)	No	Yes

*Web 1.0 = HTML/HTTP/HTTPS/browser traffic

ABOUT THE PALO ALTO NETWORKS FIREWALL

Powering the Palo Alto Networks next generation firewall is a Single Pass Parallel Processing Architecture that uses single pass software to scan traffic once, thereby minimizing latency. A purpose-built hardware platform applies dedicated processing to networking, security, threat prevention and management functions to maximize throughput. Control over applications, users and content is delivered by three unique identification technologies: App-ID, User-ID and Content-ID.

- **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.
- **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** uses a single pass architecture and stream-based scanning to inspect traffic only once and prevent a wide range of threats, control non-work related web surfing and block the transfer of files and confidential data such as social security number and credit card number.

ABOUT PROXY-BASED PRODUCTS

Proxies (both firewall and caching) sit between the source and destination, intercepting traffic and inspecting it by terminating the application session and re-initiating it to the target destination. The proxy establishes the connection with the destination, acting on behalf of the client, hiding individual computers on the network behind the firewall. The result is the establishment of a connection between the client and the proxy and one between the proxy and the destination. When the connection process is complete, the proxy executes traffic forwarding and associated security decisions.

COMPARISON DETAILS

While the descriptive terminologies for Palo Alto Networks firewalls and proxies utilize similar words, the approach and end result are very different. Additional details on comparing Palo Alto Networks with proxy-based solutions in terms of application support, management and performance are outlined below.

- **Application Support:** By design, proxies must mimic the applications exactly, and because the process of developing and updating proxies is not trivial, the number of proxies supported tends to be limited to common applications (and protocols)—typically less than 20. Of the applications supported by proxies, many are traditional, well documented protocols (as opposed to applications) such as HTTP and FTP. Few if any proxies exist for many of the newer, end-user applications commonly found on today’s corporate network (e.g., CRM, database, email, instant messaging, P2P, social networking and media). These applications are constantly evolving and are, in many cases, integral to employee daily work environments.

In contrast, Palo Alto Networks can identify over 900 applications because App-ID monitors the application flow inline, applying identification mechanisms to the traffic, but does not have to rewrite the entire application. App-ID looks at all traffic across all ports, taking into account the fact that port, protocol and their association to the application are no longer fixed or known. As new applications are identified, the process to update the App-ID engine is as simple as updating the Palo Alto Networks application database with a new application signature. Translating this simple update process into an administrative context, if a policy is in place that says “Block all IM”, then the addition of a new IM signature or decoder is automatically covered, without any input required on behalf of the administrator.

- **Management:** With support for a limited set of applications, proxies are typically combined with other security elements such as a stateful inspection firewall and an IPS. Each of these security technologies are separate scanning mechanisms that run on a single, high-powered platform or multiple platforms. In either case, managing the security policy can be difficult because the proxy, firewall and IPS each have their own policy table. The separation of policy tables makes management a complex task and it also means that there is no ability to share what the proxy “learns” about traffic with the other security components. Palo Alto Networks applies App-ID to all traffic on all ports and then uses the identification of the application as the basis for all security decisions, so managing the policy is developed and deployed from a single policy table.
- **Performance:** Any type of security processing is computationally intensive and proxies tend to require significantly more processing than other inspection technologies because of the plain fact that the application connection is being terminated, inspected and then sent on to its destination. The extraordinary processing demands that proxies impose dictates that they be deployed in environments where high speed through-put is not a key requirement.

Palo Alto Networks next-generation firewalls are designed to act as the primary firewall, sitting inline to protect the network without impeding traffic. A purpose-built platform manages multi-Gbps traffic flows using a single pass software engine that is tightly integrated with parallel processing hardware that includes function specific processing for networking, security, threat prevention and management. A 10 Gbps data plane smoothes traffic flow between processors and eliminates potential bottlenecks while the physical separation of control and dataplane ensures that management access is always available, irrespective of traffic load.

SUMMARY

The Palo Alto Networks firewall and those products based upon proxies carry some similarities in that they are both designed to protect the network. That is where the similarities end. Palo Alto Networks can accurately identify and apply policy controls to more than 800 applications, irrespective of port, protocol, evasive tactic or SSL encryption, all while operating inline, at speeds of up to 10 Gbps.