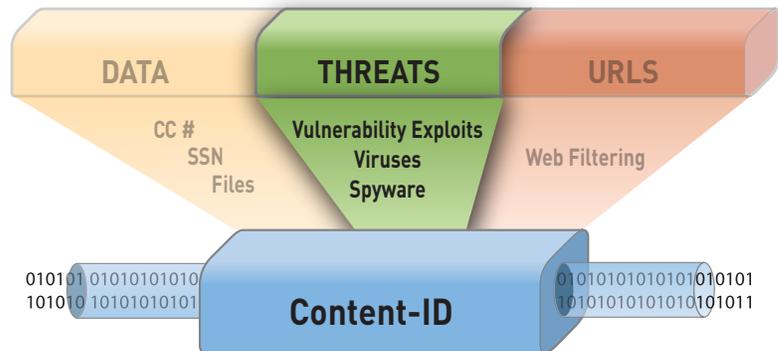


Integrated Threat Prevention

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, spyware and unknown threats in full application context.
- 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's 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 a dangerous situation, where security solutions are increasingly fractured and difficult to manage, while the hackers are increasingly adept at penetrating them.

Palo Alto Networks offers a unique and modern approach to threat prevention that begins by proactively reducing the vulnerability of the network, and then fully inspecting all allowed traffic for threats. Palo Alto Networks lets organizations instantly and dramatically reduce the attack surface of their networks by preventing or limiting risky or unnecessary applications or features. This includes a variety of applications and technologies that are regularly used by attackers to hide their attacks such as proxies, encryption and encrypted tunnels.

Next, Palo Alto Networks takes the unique step of fully inspecting all allowed traffic irrespective of port or evasion attempt. This enables Palo Alto Networks to catch all threats even if they are transmitted over non-standard ports or tunneled within other applications or protocols. A single unified threat engine performs IPS, stream-based anti-virus prevention, and blocking of unapproved file types and data. Additionally, the cloud-based WildFire™ engine identifies unknown and targeted malware and exploits that may have no known signature. This gives organizations the unique ability to reduce their exposure, ensure visibility into evasive traffic and protect from all types of threats in a single pass of traffic.

Control the Application, Block the Threat

Applications are integral to virtually all cyber threats. In some cases, the application is the threat, such as a botnet communicating via a peer-to-peer network. In other cases the threat is enabled by an application that provides a vector for the threat or obscuring it from security solutions, such as an SSL encrypted browser session that obscures the delivery of malware. By leveraging App-ID™, Palo Alto Networks provides visibility into all applications, where they can be controlled by policy and fully inspected for threats. Undesirable applications such as P2P file sharing, external proxies or circumventors, can be summarily blocked, or limited to the few users with a valid use case. Additionally, staff can easily restrict applications by their ability to tunnel other applications, transfer files, or history of being used by malware. These controls can instantly reduce the attack surface of the enterprise. Applications that are permitted can be controlled and inspected at a very granular level for viruses, spyware and vulnerability exploits. App-ID enhances the threat prevention logic through the use of more than 100 application and protocol decoders, which further reveal 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 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.

Independent Vulnerability Research

Unlike other security vendors who source their signatures from 3rd Parties, Palo Alto Networks performs all IPS research in-house by Palo Alto Networks researchers. Over the past 4 years, this elite team has discovered more Microsoft and Adobe Flash vulnerabilities than any other security vendor research team.

Additionally, the IPS solution has been validated by NSS Labs and received their highest rating of 'Recommended' based on the high observed high block rate, performance, resistance to evasion and overall value.

Palo Alto Networks researchers are active in the threat prevention community, working closely with



Proven IPS:
Validated by
NSS Labs

software vendors, both informally and formally, through programs such as the Microsoft Active Protections Program (MAPP). As a member of MAPP, Palo Alto Networks receives priority access to Microsoft's monthly and out-of-band security update releases. 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.

The Palo Alto Networks IPS protects organizations 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 either the anti-spyware or vulnerability protection profiles.

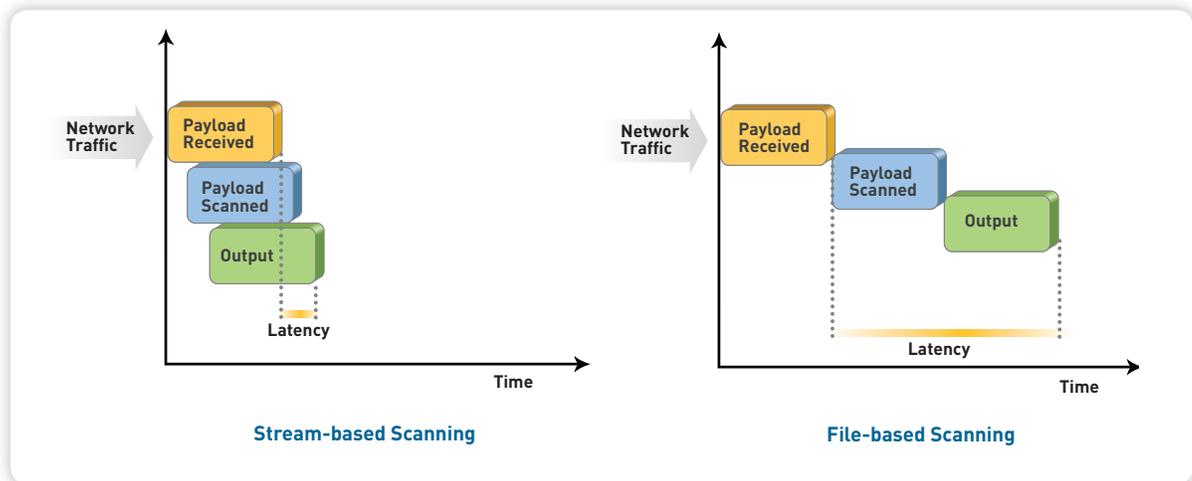
In addition to these traditional IPS capabilities, Palo Alto Networks also provides the unique ability to detect and block threats on non-standard ports. Traditional IPS solutions invoke their signatures based on the observed port number, which is a serious flaw given that applications no longer adhere to traditional port conventions. By leveraging App-ID, which identifies all traffic, on all ports, the threat prevention engine never loses sight of threat regardless of port evasion.

Network Antivirus: Stream-based Malware Prevention

Inline antivirus protection detects and blocks malware at the gateway before it ever reaches the target host. Antivirus protection leverages the same uniform signature format used for IPS. The stream-based scanning engine protects the network without introducing significant latency—which is a serious drawback of 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

Stream-based scanning

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



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 PDF, 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 collected by Palo Alto Networks from several sources including a worldwide network of honeypots deployed around the world, from the WildFire malware analysis service and from other 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.

Drive-by Download Protection

Drive-by downloads have become the preferred method for hackers to deliver malware to unsuspecting users. Instead of a user clicking on an attachment in an email, users can become infected via a drive-by-download simply by visiting a webpage with an infected image. Often the user and even the owner of the website may be unaware that the site has been compromised. Palo Alto Networks can look within the application session, see that a download is taking place and verify with the user if the file is an approved download.

DNS Sinkholing and Monitoring

DNS traffic exists in nearly every organization, creating an overwhelming ocean of data security teams often ignore, or do not have the tools to properly analyze. Knowing this, cyber attackers are increasingly abusing DNS to mask

their command-and-control (C2) activity in order to deliver additional malware or steal valuable data. Malicious domain names controlled by attackers enable the rapid movement of command-and-control centers from point to point, bypassing traditional security controls such as blacklists or web reputation. Palo Alto Networks addresses this by:

- Allowing opt-in passive DNS monitoring, creating a database of malicious domains and infrastructure across our global customer base. This intelligence is consumed by PAN-DB URL filtering, DNS-based command-and-control signatures, and WildFire to prevent future attacks.
- Enabling customers to create a local DNS sinkhole, re-directing malicious queries to an address of your choosing to quickly identify and block compromised hosts on the local network.

Botnet Detection and Prevention

Protecting the network from botnets has proven to be a very difficult challenge for both IT security teams and the industry at large. Botnets leverage many techniques to remain undetected including the ability to use applications to remain hidden in transmission as well as to update the botnet itself, making it more difficult to detect with a signature. Palo Alto Networks provides a unique ability to find and control botnets by using a combination of elements including application identification, threat signatures and the analysis and correlation of unusual traffic patterns.

- Control botnet vectors. Organizations can use the application control enabled by App-ID to deploy firewall policies that control those applications that may be used by botnets as propagation channels or for command and control. Examples include:
 - Block P2P and IM applications such as MSN, which have been known to propagate the Mariposa botnet.
 - Block known botnet command and control applications (e.g., IRC)
- Control, inspect and monitor those applications that are emerging as command and control channels (Twitter, Gmail, Google Docs).

- Prevent the propagation of known botnets. The threat prevention engine can identify and block the download as well as the command and control traffic for known botnets such as Mariposa, Dark Energy and Rustock.
- Pinpoint bot-infected machines. The Palo Alto Networks solution integrates a range of datapoints to identify machines on the network that may be infected by both known, unknown or polymorphic botnets. These factors include tracking of unknown applications, IRC traffic, malware sites, dynamic DNS, and newly created domains is analyzed, resulting in a report that displays a list of potentially infected hosts that can be investigated as members of a botnet.

WildFire: Protection From Targeted and Unknown Threats

Advanced cyber threats have evolved to highly evasive and adaptable network applications that allow hackers to launch increasingly sophisticated and targeted attacks. This new breed of threats are at the heart of many of today's most sophisticated intrusions—enabling attackers to gain a foothold within the enterprise from which they can dig deeper into the network, control their attack and steal information. As threats have become more powerful, they have also become more targeted and customized for a particular network, helping them avoid traditional signature-based security solutions. To meet this challenge, Palo Alto Networks has developed WildFire, which identifies unknown malware, zero-day exploits, and Advanced Persistent Threats (APTs) in a cloud-based virtual execution environment. This scalable service automatically disseminates protections in near real-time to help security teams meet the challenge of advanced cyber attacks:

- **Integration of Firewall and the Cloud:** WildFire extends customer's Palo Alto Networks next-generation firewall capabilities with no additional hardware. The in-line firewall captures and analyzes unknown files in a cloud-based virtual malware analysis environment, discovering advanced threats, and performing automated enforcement while maintaining high network throughput and low latency.
- **WildFire Virtualized Sandbox:** The WildFire service is an advanced, virtual malware analysis environment, purpose-built for high fidelity hardware emulation, analyzing suspicious samples as they execute. The cloud-based service detects and blocks targeted and unknown malware, exploits, and outbound C2 activity by observing their actual behavior, rather than relying on pre-existing signatures.
- **Automated Signature Generator:** When an unknown file is identified as malicious, WildFire automatically generates protections and delivers them to all WildFire customers globally in as little as 30 minutes.

- **Deep Visibility and Analysis:** WildFire users receive integrated logs, analysis, and visibility into WildFire events in the Palo Alto Networks management interface, Panorama, or the WildFire portal. This includes the ability to see all behaviors of the malicious file, the user that was targeted, the application that delivered the threat, and all URLs involved in delivery or phone-home of the malware or exploit.

Behavioral Botnet Report

In addition to the direct analysis of malware in WildFire, the Palo Alto Networks solution also includes the ability to identify the presence of modern malware through the monitoring and correlation of network traffic. The behavioral botnet report looks for a variety of tell-tale signs of a botnet infection such as the presence of unknown application traffic, IRC traffic, repeated attempts to download files and connections to newly registered domains. The report leverages User-ID™ to specifically identify the specific user that is infected, along with the key factors that contributed to the analysis.

Hardware Enabled

Unlike many current solutions that may use a single CPU or an ASIC/CPU combination to try and deliver multi-Gbps 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-5060 | 10 Gbps | PA-3050 | 2 Gbps |
| PA-5050 | 5 Gbps | PA-3020 | 1 Gbps |
| PA-5020 | 2 Gbps | PA-2050 | 500 Mbps |
| PA-4060 | 5 Gbps | PA-2020 | 200 Mbps |
| PA-4050 | 5 Gbps | PA-500 | 100 Mbps |
| PA-4020 | 2 Gbps | PA-200 | 50 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.



the network security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

Copyright ©2014, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN_DS_ITP_011314