

Comparing Palo Alto Networks With IPS 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 at the application layer using application decoders and application signatures, logical comparisons are drawn between Palo Alto Networks and IDS/IPS offerings.

Application visibility and control with Palo Alto Networks is focused identifying all application traffic flowing through all ports, not just the potential threats and vulnerabilities. The Palo Alto Networks advantages over IPS offerings can be summarized as follows:

- **Broader Application Support:** Palo Alto Networks identifies a broader range of applications, irrespective of port or protocol whereas IPS offerings are threat oriented, focusing only a subset of their effort on identification of the application.
- **Simplified Policy Management:** Palo Alto Networks application control and threat prevention 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 identify and control 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.

Application visibility and control must begin with identifying the application first – not just the threat. With Palo Alto Networks, application identification is the basis of all policy controls, allowing administrators to identify and control over 500 applications from a single policy table.

ABOUT THE PALO ALTO NETWORKS FIREWALL

The enabling technology 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 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. 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-BASED 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 comparing Palo Alto Networks with IPS-based solutions in terms of application support, management and performance are outlined below.

Application Support: Today's application landscape is extensive and growing quickly, both in breadth and sophistication. To provide visibility and control of these applications, Palo Alto Networks can identify over 500 applications, ranging from file sharing to instant messaging to video P2P to business applications—all irrespective of the port/protocol being used. In addition, SSL traffic can be decrypted on a per-policy basis, enabling visibility into an increasingly large segment of the network traffic. An IPS is designed to block vulnerabilities or attacks. They typically identify the most targeted applications using port-based classification, and then look for vulnerability exploits in the traffic. Many IPS systems are now extending their reach to look for “bad” applications, such as P2P applications, using signatures. The problem is that P2P is a very small subset of the many different applications that are operating on the corporate network.

- **Policy Management:** Application visibility and control is what a firewall is supposed to provide, and given the application landscape, it simply needs to evolve to content-based classification instead of port-based classification. Accurately identifying the application is the basis of all Palo Alto Networks policy management decisions. The policy-management process remains consistent with a firewall—from a single policy table, an administrator identifies the applications that are allowed on the network and who is allowed to use them, and blocks other applications. This is the essence of deploying and enforcing an acceptable application use policy. With a focus on blocking threats, IPS policy management focuses on defining a list of “bad” things to block. There is an implicit assumption that all traffic is allowed unless it meets the block criteria. This works well for blocking threats, but not that well for providing application visibility and control. 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 separate box next to the firewall or as combined solution, which means that they will require separate policy tables, 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 application visibility and control is required to enforce an acceptable network use policy for compliance, security, and bandwidth reasons, IPS products are not the right solution.