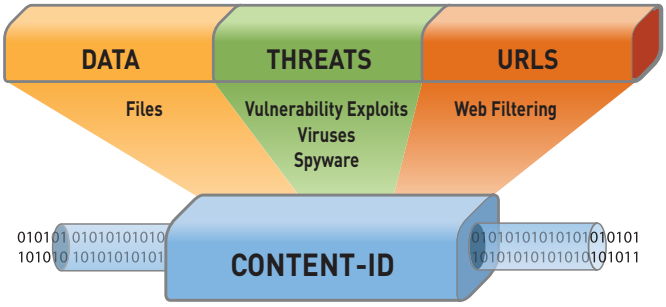
Content-ID

Content-ID enables customers to apply policies governing content traversing the network. This includes limiting unauthorized file transfers, detecting and blocking a wide range of threats and controlling non-work related web surfing.



- Protects against a broad range of malware including spyware, worms, viruses and vulnerability exploits
- Integrated policy management enables rapid policy creation and deployment
- Optimized scanning process means traffic is scanned only once, regardless of which Content-ID features are enabled

Palo Alto Networks next-generation firewalls enable policy-based visibility and control over applications, users and content using three unique identification technologies: App-ID, User-ID and Content-ID. The accurate identification of the application by App-ID solves only part of the visibility and control challenge that IT departments face with today's Internet-centric environment. Inspecting permitted application traffic becomes the next significant challenge and one that is addressed by Content-ID.

Content-ID melds stream-based scanning, a uniform threat signature format, and a comprehensive URL database with elements of application visibility to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing. Content-ID works in concert with App-ID, leveraging the application identity to help make the content inspection process more efficient while dedicated hardware and multiple banks of RAM help maximize throughput.

paloalto NETWORKS

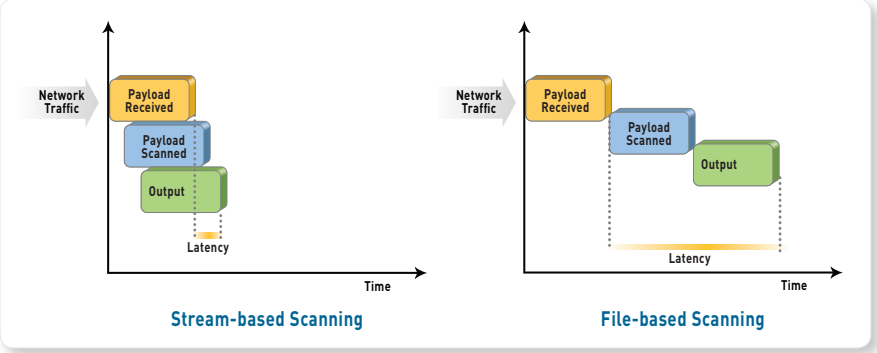
Threat Prevention

Enterprise networks are rife with a new class of application that can dynamically hop ports, re-use other ports, emulate other applications or tunnel inside SSL to avoid detection by most security solutions. Evasive applications have not gone unnoticed by attackers as they increasingly use these invisible applications to transport threats past the firewall. Content-ID leverages several innovative features to address the changes in the threat landscape and prevent spyware, viruses, and application vulnerabilities from penetrating the network.

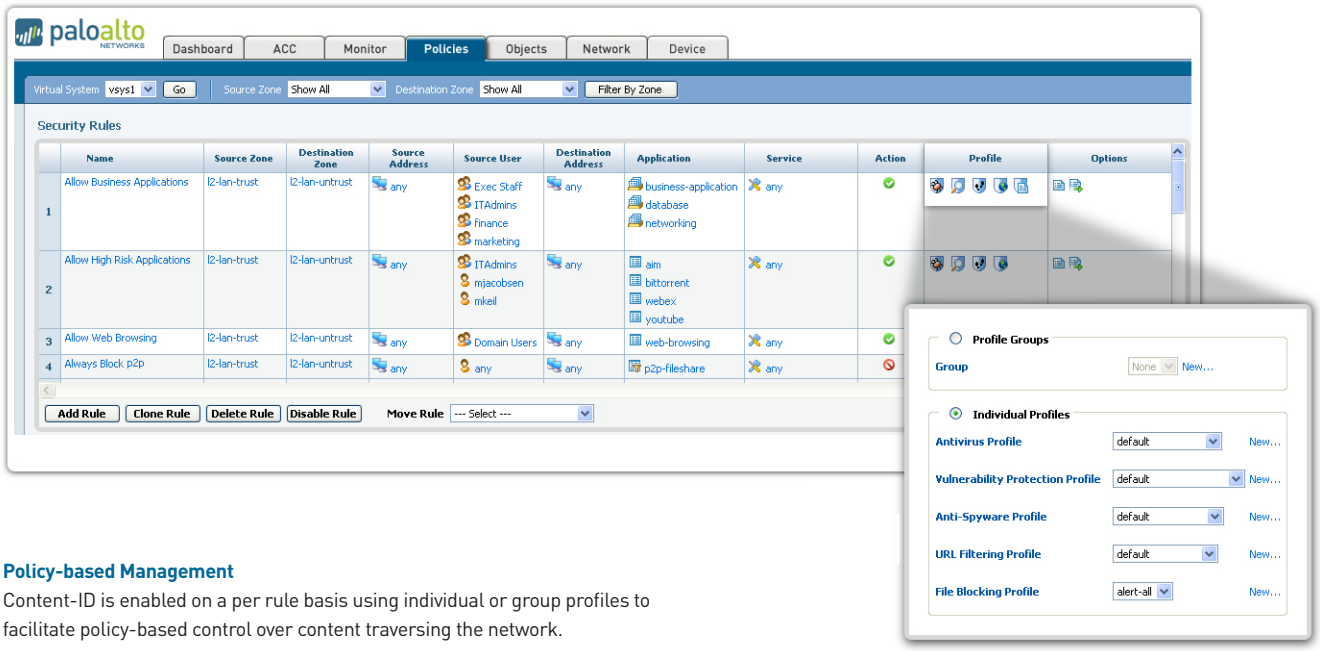
- **Application decoder:** The key traffic classification component within App-ID that enables Content-ID to more accurately identify and block threats is the application decoder. Content-ID takes streams of application data that has been reassembled and parsed by the application decoder, and inspects that stream for specific threat identifiers, responding to the threat based on the security policy.
- **Stream-based virus scanning:** Virus and spyware 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 means that performance and latency issues are minimized by receiving, scanning, and sending traffic to its intended destination immediately without having to first buffer and then scan the file.
- **Uniform threat signature format:** Rather than use a separate set of scanning engines and signatures for each type of threat, Content-ID leverages a uniform threat engine and signature format to detect and block a wide range of malware including viruses, spyware, and vulnerability exploits in a single pass.
- **Vulnerability attack protection:** Utilizing application and protocol decoder-based analysis in conjunction with anomaly and heuristic-based protection, Content-ID prevents network attacks on vulnerable applications and operating systems. Content-ID normalizes traffic to eliminate invalid packets, and performs TCP reassembly and IP de-fragmentation to ensure the utmost accuracy and protection despite any attack evasion techniques.

URL Filtering

Complementing the threat prevention and application control capabilities is a fully integrated, on-box URL filtering database that enables IT departments to monitor and control employee web surfing activities. With a fully integrated URL filtering database, administrators can apply more granular web browsing policies, complementing the application visibility and control policies and safeguarding the enterprise from a full spectrum of legal, regulatory, productivity and resource risks. URL filtering visibility and policy controls can be tied to specific users through the transparent integration with Microsoft's Active Directory (AD) with additional insight provided through customizable reporting and logging.



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



Policy-based Management

Content-ID is enabled on a per rule basis using individual or group profiles to facilitate policy-based control over content traversing the network.

File Transfer Control

File blocking controls within Content-ID enables organizations to stop the flow of a wide range of file types by looking deep within the payload to identify the file type (as opposed to looking only at the file extension). File blocking by type complements the ability to control file transfer functionality within some of the applications identified by App-ID. The combination of the two elements gives administrators more granular control over file-based content moving in and out of the network which results in a reduction of risk associated with unauthorized file and data transfer.

Log Correlation and Reporting

Powerful log filtering enables administrators to quickly investigate security incidents by correlating threats with applications and user identity. The log viewer enables an administrator to click on a cell value to immediately create a filter that can be narrowed down further by combining multiple criteria using an expression builder and additional log fields, even if they are not visible in the log viewer. To tie the user identity to the threat, the log viewer leverages the integration with Active Directory. Log results can be exported to a CSV file for offline archival or further analysis.

Reporting is enabled through a set of predefined reports that can be customized, pulling data from any of the log databases and then saving them for future use. Once the desired report is created, it can be configured to run on a regular basis, emailing a set of PDF reports or exporting them to CSV or PDF.

Performance and Deployment Flexibility

Palo Alto Networks next-generation firewalls are purpose-built platforms that are architected to maximize throughput using function-specific processing and memory for networking, security, content inspection, and management. Content-ID is enabled on all Palo Alto Networks platforms through annual subscriptions for URL filtering and/or threat prevention, both of which provide support for unlimited users. The unlimited user support helps maintain a consistent annual cost structure while ensuring that new employees are protected as they are hired.

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
Note: Threat prevention subscription includes antivirus, anti-spyware, vulnerability exploit protection and file blocking.		
PA-4060 URL filtering subscription	Future	Future
PA-4050 URL filtering subscription	PAN-PA-4050-URL	PAN-PA-4050-URL-R
PA-4020 URL filtering subscription	PAN-PA-4020-URL	PAN-PA-4020-URL-R
PA-2050 URL filtering subscription	PAN-PA-2050-URL	PAN-PA-2050-URL-R
PA-2020 URL filtering subscription	PAN-PA-2020-URL	PAN-PA-2020-URL-R

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