

Comparing Palo Alto Networks IPS Products for Application Control

OVERVIEW

Palo Alto Networks next-generation firewalls enable policy based visibility and control over applications, users and content using three unique identification technologies: App-ID, User-ID and Content-ID. Because traffic is being classified at the application layer using application decoders and application signatures, logical comparisons are drawn between Palo Alto Networks and IDS/IPS offerings. Delivered as a purpose-built platform, Palo Alto Networks next generation firewalls have several distinct advantages over IPS offerings from an application visibility and control perspective.

- **Breadth of visibility and control:** Palo Alto Networks identifies more than 800 applications and the uses that identify as the basis for a positive enforcement security policy (allow only what is desired, block all else). Policies can be based on applications as well as users from Active Directory, as opposed to IP addresses. IPS offerings are purely threat oriented, looking for a few bad applications using a negative enforcement security policy (look for known bad items and block them, allow all else).
- **Simplified Policy Management:** Palo Alto Networks application, user and content control policies are implemented from a single, centralized policy table whereas IPS management is typically cumbersome, requiring multiple interfaces to implement a security policy.
- **High Performance:** The Palo Alto Networks solution has been built from the ground up to act as a firewall, identifying and controlling applications traversing all ports – not a subset thereof. An IPS is designed to look only at a subset of the network traffic to identify threats and as such, they would lack the performance required to look at all traffic across all ports.

The visibility and control over applications, users and content that Palo Alto Networks provides enables IT to more effectively manage the business and security risks associated with application traffic.

ABOUT THE PALO ALTO NETWORKS FIREWALL

Palo Alto Networks' family of next-generation firewalls enables more effective risk management on enterprise networks by employing business-relevant elements such as applications, users, and content as the basis for policy control. With its next generation firewalls, Palo Alto Networks addresses key shortcomings that plague traditional Stateful Inspection-based firewalls—a reliance on port/protocol to identify the applications and the assumption that IP address equates to a users identity. Palo Alto Networks uses App-ID to accurately identify the application, and maps the application to the user identity while inspecting the traffic for content policy violations. Deployed either as a complement to existing security infrastructure components, or as a primary firewall, Palo Alto Networks takes a traditional, positive approach to security enforcement—deny all traffic except that which is expressly allowed.

ABOUT IPS OFFERINGS

Intrusion Prevention Systems (IPS) detect and block attacks focused on vulnerabilities that exist in systems and applications. Unlike Intrusion Detection Systems (IDS) that focus only on alerting, IPS systems are intended to be deployed in-line to actively block attacks as they are detected. One of the core capabilities of an IPS is the ability to decode protocols to more accurately apply signatures. This allows IPS signatures to be applied to very specific portions of traffic, thereby reducing the percentage of false positives that were often experienced with signature-only systems. It is important to note that most IPS offerings will use port and protocol as the first pass of traffic classification, which, given the evasive characteristics of today's applications, may lead to an erroneous identification of the application. And because an IPS is focused mainly on attacks, they are typically deployed in conjunction with a firewall as a separate appliance or as a combination FW+IPS.

COMPARISON DETAILS

Additional details on the key differences between Palo Alto Networks and IPS offerings is outlined below.

- **Breadth of visibility and control:** IPS offerings are designed to look only for application related threats, a critical, yet narrow set of the overall traffic traversing the network. Palo Alto Networks provides visibility and control over applications, users and content with App-ID, User-ID and Content-ID.
 - App-ID™ accurately identifies exactly which applications are running on their network—irrespective of port, protocol, SSL encryption or evasive tactic employed. Administrators can use the identity of the application to deploy inbound and outbound application usage control policies.
 - User-ID seamlessly integrates with Microsoft Active Directory, linking the IP address to specific user and group information enabling IT organizations to leverage employee information for application visibility, policy control, logging and reporting.
 - Content-ID melds stream-based scanning, a uniform threat signature format, and a comprehensive URL database with elements of application visibility to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing.

The threat oriented nature of IPS offerings provides very little visibility and control over the applications on the network and in so doing, addresses only a small piece of the security puzzle IT departments are faced with today.

- **Policy management:** Controlling applications used to be achievable because traffic could easily be classified based on ports and protocols, but times have changed. Applications are no longer tied to ports or protocols, users cannot be controlled by IP address and content is more than just packets. The result? IT departments have lost visibility and control over applications, users, and content traversing the network and IPS were developed to “help” the firewall maintain control over threats.

Controlling applications, users and content traversing the network is amazingly simple to do with a Palo Alto Networks next-generation firewall. Policy-management is performed using a single policy table to select applications, users and threat protection profiles. In addition to covering application vulnerability exploits, threat protection profiles can be assembled for viruses, spyware, DoS attacks and file blocking. With a focus on blocking application threats, IPS policy management requires the definition of a list of “bad” things to block which implies that all traffic is allowed unless it meets the block criteria (a negative enforcement model). This an appropriate assumption when blocking application threats, but not for enabling secure use of applications. With a threat orientation, IPS offerings were never designed to act as the primary traffic gateway – they have been designed to be deployed as a stand alone solution, in conjunction with a firewall or as a combined solution. In either case, separate policy tables are required, making management more cumbersome and limiting policy control to that which is known “bad”.

- **Performance:** Application visibility and control requires that the solution implemented be deployed inline, looking at all traffic traversing the network on all ports. Designed to be deployed inline within high speed networks, Palo Alto Networks powers its flow-based architecture with a purpose-built platform that uses dedicated processing and memory for networking, security, threat prevention and management. The result is a system that scales to 10 Gbps while scanning all traffic on all ports for all applications. The integrated threat prevention works at up to 5 Gbps, enabling high speed content security as well. IPS systems have traditionally been relatively computationally constrained, often resulting in significant trade-offs between scanning all traffic and achieving stated performance. In deployments, most IPS systems only look at a subset of the traffic—often dictated by port-based classification—and many aren’t even deployed in-line.

SUMMARY

Dedicated IPS products will always provide a solution for identifying and blocking threats targeted at specific systems and applications, and may do this very well. But for high-speed traffic environments where visibility and control over applications, users and content is required to enforce an acceptable network use policy for compliance, security, and bandwidth reasons, IPS products are not the right solution.