The Future of Intrusion Prevention

Why Your Next IPS is a Next-Generation Firewall

August 2010

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA 94089
408.738.7700
www.paloaltonetworks.com

Table of Contents

Executive Summary

Many IT organizations have deployed Intrusion Prevention Systems (IPS), mostly to protect datacenters from information security threats. While traditional IPS systems have provided some value historically, their effectiveness has steadily and significantly eroded in the face of evolving threat vectors that leverage application level intelligence to evade traditionl IPS and firewall solutions. Given the lack of control over this new threat vector in the enterprise, organizations are re-thinking their approaches to IPS. Where traditionally, organizations focused IPS considerations on server/datacenter protection, support, and performance, many organizations are now being forced to think about the client as an increasingly important threat conduit, and incorporate encrypted traffic and applications that carry threats into their thinking about IPS. Which leaves one with a question: given that we've moved from IDS to IPS, and we now have significant control requirements, is standalone IPS still the right model to keep threats out of the enterprise?

Gartner's research and recommendations on next-generation firewalls suggests that organizations should migrate to a different model. Gartner recommends that IT organizations migrate their IPS deployment (and firewall deployments, for that matter) to next-generation firewalls, which incorporate IPS, at the next refresh point. Not to be confused with simple device consolidation (a la UTM), next-generation firewalls start with a single architecture, designed from the ground up to classify traffic in terms of applications (rather than ports or protocols), and incorporate IPS functionality with enterprise-grade throughput and control.

Palo Alto Networks is the leader in next-generation firewalls, enabling enterprises first to control which applications run on their networks, and second, scan the allowed applications for threats. When compared to traditional IPS, even in concert with traditional firewalls, Palo Alto Networks' next-generation firewalls offer organizations unprecedented control, protection, performance, and support.

Many Enterprises Have Intrusion Prevention Systems, But…

In 2003, Gartner expressed what many organizations were feeling, and proclaimed the need to shift from intrusion detection to intrusion prevention. Organizations were inundated with events and false positives, and they rightfully demanded a more efficient method of protecting themselves from information threats. A similar transition is underway today – as threats have expanded beyond traditional vulnerability exploits and harnessed the power of applications to avoid detection, organizations are seeing their traditional IPS solutions becoming less and less effective while simultaneously delivering worse and worse performance. Clearly as the application and threat landscapes change, a new approach to IPS is required that protects against a new generation of threats and threat vectors. But perhaps most importantly, the IPS needs to play a key role in safely enabling high-value, high-risk applications.

…The Application and Threat Landscape Has Changed

Over the past several years there have been a number of significant changes to both the application and threat landscapes. Personal applications are pervasive, and increasingly indistinguishable from business applications (often, they're the same) – and threats are targeting these applications for a free ride into the enterprise. Originally intended primarily for personal communications, this class of applications includes instant messaging, peer-to-peer file sharing, web mail, and a plethora of social networking applications. Their presence on enterprise networks is practically guaranteed, even if an organization's policies dictate otherwise. This is due in part to their popularity, but they've also been designed to evade traditional countermeasures, such as firewalls, by dynamically adjusting how they communicate. Common tactics include: port hopping, use of non-standard ports, tunneling within commonly used services, and hiding within SSL encryption.

Many of these applications have proven to be extremely useful for more than just personal communications. Enterprises worldwide are routinely employing them for legitimate business purposes as well – helping to accelerate key processes, improve customer service, and enhance collaboration, communications, and employee productivity in general.

Even "pure" business applications are being designed to use the same evasive techniques – to be accessible and functional in every network, for every user, regardless of the security infrastructure in place. Additionally, wide ranges of conventional applications are being displaced altogether in favor of hosted, cloud-based services such as Salesforce.com, WebEx, and Google Apps. The result is that HTTP and HTTPS now account for approximately two thirds of all enterprise traffic – exacerbating an inherent weakness of traditional security infrastructure. Specifically, for older security infrastructures, the wide variety of applications riding on top of this universal protocol, whether or not they serve a legitimate business purpose, are practically indistinguishable.

Turning to the threat landscape, there have been significant changes there, too. In particular, a shift in motivation – from building fame and notoriety to actually making money – means that hackers are now focused more on easier evasion techniques. In this regard, one of the general approaches they are pursuing is to build threats that operate on, and through applications. This is because applications give attackers access to a plethora of options to avoid detection such as tunneling, encryption, compression and port evasion just to name a few. This allows their malicious creations to pass right through the majority of enterprise defenses, which have historically been designed to provide network-layer protection. Today's hackers are also paying considerable attention to the growing population of user-centric applications. Looking at social networking applications, we see worms, trojans and exploits. Worms and botnets target P2P file sharing networks – not just using them to spread, but also using them for command and control communication. Not only are such transmission vectors (a.k.a. applications) interesting targets due to their high degree of popularity, but also because their evasive capabilities can be leveraged to provide threats with “free passage” into enterprise networks.

The Traditional IPS vs. New Threats: A Poor Match

As defenses mature, attackers evolve. Given that IPS, like firewalls, are relatively well-understood, new attacks exploit well-known weak spots. These include attacking networks through client machines by targeting/tunneling though applications, and encrypting the attacks.

- **Application-borne Threats** – Threat developers are using applications, both as targets and as transmission vectors. Applications provide fertile ground for both methods – and remember, these applications are evasive, so they can pass through enterprise defenses easily. The number of evasive applications continues to increase. Palo Alto Networks, as part of its research effort, maintains Applipedia, a growing database of over 900 applications and their behaviors. Of the 900+ applications in Applipedia, 446 can transfer files, 200 are known to carry malware, and 470 have known vulnerabilities. Some of the application-borne threats are well-understood (e.g., many of the threats that move across social networks – koobface, boface, or fbaction), others not (Mariposa using MSN Messenger and P2P file sharing applications to spread). Regardless, attackers find it far easier to piggyback on applications, and start their attack with the client.

- **The Encrypted Threat Vector** – In addition to applications, threats have learned to leverage encryption and compression to avoid detection by traditional IPS solutions. While security researchers have warned for years that encryption would be used by various threats, encrypted attacks still needed a conduit – enter user-centric applications. Users are easily duped into clicking on encrypted links (too many users think that HTTPS means that “it’s safe”), which can send encrypted threats sailing through enterprise defenses. This is increasingly simple on social networks, where the level of trust is extremely high. The other, closely related vector is obfuscation via compression (zip and compressed HTTP). Traditional, stand-alone IPS can’t decompress, and thus cannot scan compressed content.

- **A Word on Data Leaks** – One of the biggest information security news items in the past 2 years is the leaking of confidential or sensitive data via applications (e.g., U.S. government – both agencies and contractors, pharmaceuticals, and retailers). In most cases, the applications that the data leaked across were expressly forbidden – unfortunately, their policies couldn’t be enforced with traditional firewalls and IPS. Given these high-profile security breaches, it is no wonder that organizations are starting to look to intrusion prevention to help protect organizations from these embarrassing incidents. (*Infonetics*).

A common theme here is the level of control needed to prevent these newer threats – controlling applications and content, decrypting SSL, unzipping content to look for threats– all of which goes well beyond what IPS traditionally does. A major limitation of IPS, despite all of the work to transition from IDS, is that it remains a negative security model, and is architected as such. Put more simply, IPS relies on a “find it and kill it” model – which doesn’t work very well for the types of control necessary to deal with many of these new threats that move over applications. Nor does it lend itself to an architecture and platform capable of decrypting and classifying all traffic.

New Enterprise Requirements for Intrusion Prevention

The current application and threat landscape dictates a new set of requirements for complete intrusion prevention. This includes the traditional set of IPS requirements – it is inappropriate in today's economic environment to propose even more network security appliance sprawl – but should also address the new types of threats organizations are seeing. These requirements, at a high level are: control, protection, performance, and support.

- **Control the Attack Surface** – One of the fundamental limitations of a traditional IPS is that it is reactive by nature – it sits and waits to see a threat and then block it. A better approach is to first limit traffic on the network to the applications (and even the features) that you have approved. This means that instead of allowing all the vulnerabilities of all the applications in the world on your network, you can limit the scope to the applications that you actually need and use. This allows the organization to instantly shrink the attack surface of the enterprise and prevent unnecessary exposures.

- **Prevent All Types of Threats** – Threats are no longer limited to traditional vulnerability exploits, and IPS solutions need to expand their horizon as well. This means detecting viruses, malware, botnets, dangerous URLs, phone-home behavior and a variety of attacks against clients in addition to preventing more traditional vulnerability exploits.

- **Prevent the Application-Enabled Threat** – In addition to looking for the threats themselves, we also must look within the hidden transmission vectors that traditional IPS has overlooked. This includes looking within tunneled applications, encrypted traffic, compressed traffic and files and preventing the unauthorized use of proxies and encrypted tunnels. The importance of this requirement can't be overstated – if your IPS can't see the threat, it won't be able to stop it.

- **Focus on Enablement** – While applications can be threats or at the very least, enable threats, we often can't simply completely block a given application if it has business value. Traditional IPS typically only has a notion of allow and block, so even in the rare instance that the IPS identifies an application, there is no concept of enablement. The new generation of IPS should have more granular controls that let security teams allow but control applications, such as limiting an app to certain users, controlling bandwidth usage, disabling certain application features and of course, cleaning the traffic of any and all threats.

- **Enterprise Performance** – Simply put, IPS must provide all of these requirements at multi-gigabits per second throughput and low latency – with real world traffic and with full scanning enabled to protect both servers AND clients.

- **Industry Leading Research** – The IPS vendor must support enterprise customers with leading edge research and rapid deployment of protections from new and evolving threats.

A final word on requirements might be a note on architecture and the future of network security. Gartner recently released a note on next-generation firewalls, providing specific advice for enterprises regarding moving from IPS to next-generation firewalls:

> - If you have not yet deployed network intrusion prevention, require NGFW capabilities of all vendors at your next firewall refresh point.
> - If you have deployed both network firewalls and network intrusion prevention, synchronize the refresh cycle for both technologies and migrate to NGFW capabilities.
> - If you use managed perimeter security services, look to move up to managed NGFW services at the next contract renewal.
>
> *Source: Gartner*

Palo Alto Networks Delivers

With its unique combination of application control, user control and threat prevention, Palo Alto Networks delivers the industry's best IPS solution, bar none. In recent IPS testing performed by NSS Labs, the Palo Alto Networks solution showed consistently stellar results including an outstanding IPS prevention rate (93.4%), 100% resistance to IPS evasion and all while maintaining the rated performance for the appliance. These tests simply provide the validation for what is the industry's best IPS solution based on control, protection, performance, and research/support.

Control. With regard to control, Palo Alto Networks next-generation firewalls have several advantages – first, it's a firewall, so it sees all traffic flowing across the trust boundary. Second, Palo Alto Networks' App-ID technology is the traffic classification engine of the firewall – meaning regardless of port, protocol, encryption, or evasive technique, App-ID classifies the application and governs it per policy. Palo Alto Networks' User-ID technology adds further control, enabling organizations to use enterprise directory user and group information in policy as well. Giving policy control of applications and users to IT and security staffs has significant benefits, not the least of which is a vastly simplified way to create and manage network security policy.

Protection. Recently validated as 93.4% effective in IPS tests performed by NSS labs, the Palo Alto Networks threat prevention suite integrates all of the key IPS and threat scanning techniques into a stream-based scanning engine. It also includes an ability to scan for certain types of confidential data (e.g., credit card numbers or custom regular expressions) in the same engine. Vulnerability exploits, buffer overflows, DoS attacks and port scans are detected along with confidential data (e.g., credit card numbers) by scanning the traffic only once, using proven threat detection and prevention (IPS) mechanisms including:

- Protocol anomaly-based protection detects non-RFC compliant protocol usage such as the use of overlong URI or overlong FTP login.

- Stateful pattern matching detects attacks across more than one packet, taking into account elements such as the arrival order and sequence.

- Statistical anomaly detection prevents rate-based DoS flooding attacks.

- Heuristic-based analysis detects anomalous packet and traffic patterns such as port scans and host sweeps.

- Other attack protection capabilities such as blocking invalid or malformed packets, IP defragmentation and TCP reassembly are utilized for protection against evasion and obfuscation methods employed by attackers.

Palo Alto Networks, like many IPS vendors, uses primarily vulnerability-facing signatures, and has thousands of them. The other important element of this is that Palo Alto Networks next-generation firewalls can scan SSL encrypted traffic (both inbound and outbound) and compressed content for threats. Given the amount of SSL-encrypted traffic in the enterprise, this is critical

Performance. Unlike traditional IPS solutions that force security teams to choose between security and performance, Palo Alto Networks actually provides full IPS protection while maintaining published threat prevention speeds. This unique performance is enabled by the Single Pass Parallel Processing (SP3) Architecture – which enables high-throughput (up to 5 Gbps), low-latency (less than 1 millisecond) network security, even while performing full content and threat scanning. Palo Alto Networks solves the performance problems that IPS has struggled with in the past with the SP3 architecture, which combines two complementary components:

- **Single Pass software:** Palo Alto Networks Single Pass software performs operations once per packet. As a packet is processed, networking functions, policy lookup, application identification and decoding, and threats and content scanning are all performed just once. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device. This Single Pass traffic processing enables very high throughput and low latency – with all security functions active. It also offers the additional benefit of a single, fully integrated policy, enabling simple, easier management of enterprise network security.
- **Parallel Processing hardware:** Palo Alto Networks next-generation firewalls use Parallel Processing hardware to ensure that the Single Pass software runs fast. First, Palo Alto Networks engineers designed separate data and control planes. This separation means that heavy utilization of one won't negatively impact the other. The second important element of the Parallel Processing hardware is the use of discrete, specialized processing groups that work in harmony to perform several critical functions: networking, security, content and threat scanning, and management.

The combination of Single Pass software and Parallel Processing hardware is completely unique in network security, and enables Palo Alto Networks next-generation firewalls to achieve very high levels of performance. The other, minor, but perhaps more practical point is that Palo Alto Networks next-generation firewalls have very high port density, making protecting large, increasingly segmented networks easier, and less expensive.

Research/Support. As mentioned previously, research and support is critical for customers: is the vendor knowledgeable and responsive enough to help organizations protect their networks? This is particularly challenging to measure. Given their ubiquity, examining Microsoft vulnerabilities are a good approximation for both. Palo Alto Networks has been credited with discovering more Microsoft vulnerabilities than any IPS vendor research team in the last 12 months. The next closest had half as many discoveries. The other aspect to examine is responsiveness. Using Conficker as an example, which targets the MS08-067 vulnerability, we can see that Palo Alto Networks released protection for that vulnerability hours after Microsoft announced it (Palo Alto Networks is part of the Microsoft Active Protections Program). Furthermore, Palo Alto Networks had the ability to recognize and block Conficker download traffic within days of the appearance of the first variant.

In summary, Palo Alto Networks next-generation firewalls deliver the control, protection, performance, and research and support that organizations need to defend against modern threats. To compare against traditional IPS, see the below table:

Requirement	**Palo Alto Networks NGFW**	**Traditional IPS**
Control Applications	Over 1,000 applications	Can treat a few "bad" applications like threats
Scan allowed traffic for threats	Yes, 1000s of signatures, across SSL-encrypted and compressed content	Yes, 1000s of signatures. Blind to SSL-encrypted and compressed content.
Real-world, Multi-Gbps Performance	Yes	Depends on the vendor
Research and Support	Class-leading – more Microsoft vulnerabilities discovered than any IPS vendor (in the last 12 months)	Lots of noise, little action – the best in-house IPS research team discovered 3 Microsoft vulnerabilities in the last 6 months. Some haven't done anything for 2 years.

Figure 1: Palo Alto Networks next-generation firewalls deliver, where IPS products cannot

The Future of Intrusion Prevention is a Next-Generation Firewall

The application and threat landscape has changed – with threats using evasive applications and encryption. Traditional IPS cannot control these new threat vectors. A new set of enterprise requirements for intrusion prevention has emerged, focusing on control, protection, performance, and research/support. Palo Alto Networks is uniquely positioned to deliver on these requirements, owing to strong control over users and applications, all of the relevant IPS techniques, a high-performance platform, and solid research and support – all of which enables enterprises to first control which applications run on their networks, and then scan the allowed applications for threats. Furthermore, Gartner has written that enterprises should migrate traditional standalone IPS deployments to next-generation firewalls, providing another indicator that the transition started with IDS moving to IPS is finishing with next-generation firewalls.