# Integrated Threat Prevention

Fully integrated real-time threat prevention protects enterprise networks from a wide range of threats, complementing the policy-based application visibility and control that the Palo Alto Networks next-generation firewalls deliver.

- Proven protection from network and application vulnerability exploits (IPS), viruses and spyware.

- Protection delivered in a single stream-based scan, resulting in high throughput and low latency.

- Single policy table reduces the management overhead associated with policy creation to block threats, control applications and limit non-work related web activity.
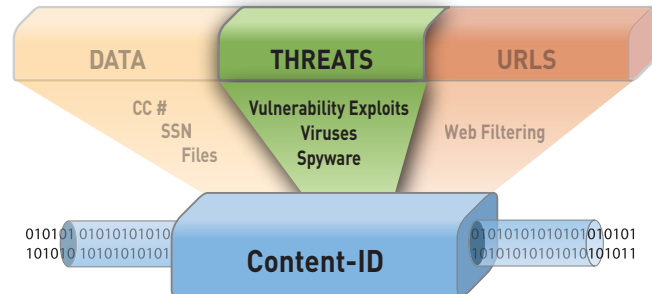
Today enterprise networks and their users are under attack from an ever-expanding universe of threats, malware, and vulnerabilities. More and more of these threats are focused on financial gain as opposed to notoriety, and hackers have learned to use evasive applications, tunneling and encryption to avoid detection by traditional IPS solutions. To make matters worse, many organizations have resorted to the habit of "see a security problem, buy an appliance", leading to a lack of coordination, poor visibility, and poor performance. This has left us with a dangerous situation, where our security solutions are increasingly fractured and difficult to manage, while the hackers are increasingly adept at penetrating them.

Palo Alto Networks' next-generation firewall provides administrators with a two-pronged solution to threat prevention, each of which are industry firsts. Using App-ID, the first firewall traffic classification engine to identify applications irrespective of port, protocol, evasive tactic or SSL. This means administrators can immediately shrink the attack surface of the enterprise by identifying all traffic at the application level and limiting traffic to approved applications. Traffic from approved applications is then fully inspected and protected by an industry leading threat prevention suite, including a proven IPS* as well as stream-based virus and malware prevention. The solution offers the ability to scan within SSL encrypted content and compressed files to ensure reliable threat prevention and also leverages a unified signature format, allowing all threat prevention, content scanning and malware detection to be performed in a single scan of traffic.

Control the Application, Block the Threat

The first step towards eliminating threats from enterprise networks is to regain visibility and control over the applications traversing the network with App-ID, a patent-pending traffic classification technology that determines exactly which applications are traversing the network irrespective of port, protocol, SSL or evasive technique. The identity of the application generated by App-ID plays two key roles in the threat detection solution.

The first role is to help administrators reduce the attack surface by enabling them to make a more informed decision about how to treat the application via policy. Undesirable applications such as P2P file sharing, external proxies or circumventors, can be summarily blocked. Applications that are permitted can be controlled and inspected at a very granular level for viruses, spyware and vulnerability exploits. The second threat prevention role that App-ID plays is it improves the breadth and accuracy by decoding the application, then reassembling and parsing it to know exactly where to look for different types of threats.

Scan for all Threats in a Single Pass

Palo Alto Networks' threat prevention engine represents an industry first by detecting and blocking both malware and application vulnerability exploits in a single pass. Traditional threat prevention technologies require two, sometimes three scanning engines which adds significant latency and dramatically slows throughput performance. Unlike these solutions Palo Alto Networks leverages a uniform signature format for all threats and malware and ensures fast processing by performing all analysis in a single integrated scan. The uniform signature format eliminates many redundant processes common to multiple scanning engine solutions (TCP reassembly, policy lookup, inspection, etc.) and in so doing, improves performance. Stream-based scanning means that the scanning process begins as soon as the first packets of the file are received, thereby eliminating the latency issues associated with the traditional buffer-based approaches.

Validated by NSS Labs*

Palo Alto Networks has been validated by NSS Labs in live in-depth intrusion testing covering more than 1,000 live exploits. Key results include:

- 93.4% Effectiveness at Blocking Attacks
- 100% Resistance to IPS Evasion
- Scalability - Full IPS Protection at Rated Speed
- Simple IPS Tuning

Industry Leading Intrusion Prevention (IPS)

The Palo Alto Networks IPS prevents enterprises from all types of threats including vulnerability exploits, buffer overflows, DoS/DDoS attacks and port scans using proven threat detection and prevention (IPS) mechanisms:

- Protocol decoder-based analysis statefully decodes the protocol and then intelligently applies signatures to detect vulnerability exploits.

- 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.

- Custom vulnerability or spyware phone home signatures that can be used in the either the anti-spyware or vulnerability protection profiles.

The intrusion prevention engine is supported by a team of seasoned threat signature developers that work closely with Microsoft as part of the Microsoft Active Protections Program (MAPP). As an inaugural member of MAPP, Palo Alto Networks is provided priority access to Microsoft's monthly and out-of-band security update release. By receiving vulnerability information earlier, Palo Alto Networks can develop signatures and deliver them to customers in a synchronized manner, thereby ensuring that customers are protected. In addition to receiving vulnerability information from Microsoft for the purposes of signature development, Palo Alto Networks performs its own, ongoing research and has been credited with the discovery of numerous critical and high severity vulnerabilities within Microsoft operating systems and applications. Signature updates are delivered on a weekly schedule or on an emergency basis.

Network Antivirus: Blocking Viruses, Spyware and Trojans

Inline antivirus protection detects and blocks most types of malware at the gateway. Antivirus protection leverages the uniform signature format and stream-based engine to protect enterprises from millions of malware variants. Stream-based scanning helps protect the network without introducing

Stream-based Scanning

File-based Scanning
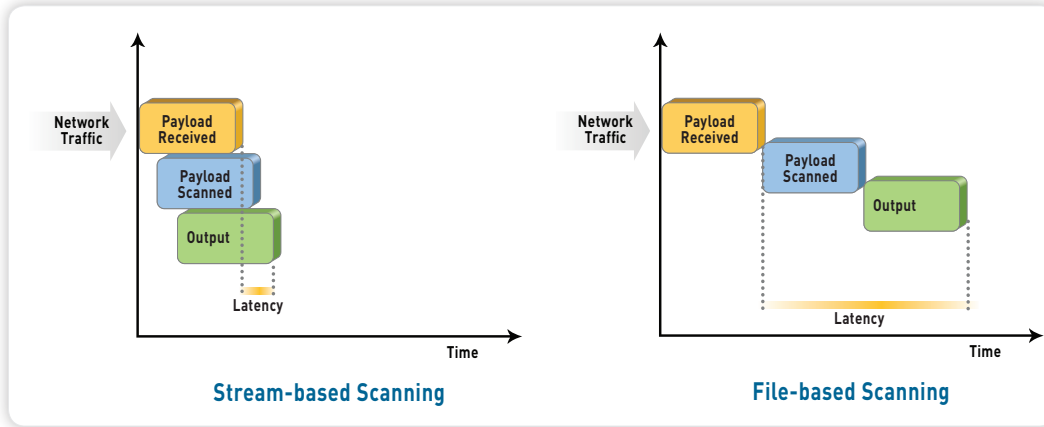
Stream-based scanning
Stream-based scanning helps minimize latency and maximize throughput performance.

significant latency – which is the problem with network antivirus offerings that rely on proxy-based scanning engines. Proxy-based network antivirus solutions have historically lacked the performance capacity to be widely deployed in a real-time environment (e.g., web applications) because they pull the entire file into memory before the scanning process began. Stream-based virus scanning inspects traffic as soon as the first packets of the file are received, eliminating the performance and latency issues associated with the traditional proxy-based approach. Key antivirus capabilities include:

- Protection against a wide range of malware such as viruses, including HTML and Javascript viruses, spyware downloads, spyware phone home, Trojans, etc.
- Inline stream-based detection and prevention of malware embedded within compressed files and web content.
- Leverages SSL decryption within App-ID to block viruses embedded in SSL traffic.

Signatures for all types of malware are generated directly from millions of live virus samples delivered to Palo Alto Networks by leading third-party research organizations around the world. The Palo Alto Networks threat team analyzes the samples and quickly eliminates duplicates and redundancies. New signatures for new malware variants are then generated (using our uniform signature format) and delivered to customers through scheduled daily or emergency updates.

Hardware Enabled

Unlike many current solutions that may use a single CPU or an ASIC/CPU combination to try and deliver enterprise performance, Palo Alto Networks utilizes a purpose-built platform that uses dedicated processing for threat prevention along with function-specific processing and dedicated memory

for networking, security and management. Using four dedicated types of processing means that key functions are not competing for processing cycles with other security functions, as is the case in a single CPU hardware architecture. The end result is low latency, high performance throughput with all security services enabled.

Threat Prevention Throughput

MODEL	THROUGHPUT		MODEL	THROUGHPUT
PA-4060	5 Gbps		PA-2050	500 Mbps
PA-4050	5 Gbps		PA-2020	200 Mbps
PA-4020	2 Gbps		PA-500	100 Mbps

World Class Research and Partnerships

The Palo Alto Networks threat research team is a world-class research organization dedicated to the discovery and analysis of threats, applications and their respective network behavior. Through internal research, third party relationships with software vendors (e.g., Microsoft) and the same research organizations used by other leading security vendors, customers are assured that Palo Alto Networks is providing them with the best network threat protection and application coverage.

ORDERING INFORMATION	YEAR 1 PART NUMBER	RENEWAL PART NUMBER
PA-4060 Threat prevention subscription	PAN-PA-4060-TP	PAN-PA-4060-TP-R
PA-4050 Threat prevention subscription	PAN-PA-4050-TP	PAN-PA-4050-TP-R
PA-4020 Threat prevention subscription	PAN-PA-4020-TP	PAN-PA-4020-TP-R
PA-2050 Threat prevention subscription	PAN-PA-2050-TP	PAN-PA-2050-TP-R
PA-2020 Threat prevention subscription	PAN-PA-2020-TP	PAN-PA-2020-TP-R
PA-500 Threat prevention subscription	PAN-PA-500-TP	PAN-PA-500-TP-R

* Testing by NSS Labs performed July, 2010. The full report can be found on the Palo Alto Networks website.

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.320.4788
          408.738.7700
www.paloaltonetworks.com