Palo Alto Networks Threat Prevention:
A Summary of IPS Test Results and Core Capabilities

A Note on the Data and Testing Methodology

Statements in this paper draw heavily upon the results of in-depth, hands-on testing of the Palo Alto Networks PA-4020 appliance performed by NSS Labs. NSS is an independent 3rd-party testing lab and is renown for their industry expertise in IPS testing and as the operators of the largest independent security lab in the world. NSS Labs tested the Palo Alto Networks solution against 1,179 live exploits in what was the industry's most comprehensive IPS test to date. The system was tested against a wide variety of traffic that varied by payload size, protocol, attack target and end-user delay time to ensure a reliable, real-world test bed. The full Palo Alto Networks product test report including the NSS testing methodology can be found here (*http://www.paloaltonetworks.com/literature/forms/nss-report.php*).

The Best Choice for IPS is the Next-Generation Firewall

Palo Alto Networks provides customers with the best intrusion prevention option in the industry based on effectiveness, performance and overall cost of the solution. Simply put, Palo Alto Networks offers leading-edge IPS functionality validated by extensive 3rd party testing at a cost per segment that is unrivaled by any IPS in the industry. The Palo Alto Networks solution also offers simple system configuration and high performance even with all IPS features enabled, meaning that for the first time, security teams can get the highest levels of network security without impacting the network operations team. Additionally, the system is supported by an unrivaled threat research team and vulnerability partnerships ensuring that the enterprise is continually protected through the never-ending changes in the threatscape for years to come.

In addition to these core IPS capabilities provides additional security abilities that go well beyond what any IPS today can provide. By leveraging application visibility and control, security teams can immediately reduce their exposure to threats by limiting network traffic to approved apps and use cases, while avoiding risks from unnecessary apps that are not approved for the network. Palo Alto Networks also has the ability to find threats hidden within application, SSL encrypted traffic and compressed files – immediately closing the loopholes that attackers use to avoid traditional IPS solutions.

---------- Proven IPS Quality ----------

- **Industry Leading IPS Effectiveness – 93.4% block rate and 100% Resistance to IPS Evasion Techniques**
- **Performance and Scalability – Maintains or exceeds stated datasheet performance even with all IPS enabled**
- **Simple IPS Tuning and Management**

---------- Long-Term IPS Value ----------

- **Reduced Attack Surface by Controlling Applications on the Network**
- **Prevention of Application-Enabled Threats**
- **Industry-Leading IPS Research**
- **Unrivaled TCO – Savings of between 40% and 84%**

Industry Leading IPS Effectiveness

The results of the NSS tests referenced above found that Palo Alto Networks accurately detected and blocked 93.4% of all of the 1,179 attacks, putting Palo Alto Networks easily in the uppermost echelon of IPS solutions based on core functionality. As a reference, the 2009 IPS group test found IPS block rates ranging from 17% to 89%. Additionally, Palo Alto Networks achieved a 97% block rate on attacks targeting end-users, an area where traditional IPS has typically seen very spotty results. Tests included all types of attack methodologies, applications and targets.

93.4 % IPS Effectiveness at 2,258 Mbps (115% of datasheet performance)

100% Resistance to IPS Evasion Techniques

In addition to its ability to protect the network from threats, Palo Alto Networks was also tested against a variety of IPS evasion techniques designed confuse or circumvent the IPS. The solution proved to be impervious to these techniques, continuing to detect and prevent all threats regardless of the type of evasion attempted.

> *"Resistance to known evasion techniques was perfect, with the Palo Alto Networks PA--4020 achieving a 100% score across the board in all related tests. IP fragmentation, TCP stream segmentation, RPC fragmentation, URL obfuscation, and FTP evasion all failed to trick the product into ignoring valid attacks. Not only were the fragmented and obfuscated attacks blocked successfully, but all of them were also decoded accurately."*
>
> *- NSS Lab report, July 2010*

Performance and Scalability

IPS systems are notoriously prone to degrading network performance in direct relation to the number of signatures that are enabled on the system, which almost invariably leads to a conflict between the security and network operations teams. In NSS lab tests, the Palo Alto Networks delivered an industry-best 93.4% block rate, while maintaining 115% of the stated datasheet IPS performance for the appliance.

115% of Stated Datasheet Performance With Full IPS Protection

The NSS testing performed baseline accuracy and performance tests on the Palo Alto Networks solution in its "out of the box" configuration for comparison with the system in its "fully loaded" configuration where it was set to block all known intrusions. The Palo Alto Networks solution proved to be remarkably steady with only small changes in top-end performance based on changes to the IPS configuration, meaning that staff can confidently check for the full complement of threats while preserving network performance.

- **Connections and Transactions per second** – Palo Alto Networks maintained **98%** of baseline
- **Megabits per second** – Palo Alto Networks maintained **89%** of baseline

Simple IPS Tuning

IPS configuration is often a complex, time-consuming task requiring considerable staffing cycles and ongoing maintenance. NSS strongly recommends that customers tune their IPS systems and historically has found that customers who failed to tune the solution could miss 44% of detectable attacks. NSS found the Palo Alto Networks was incredibly easy to tune and "consisted of changing just 3 settings within the policy". This makes Palo Alto Networks not only powerful, but also operationally practical to deploy, ensuring a fast return on the investment.

> *"…rapid tuning consisted of changing just three settings within the policy"*
>
> *- NSS Lab report, July 2010*

Reducing the Intrusion Attack Surface with Application Control

In addition to best-of-breed IPS capabilities, Palo Alto Networks next generation firewalling delivers the industry's most fundamental reduction of enterprise risk in more than a decade. For the first time, security teams can limit traffic to approved applications and use cases, while automatically blocking unapproved or risky applications regardless of evasive tactic, encryption or tunneling behavior. This positive control model lets security teams immediately negate the risk of the universe of applications that provide no business value, while retaining the freedom to enable enterprise initiatives and empowering network users. This provides Palo Alto Networks customers with, quite literally, the best of both worlds – a firewall that fundamentally changes the threat profile of the organization, backed by a best-in-class IPS to thoroughly and reliably prevent active threats in the allowed traffic classes.

Preventing the Application-Enabled Threat

While detecting applications is a good start, it is also critically important to understand how attackers use applications to circumvent traditional IPS and security infrastructure. For example, many applications can tunnel other applications, applications can use SSL to avoid inspection, compressed HTTP or zipped files can hide threats, and remote desktop and proxy applications can create blind spots where traditional IPS can't see. Palo Alto Networks uses its unique App-ID capabilities to recognize all of these communications and then detect and prevent threats that are hidden within. Palo Alto Networks is the only solution to provide this protection and as such is the only solution to provide true IPS on real-world, modern traffic.

Industry Leading IPS Research

In addition, to gaining access to the best IPS available today, Palo Alto Networks customers are uniquely positioned for the future with protection from one of the most prolific and innovative security research teams in the industry. For more than a year, Palo Alto Networks internal threat researchers have discovered more than twice as many Microsoft vulnerabilities than any other research team and regularly released protections for the new threats within hours of their announcement. The team was also recently credited for discovering a series of new Adobe vulnerabilities and continues to add new threat and application signatures on a daily basis.

Unrivaled Value and TCO

Whether in a data center, gateway or a remote office, Palo Alto Networks offers remarkable cost savings when compared to other similarly sized IPS appliances. Depending on the appliances involved, a comparison of Palo Alto Networks, Tipping Point and IBM appliances showed that customers could save between 24% and 86% in IPS costs on a per protected segment basis. The chart below provides a summary of all appliances, and additional details and specific model comparisons are available from your Palo Alto Networks partner or sales representative.