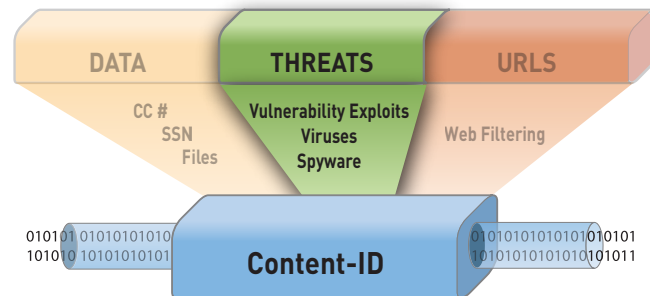


# Integrated Threat Prevention

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.

- Prevents a wide range of threats including network and application vulnerability exploits (IPS), viruses and spyware.
- Leverages the application identity generated by App-ID™ to eliminate undesirable or risky applications resulting in a reduction of the threat footprint.
- Unified policy management reduces management overhead associated with policy creation to block threats, control applications and limit non-work related web activity.
- Single pass architecture scans all the traffic only once and is stream-based, eliminating the need to buffer or proxy the traffic, resulting in improved throughput and reduced latency.



Today, enterprise users are armed with high speed Internet connectivity and a browser which gives them immediate access to the latest and greatest web applications. Unbeknownst to most users is the fact that many of these new applications are threat vectors that expose enterprise networks to business risks including network downtime, data loss, and increased operational expenses.

Many of these new threats are focused on financial gain, as opposed to notoriety, which means that stealth and ingenuity are a priority in achieving the end goal. Amplifying the challenge that security managers face the battle against threats is the fact that their security infrastructure is built largely on the premise of “see a security problem, buy an appliance.” Unfortunately, the lack of coordination between solution functionality, management interface inconsistencies, and poor performance have resulted in less than stellar success for these disparate offerings. More importantly, this silo-based security model does not address the fact that attackers are taking full advantage of the unchecked access to thousands of applications that end-users currently enjoy.

Palo Alto Networks’ next-generation firewall provides security administrators with a two pronged solution to threat prevention. First, identify and control the applications traversing the network to reduce the threat footprint, then inspect the permitted applications for viruses, spyware, and vulnerability exploits in a single pass.

### 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 application identity, combined with its description, its characteristics, and knowledge of who is using it enables security administrators to make a more informed decision about how to treat the application via policy. Applications that may have no business use on enterprise networks, P2P file sharing or circumventors for example, can be summarily blocked. Applications that are permitted can be identified and controlled at a very granular level and then inspected 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.

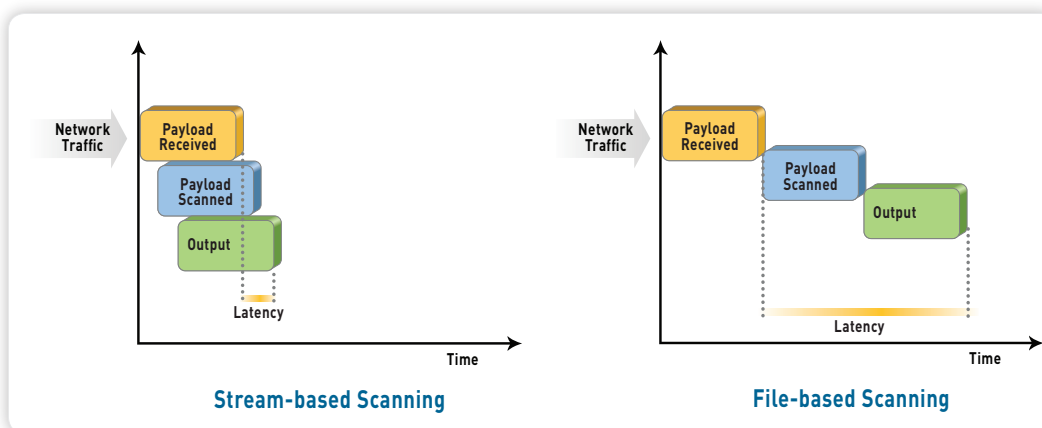
Whereas traditional port-based solutions use a single classification technique (protocol/port) to identify traffic, App-ID inspects all of the traffic passing through the firewall using one or more of these techniques – application protocol detection and decryption, application decoding, application signatures, and heuristic analysis – to quickly identify the application associated with each packet stream. By looking at the application, and not solely the port or protocol, App-ID is able to identify applications that have typically been able to bypass security.

### Single Pass Architecture: Scan it Once, Scan it All

Palo Alto Networks threat prevention engine is based on a single pass architecture that combines several innovative features to scan all the traffic for viruses, spyware and vulnerability exploits in a single pass. Application traffic flowing through the threat prevention engine is inspected and if an attack is detected, the appropriate response is taken, as defined in the policy. Traffic is normalized to eliminate invalid packets, and TCP reassembly and IP de-fragmentation ensures the utmost accuracy and protection despite attack evasion techniques employed.

- **Uniform signature format:** Rather than use a separate set of scanning engines and signatures for each type of threat, Palo Alto Networks uses a uniform threat engine and signature format to detect and block a wide range of malware while dramatically reducing latency.
- **Stream-based threat scanning:** Virus, spyware, and vulnerability prevention is performed through the use of stream-based scanning, a technique that begins scanning as soon as the first packets of the file are received, as opposed to waiting until the entire file is loaded into memory to begin scanning. This eliminates the performance and latency issues with the traditional proxy approach by receiving, scanning, and sending traffic to its intended destination immediately without having to first buffer and then scan the file.

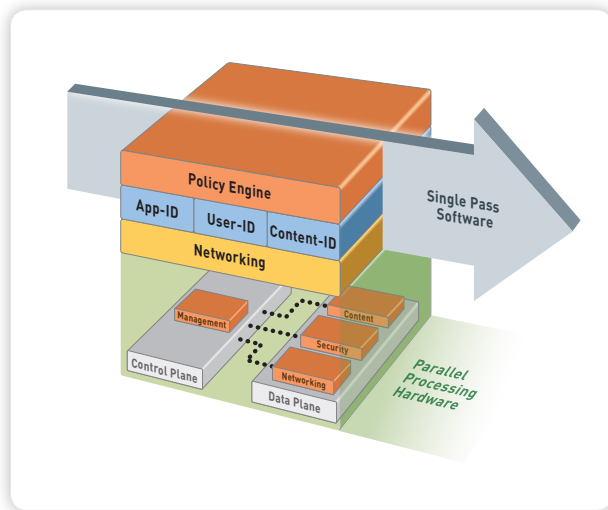
In contrast, traditional file-based AV engines start scanning only after a complete file is received and buffered into memory, where files are typically held until the scanning is finished and deemed to be clean. Traditional file-based threat prevention introduces significant performance delays and latency, and can often result in a timed-out connection while waiting for the file to fully transfer and be scanned.



#### Stream-based scanning

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

- **Hardware enabled:** Unlike many current solutions that may use a single CPU or an ASIC/CPU combination to try and deliver adequate performance, Palo Alto Networks utilizes a purpose-built platform, designed to deliver maximum throughput. The threat prevention engine takes full advantage of the single pass parallel processing architecture by using a uniform signature format and stream-based scanning to inspect traffic in a single pass. Low latency, high performance throughput with all security services enabled is achieved through the use of function-specific processing and dedicated memory for networking, security, management and threat prevention. Specifically, the threat prevention engine is accelerated by a dedicated processor, not a general purpose, shared CPU that is competing for processing cycles with other security functions. The combination of dedicated processing, and a single pass architecture means that latency is minimized and throughput maximized.



**Single pass parallel processing architecture maximizes threat prevention throughput and minimizes latency.**

- **Network and application vulnerability exploit prevention:** Incorporated into the uniform signature format is a set of intrusion prevention system (IPS) features that block known and unknown network and application-layer vulnerability exploits from compromising and damaging enterprise information resources. Vulnerability exploits, buffer overflows, DoS attacks and port scans are detected along side viruses and spyware 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.

**World Class Research and Partnerships**

The Palo Alto Networks threat prevention engine is backed by a worldwide research team who are active in the threat prevention community and are credited with the discovery of critical severity threats over the past two years. In addition to the dedicated internal resources, Palo Alto Networks is an inaugural member of the Microsoft Active Protections Program (MAPP) which provides access to Microsoft Corp.’s monthly security update release. By receiving vulnerability information earlier, Palo Alto Networks can provide customers with timely updates to the threat prevention engine.

**ORDERING INFORMATION**

- PA-4060 Threat prevention subscription
- PA-4050 Threat prevention subscription
- PA-4020 Threat prevention subscription
- PA-2050 Threat prevention subscription
- PA-2020 Threat prevention subscription
- PA-500 Threat prevention subscription

**YEAR 1 PART NUMBER**

- PAN-PA-4060-TP
- PAN-PA-4050-TP
- PAN-PA-4020-TP
- PAN-PA-2050-TP
- PAN-PA-2020-TP
- PAN-PA-500-TP

**RENEWAL PART NUMBER**

- PAN-PA-4060-TP-R
- PAN-PA-4050-TP-R
- PAN-PA-4020-TP-R
- PAN-PA-2050-TP-R
- PAN-PA-2020-TP-R
- PAN-PA-500-TP-R



**Palo Alto Networks**  
 232 E. Java Drive  
 Sunnyvale, CA. 94089  
 Sales 866.207.0077  
 www.paloaltonetworks.com

Copyright ©2009, 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-OS 3.0, June 2009.

840-000004-00A