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 and detect and block a wide range of exploits, malware, dangerous web surfing as well as targeted and unknown threats. 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 related content.

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

- Detect and block known and unknown threats in a single pass.
- Implement policy control over unapproved web surfing.
- Limit unauthorized transfer of files and sensitive data, such as credit card or Social Security numbers.
- Proactively identify and defend against unknown, new or custom malware and exploits.
- Single-pass software architecture maximizes performance by scanning traffic only once, regardless of which Content-ID features are enabled.

Enterprises of all sizes are at risk from a variety of increasingly sophisticated network-borne threats that have evolved to avoid many of the industry's traditional security measures. Palo Alto Networks® Content-ID delivers a new approach based on the complete analysis of all allowed traffic using multiple threat prevention and data-loss prevention techniques in a single, unified engine. Unlike traditional solutions, Palo Alto Networks actually controls the threat vectors themselves through the granular management of all types of applications. This immediately reduces the "attack surface" of the network, after which all allowed traffic is analyzed for exploits, malware, malicious URLs, and dangerous or restricted files or content. Palo Alto Networks then goes beyond stopping known threats to proactively identify and block unknown malware and exploits, which are often used in sophisticated network attacks.

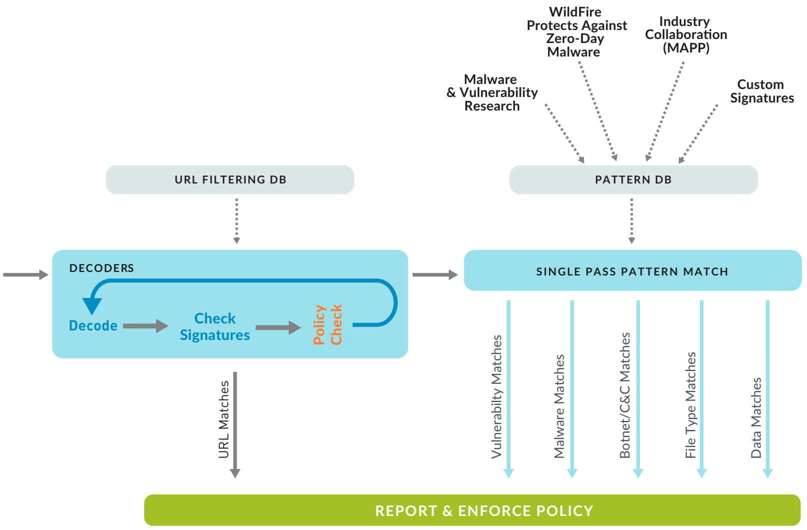


Figure 1: How Content-ID works

Content-ID is built on a single-pass, parallel processing architecture, which is a unique integration of software and hardware that simplifies management, streamlines processing and maximizes performance. The single-pass architecture (SP3) integrates multiple threat prevention disciplines (IPS, anti-malware, URL filtering, etc.) into a single stream-based engine with a uniform signature format. This allows traffic to be fully analyzed in a single pass without the incremental performance degradation seen in other multi-function gateways. 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.

Threat Prevention

Enterprise networks are facing a rapidly evolving threat landscape full of modern applications, exploits, malware and attack strategies that are capable of avoiding traditional methods of detection. Threats are delivered via applications that dynamically hop ports, use non-standard ports, tunnel within other applications routinely avoid proxies, and hide behind SSL or other types of encryption. These techniques can prevent traditional security solutions, such as IPS and firewalls from ever inspecting the traffic, thus enabling threats to easily and repeatedly flow across the network. Additionally, enterprises are exposed to targeted and customized malware, which may pass undetected through traditional antivirus solutions.

Palo Alto Networks Content-ID addresses these challenges with unique threat prevention abilities not found in other security solutions. First, the next-generation firewall removes the methods that threats use to hide from security through the complete analysis of all traffic, on all ports, regardless of evasion, tunneling or circumvention techniques. Simply put, no threat prevention solution will be effective if it does not have visibility into the traffic, and only Palo Alto Networks ensures that visibility through the identification and control of all traffic.

- **Application decoders:** Content-ID leverages hundreds of application and protocol decoders in App-ID to look for threats hidden within streams of application data. This enables the firewall to detect and prevent threats tunneled within approved applications that would pass by traditional IPS or proxy solutions.
- **SSL decryption:** More and more web traffic is encrypted with SSL by default. This can provide some protection to end users, but it also can provide attackers with an encrypted channel to deliver exploits and malware. Palo Alto Networks ensures visibility by giving security organizations the flexibility to, by policy, granularly look inside of SSL traffic based on application or URL category.
- **Control of circumventing technologies:** Attackers and have increasingly turned to proxies and anonymizers to hide from traditional network security products. Palo Alto Networks provides the ability to tightly control these technologies, and limit them to approved users, while blocking unapproved communications that could be used by attackers.
- **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, spyware and vulnerability exploits in a single pass.

Secondly, Palo Alto Networks brings multiple security disciplines into a single context and a single threat prevention engine. This context enables security teams to easily see beyond individual security events and recognize the full extent of a threat. Security managers can now see the interconnection of applications, exploits, malware, URLs, DNS, anomalous network behaviors, and ensures predictable performance by analyzing traffic once instead of progressively scanning in multiple engines.

Integrated by Design

Palo Alto Networks next-generation firewalls are purpose-built platforms that utilize a single-pass parallel processing architecture to maximize throughput and minimize latency. Traditional blade or UTM architectures notoriously introduce performance penalties for each feature that is enabled due to repeatedly processing traffic with the addition of each blade or feature. Palo Alto Networks designed a unique approach that performs Content-ID in a scan that leverages a common signature format. This means that content is processed only once, and performance remains steady, even as additional Content-ID features are enabled.

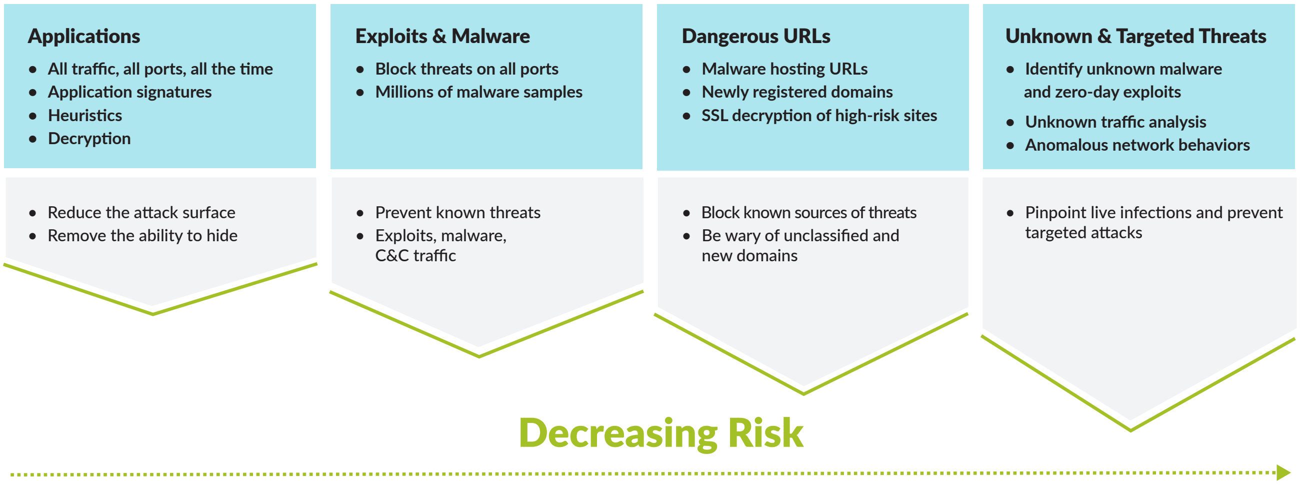

Applications
All traffic, all ports, all the time
Application signatures
Heuristics
Decryption
Reduce the attack surface
Remove the ability to hide
Exploits & Malware
Block threats on all ports
Millions of malware samples
Prevent known threats
Exploits, malware, C&C traffic
Dangerous URLs
Malware hosting URLs
Newly registered domains
SSL decryption of high-risk sites
Block known sources of threats
Be wary of unclassified and new domains
Unknown & Targeted Threats
Identify unknown malware and zero-day exploits
Unknown traffic analysis
Anomalous network behaviors
Pinpoint live infections and prevent targeted attacks
Decreasing Risk

Figure 2: Palo Alto Networks brings a unique approach to Threat Prevention, starting with reducing the attack surface through positive security controls, blocking all known threats, and quickly discovering and stopping unknown threats.

The use of a stream-based engine replaces several components commonly used in other solutions—a file proxy for data, virus, and spyware, a signature engine for vulnerability exploits, and an HTTP decoder for URL filtering. By using one common engine, two key benefits are realized. First, unlike file proxies that need to download the entire file before they can scan the traffic, a stream-based engine scans traffic in real time, only reassembling packets as needed and only in very small amounts. Second, unlike traditional approaches, all traffic can be scanned with a single engine, instead of multiple scanning engines.

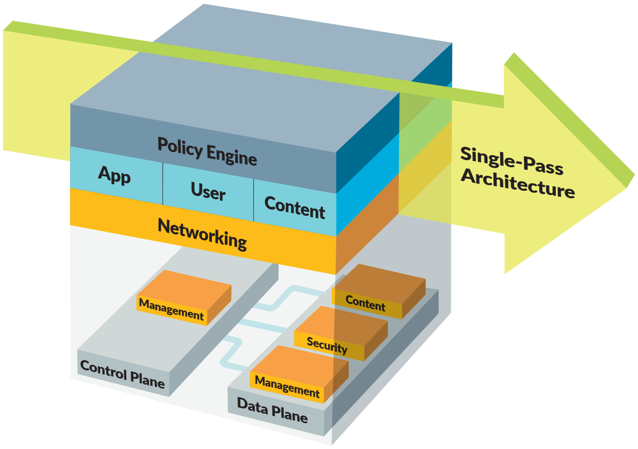


Figure 3: Palo Alto Networks single-pass parallel processing architecture accelerates content inspection performance while minimizing latency

Content-ID is enabled on all Palo Alto Networks platform deployments through annual URL Filtering and/or Threat Prevention subscriptions, 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.

Intrusion Prevention

Content-ID protects networks from all types of vulnerability exploits, buffer overflows, DoS attacks and port scans that lead to the compromise and damage of enterprise information resources. Palo Alto Networks IPS mechanisms include:

- Protocol decoders and anomaly detection
- Stateful pattern matching
- Statistical anomaly detection
- Heuristic-based analysis
- Invalid or malformed packet detection
- 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 defragmentation is performed to ensure the utmost accuracy and protection despite any packet-level evasion techniques.

WildFire: Protection from Unknown Malware and Zero-Day Exploits

Cyber adversaries have increasingly turned to unknown threats to avoid traditional security controls. Palo Alto Networks has addressed this challenge with WildFire™ cloud-based malware analysis environment, which identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) by observing their actual behavior in a virtualized environment, instead of relying solely on pre-existing signatures.

- **Integration of Firewall and the Cloud:** To support dynamic malware analysis across the network at scale, WildFire is built on a cloud-based architecture that can be leveraged by your existing Palo Alto Networks next-generation firewall, with no additional hardware. The in-line firewall captures unknown files and performs enforcement while maintaining high network throughput and low latency.

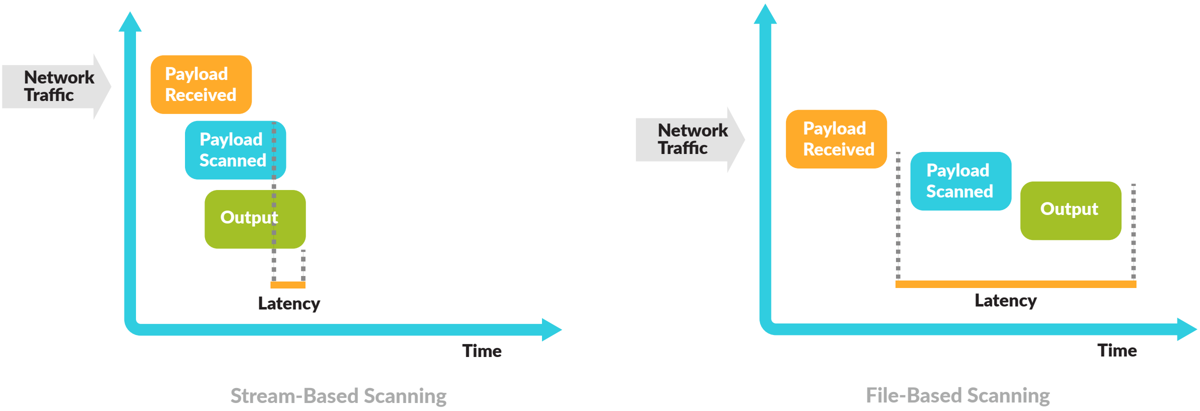
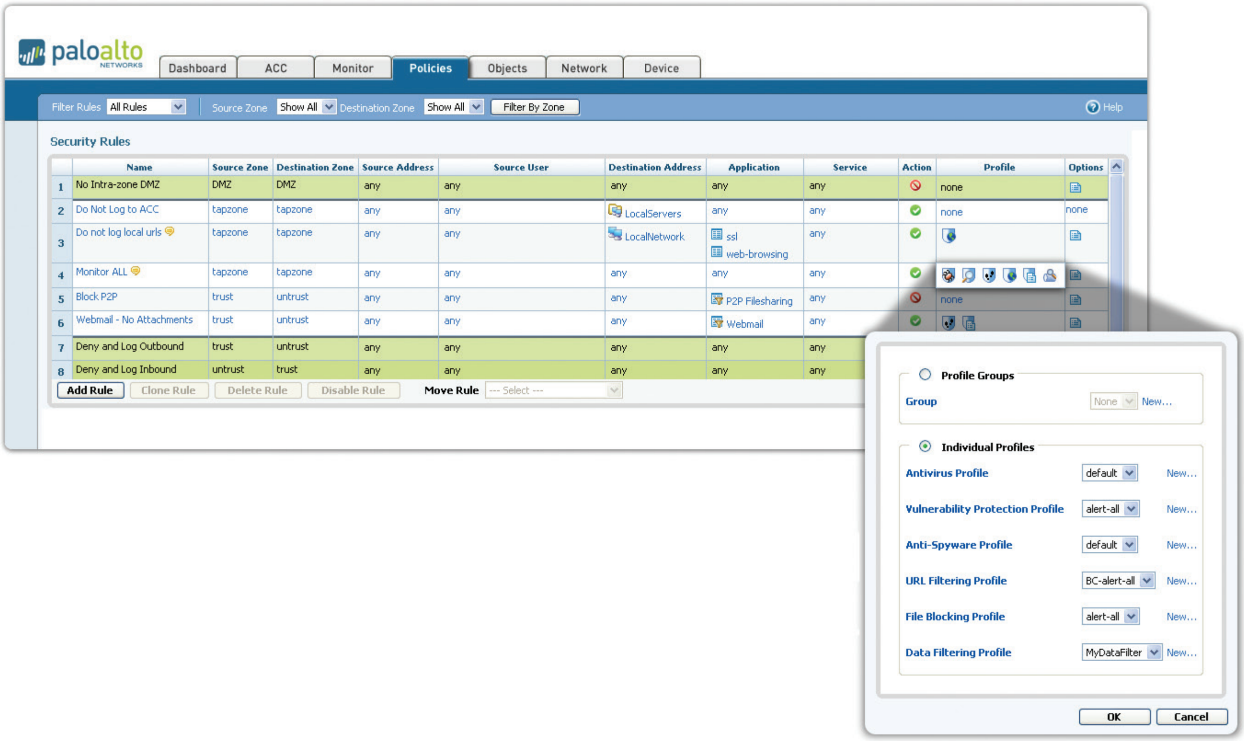


Figure 3: Stream-based scanning helps minimize latency and maximize throughput performance



Filter Rules: All Rules | Source Zone: Show All | Destination Zone: Show All | Filter By Zone

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: None New...

● Individual Profiles

Antivirus Profile	default	New...
Vulnerability Protection Profile	alert-all	New...
Anti-Spyware Profile	default	New...
URL Filtering Profile	BC-alert-all	New...
File Blocking Profile	alert-all	New...
Data Filtering Profile	MyDataFilter	New...

Figure 4: **Content-ID is enabled on a per-rule basis using individual or group profiles to facilitate policy-based control over content traversing the network**

- **WildFire Virtualized Sandbox:** WildFire 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 a sample is identified as malicious, WildFire automatically generates protections and delivers them to all subscribed WildFire customers globally in as little as 5 minutes.
- **Deep Visibility and Analysis:** WildFire users receive integrated logs, analysis and visibility into WildFire events enabling teams to quickly investigate and correlate events observed in their networks. This allows security staff to quickly locate the data needed for timely investigations and incident response. Host-based and network-based indicators of compromise become actionable through log analysis and custom signatures. An open API allows for integration with best-in-class SIEM tools, such as the Palo Alto Networks application for Splunk®, and leading endpoint agents.

URL Filtering

Complementing the threat prevention and application control capabilities is a fully integrated, on-box URL filtering database that enables security teams to not only control end-user web surfing activities but also block access to malicious URLs and phishing links used in cyber attacks. The on-box URL database can be augmented to suit the traffic patterns of the local user community with a custom URL database. URLs that are not categorized by the local URL database can be pulled into cache from a hosted 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 categorization can be combined with application and user classification to further target and define policies. For example, SSL decryption can be invoked for select, high-risk URL categories to ensure threats are exposed; QoS controls can be applied to streaming media sites. URL filtering visibility and policy controls can be tied to specific users through transparent integration with enterprise directory services (Active Directory®, LDAP, eDirectory™) with additional insight provided through customizable reporting and logging.

Administrators can configure a custom block page to notify end users of any policy violations. In order to place some of the web activity ownership back in the user's hands, administrators can allow users to continue after being presented with a warning page or require passwords to override the URL filtering policy.

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 or 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 data transfers.

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 and 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.

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

pan-content-id-tb-061416