

Comparing Palo Alto Networks With Proxy-Based Products

OVERVIEW

Palo Alto Networks next-generation firewall classifies traffic from an application-centric perspective, thereby allowing organizations to accurately identify and control applications flowing in and out of the network. Because traffic is being classified from an application-centric perspective, logical comparisons are drawn between Palo Alto Networks and proxies.

Application visibility and control needs to be applied across all ports for all application traffic – not a subset thereof. The advantages that Palo Alto Networks has over proxy-based solutions can be summarized as follows:

- **Broader Application Support:** Palo Alto Networks looks at all traffic flowing across all ports to identify and control over 500 applications while proxy solutions typically look at a limited number of ports and protocols.
- **Simplified Policy Management:** Palo Alto Networks application control and threat prevention policies are implemented from a single, centralized policy table as opposed to Proxy solutions that are complex and cumbersome.
- **High Performance:** The Palo Alto Networks solution has been built from the ground up to identify and control applications traversing all ports – not a subset thereof. Proxies are not designed to look at all traffic—they are typically optimized for protecting servers.

The Palo Alto Networks advantage over proxies is visibility into all traffic flowing across all ports and the ability to control those applications, all from a single policy table, all at line rate with low latency.

ABOUT THE PALO ALTO NETWORKS FIREWALL

The enabling technology in the Palo Alto Networks firewall is called App-ID™, a new traffic classification technique that uses the application content to accurately identify the application, irrespective of protocol, port, SSL encryption or evasive tactic employed. The App-ID classification engine primarily uses a combination of application decoders, application signatures and SSL decryption. As traffic flows through the Palo Alto Networks firewall, App-ID identifies the application and then performs a policy lookup to determine what actions to take—allow, block, mark, scan for threats, and more.

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 all traffic forwarding and associated security decisions. Since all communication is conducted through the proxy server, very granular controls can be invoked on the proxy.

COMPARISON DETAILS

While the descriptive terminologies 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 50. Of the supported by proxies, many are traditional, well documented protocols (as opposed to applications) such as HTTP, FTP and so on. Few if any proxies exist for many of the newer, end-user applications commonly found on today's corporate network. Examples of these new applications include 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 500 applications because App-ID monitors the application flow, applying identification mechanisms to the traffic, but does not have to rewrite the entire application.

App-ID has been designed to look 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 admin.

- Management:** With support for a limited set of applications, proxies tend to be combined with additional security solutions such as Stateful inspection, packet filters and IPS. Each of these security technologies are separate scanning mechanisms running on a single, high-powered platform or multiple platforms. In either case, managing the security policy can be difficult because each has 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 accomplished 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 intercepted, inspected and then sent on to its destination. Due to extraordinary processing demands from proxies, they tend to be in environments where high speed through-put is not a key requirement. Designed to be deployed inline within high speed networks, Palo Alto Networks powers its flow-based architecture with a purpose-built platform with dedicated processing and memory for networking, security, threat prevention and management.

Proxies will always have a place in security environments where deep analysis of a limited set of applications or protocols is required. But for high-speed traffic environments where all traffic on all ports needs to be classified, proxies tend to fall short.

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 through a more complete analysis of the network traffic. That is where the similarities end. Palo Alto Networks can accurately identify and apply policy controls to over 500 applications, irrespective of port, protocol, evasive tactic or SSL encryption. All while operating at speeds of up to 10 Gbps.