# Comparing Palo Alto Networks with Proxies

## OVERVIEW

Palo Alto Networks next-generation firewalls provide organizations with the ability to securely enable applications using 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. However, there are key differences between Palo Alto Networks and proxy-based offerings:

- **Breadth of Application Support:** Palo Alto Networks identifies and controls more than 1,400 applications traversing the network, regardless of what port it is using, while proxy solutions look only at a limited number of applications, 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, in conjunction with the other, required supporting security components, is complex and cumbersome.
- **High Performance:** Palo Alto Networks next-generation firewalls are architected to deliver inline application enablement performance of up to 20 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 |
|---|---|---|
| Applications identified and controlled | More than 1,400 | ~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 | Occasionally |

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

## ABOUT THE PALO ALTO NETWORKS NEXT-GENERATION FIREWALL

Palo Alto Networks next-generation firewalls are designed specifically to manage enterprise traffic flows using function-specific processing for networking, security, threat prevention and management. Control over applications, users and content is delivered App-ID, User-ID and Content-ID.

- **App-ID: Classifying All Applications, on All Ports, All the Time.** App-ID addresses the traffic classification visibility limitations that plague proxy firewalls by applying multiple classification mechanisms to the traffic stream, as soon as the firewall sees it, to determine the exact identity of applications traversing the network. App-ID continually monitors the application state, re-classifying it to determine the different functions that may be in use. The security policy then determines how to treat the application: block, allow, or securely enable (scan for, and block embedded threats, inspect for unauthorized file transfer and data patterns, or shape using QoS).
- **User-ID: Enabling Applications by Users and Groups.** Traditionally, security policies were applied based on IP addresses, but the increasingly dynamic nature of users and computing means that IP addresses alone have become ineffective as a mechanism for monitoring and controlling user activity. User-ID allows organizations to extend user- or group-based application enablement polices across Microsoft Windows, Apple Mac OS X, Apple iOS, and Linux users. User information can be harvested from enterprise directories (Microsoft Active Directory, eDirectory, and Open LDAP) and terminal services offerings (Citrix and Microsoft Terminal Services). Integration with Microsoft Exchange, a Captive Portal, and an XML API enable organizations to extend policy to users outside of the Windows Domain.
- **Content-ID: Protecting Allowed Traffic.** Many of today's applications provide significant benefit, but are also being used as a delivery tool for modern malware and threats. Content-ID, in conjunction with App-ID, provides administrators with a two-pronged solution to protecting the network. After App-ID is used to identify and block unwanted applications, administrators can then securely enable allowed applications by blocking vulnerability exploits, modern malware, viruses, botnets, and other malware from propagating across the network, all regardless of port, protocol, or method of evasion. Rounding out the control elements that Content-ID offers are a comprehensive URL database (to control web surfing) and data filtering features (to control files and data leaks).

paloalto NETWORKS

## 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, re-initiating the connection to the target destination. The proxy acts 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.

## PALO ALTO NETWORKS VS. PROXY COMPARISON DETAILS

While the descriptive terminologies for Palo Alto Networks firewalls and proxies are similar, the approach and end result are very different. Additional comparison details in terms of application support, management and performance are outlined below.

- **Application Support:** By design, proxies must mimic the applications exactly, and because the effort of developing and updating proxies is not trivial, the number of proxies supported tends to be limited to common, legacy applications (and protocols)—typically less than 20. Of the applications supported by proxies, they are the traditional, RFC documented protocols, such as HTTP and FTP. Proxies don't exist for modern end-user applications commonly found on today's corporate network (e.g., CRM, database, email, instant messaging, P2P, social networking and media). Today's modern applications are constantly evolving and are, in many cases, integral to an employee's daily tasks.

  In contrast, Palo Alto Networks firewalls operate inline, identifying over 1,400 applications of all types, no matter which port they use. App-ID does not try to mimic the application and is therefore able to easily look across all ports, for all applications on the network, all the time. 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 App-ID. Translating this simple update process into an administrative context, if a policy is in place that says "Block all P2P", then the addition of a new P2P App-ID 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 either run on a single, high-powered platform or on 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, all the time, by default 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.

## 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 applications traversing the network, irrespective of port, protocol, evasive tactic or SSL encryption, all while operating inline, at speeds of up to 20 Gbps.

Palo Alto Networks
3300 Olcott St.
Santa Clara, CA 95054
May 2012