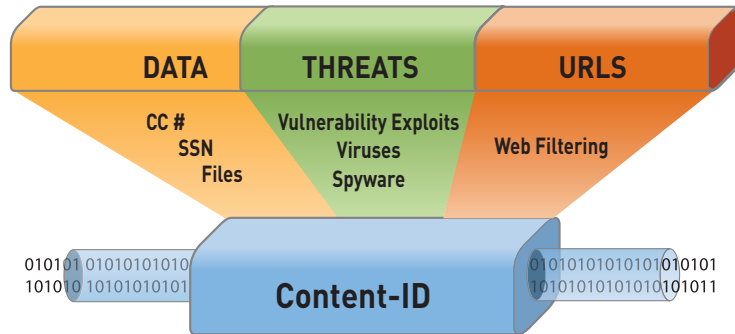


Content-ID



Content-ID combines a real-time threat prevention engine with a comprehensive URL database and elements of application identification to limit unauthorized data and file transfers, detect and block a wide range of threats and control non-work related web surfing. The application visibility and control delivered by App-ID, combined with the content inspection enabled by Content-ID means that IT departments can regain control over application traffic and the related content.

With employees using any application they desire and surfing the web with impunity, it's no wonder that enterprises struggle to protect the network from threat activity. The first step in regaining control over the threat activity is to identify and control applications to reduce the unwanted or bad application activity – which are commonly used as threat vectors. Once the application “footprint” has been diminished, policies to control content can be implemented to complement the application usage control policies.

Content-ID takes full advantage of the single pass parallel processing architecture which is a unique approach to integrating software and hardware that simplifies management, streamlines processing and maximizes performance. Within Content-ID, the single pass software melds a uniform signature format with stream-based scanning to inspect traffic in a single pass. The software is tied directly to a parallel processing hardware platform that uses function specific processors for threat prevention to maximize throughput and minimize latency.

Content-ID enables customers to apply policies to inspect and control content traversing the network.

- Block viruses, spyware, and application vulnerability exploits in a single pass.
- Limit unauthorized transfer of files and sensitive data such as CC# or SSN.
- Implement policy control over non-work related web surfing.
- Single pass software architecture maximizes performance by scanning traffic only once, regardless of which Content-ID features are enabled.

Threat Prevention

Enterprise networks are rife with applications that can evade detection. Common methods include dynamically hopping ports, re-using other ports, emulating other applications or tunneling inside SSL. The use of evasive applications has 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 application vulnerabilities, spyware, and viruses 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.
- **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.

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.

Vulnerability Attack Protection

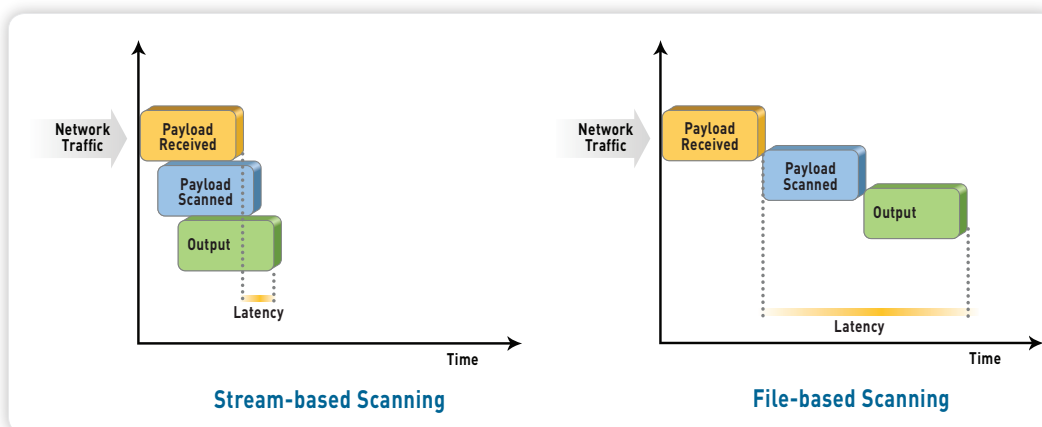
Application vulnerability prevention is enabled using a set of intrusion prevention system (IPS) features to block known and unknown network and application-layer vulnerability exploits, buffer overflows, DoS attacks and port scans from compromising and damaging enterprise information resources. IPS mechanisms include:

- Protocol decoders and anomaly detection
- Stateful pattern matching
- Statistical anomaly detection
- Heuristic-based analysis
- Block invalid or malformed packets
- IP defragmentation and TCP reassembly
- Custom vulnerability and spyware phone home signatures

Traffic is normalized to eliminate invalid and malformed packets, while TCP reassembly and IP de-fragmentation is performed 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 consisting of 20 million URLs across 76 categories that enables IT departments to monitor and control employee web surfing activities. The on-box URL database can be augmented to suit the traffic patterns of the local user community with a custom, 1 million URL database. URLs that are not categorized by the local URL database can be pulled into cache from a hosted, 180 million URL database. In addition to database customization, administrators can create custom URL categories to further tailor the URL controls to suit their specific needs. URL filtering visibility and policy controls can be tied to specific users through the transparent integration with enterprise directory services (Active Directory, LDAP, eDirectory) with additional insight provided through customizable reporting and logging.



Stream-based scanning

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

Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	No Intra-zone DMZ	DMZ	DMZ	any	any	any	any	any	⊘	none	🔗
2	Do Not Log to ACC	tapzone	tapzone	any	any	LocalServers	any	any	✔	none	none
3	Do not log local urls	tapzone	tapzone	any	any	LocalNetwork	ssl web-browsing	any	✔	🔒	🔗
4	Monitor ALL	tapzone	tapzone	any	any	any	any	any	✔	🔒🔒🔒🔒🔒	🔗
5	Block P2P	trust	untrust	any	any	any	P2P Filesharing	any	⊘	none	🔗
6	Webmail - No Attachments	trust	untrust	any	any	any	Webmail	any	✔	🔒	🔗
7	Deny and Log Outbound	trust	untrust	any	any	any	any	any	✔	🔒	🔗
8	Deny and Log Inbound	untrust	trust	any	any	any	any	any	✔	🔒	🔗

Profile Groups

Group: New...

Individual Profiles

- Antivirus Profile: New...
- Vulnerability Protection Profile: New...
- Anti-Spyware Profile: New...
- URL Filtering Profile: New...
- File Blocking Profile: New...
- Data Filtering Profile: New...

OK Cancel

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 and Data Filtering

Data filtering features enable administrators to implement policies that will reduce the risks associated with the transfer of unauthorized files and data.

- **File blocking by type:** Control 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).
- **Data filtering:** Control the transfer of sensitive data patterns such as credit card and social security numbers in application content or attachments.
- **File transfer function control:** Control the file transfer functionality within an individual application, allowing application use yet preventing undesired inbound or outbound file transfer.

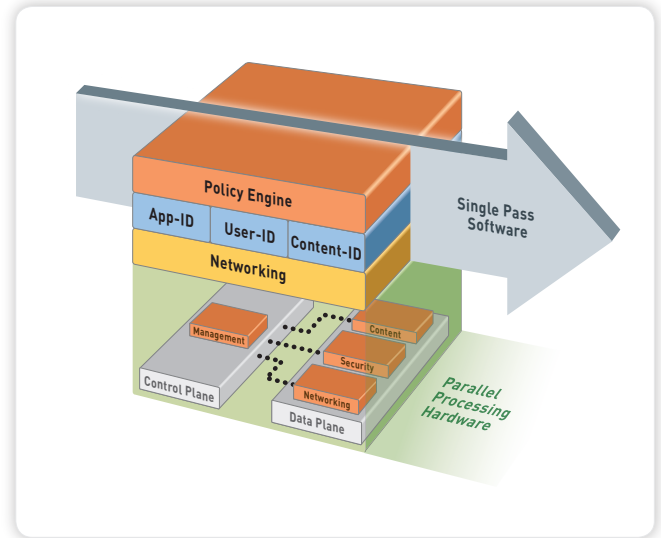
Log Correlation and Reporting

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 enterprise directory services. Log results can be exported to a CSV file for offline archival or further analysis. The trace session tool accelerates forensics or incident investigation with a centralized, correlated view across all of the logs for traffic, threats, URLs, and applications related to an individual session.

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 utilize a single pass parallel processing architecture to maximize throughput and minimize latency. The single pass software performs policy lookup, application identification and decoding, Active Directory user mapping, and content scanning (viruses, spyware, IPS) once on a given set of traffic. The software is tied to a parallel processing hardware platform with function specific processors for networking, security, threat prevention and management to maximize throughput and minimize latency. 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.



Palo Alto Networks single pass parallel processing architecture accelerates content inspection performance while minimizing latency.