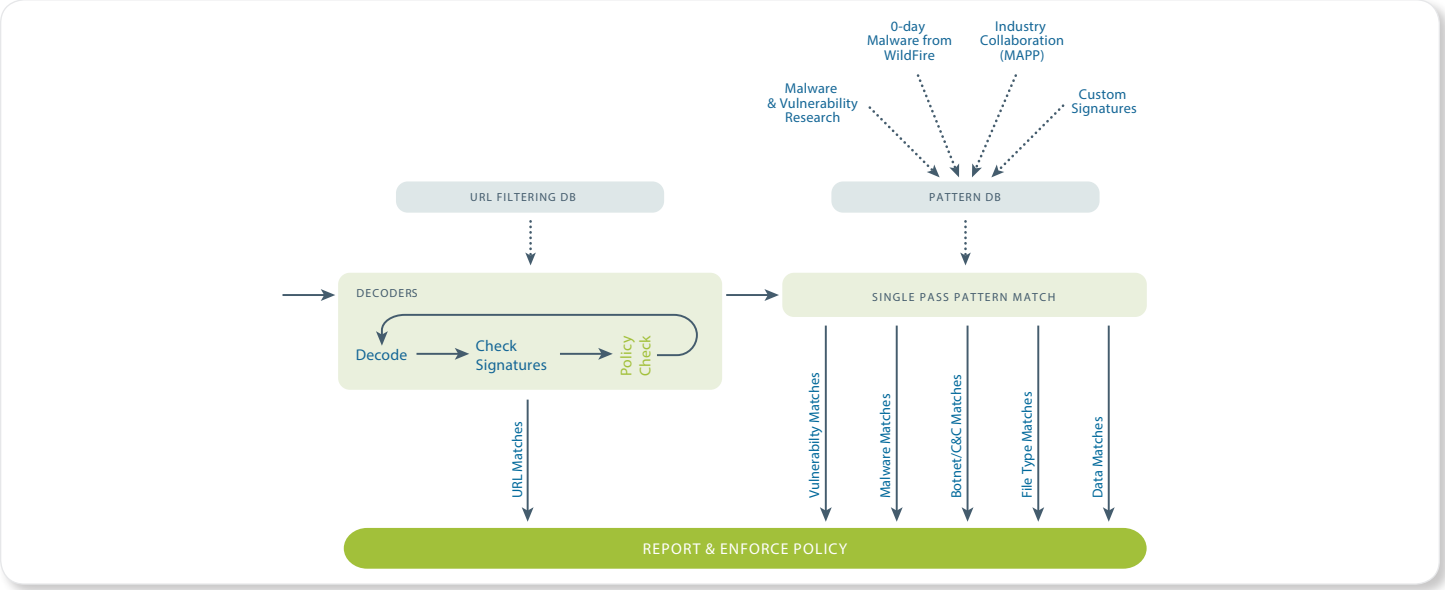
# Content-ID




**How Content-ID works.**

**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
- Implement policy control over unapproved web surfing.
- Limit unauthorized transfer of files and sensitive data such as CC# or SSN.
- Proactively identify and defend against unknown, new or customized malware.
- Single pass software architecture maximizes performance by scanning traffic only once, regardless of which Content-ID™ features are enabled.

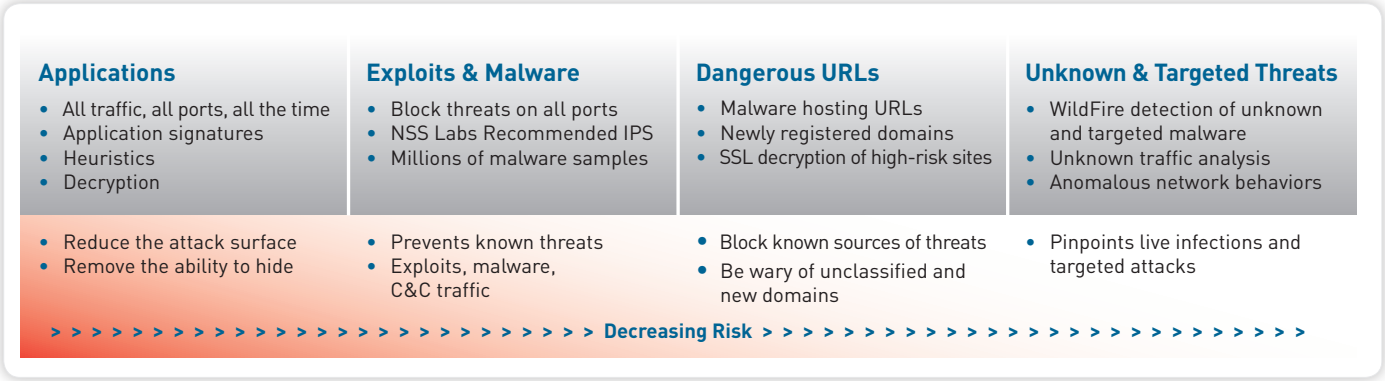
paloalto NETWORKS

the network security company™

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 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.

Enterprises of all sizes are at risk from a variety of increasingly sophisticated network-bourne 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 tight control of all types of applications. This immediately reduces the "attack surface" of the network after which all allowed traffic is analyzed for exploits, malware, dangerous URLs, dangerous or restricted files or content. Palo Alto Networks then goes beyond stopping known threats to proactively identify and control unknown malware, which is often used as the leading edge of sophisticated network attacks.

Content-ID is built on a single-pass 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.



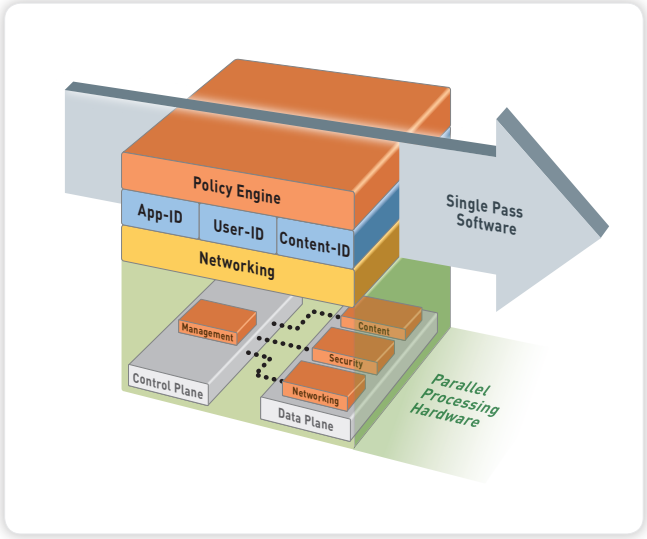

## Threat Prevention

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 or hide within proxies, 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 the more than 100 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 malware have increasingly turned to proxies, anonymizers and a variety of encrypted proxies 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 including viruses, 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, anomalous network behaviors and management and reporting and ensures predictable performance by analyzing traffic once instead of progressive scanning in multiple engines.




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

## 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 for each blade or feature. Palo Alto Networks designed a unique approach that performs Content-ID in a single unified engine and 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.

The single pass software uses a stream-based, uniform signature-matching engine for content inspection. Instead of using separate engines and signature sets (requiring multi-pass scanning) and instead of using file proxies (requiring file download prior to scanning), the single pass architecture scans traffic for all signatures once and in a stream-based fashion to avoid latency introduction.

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 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.

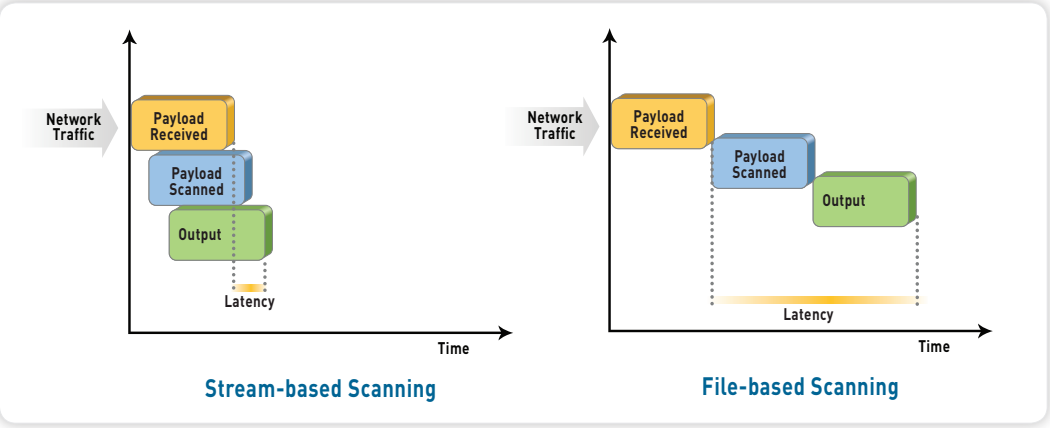
Content-ID is enabled on all Palo Alto Networks platforms through annual subscriptions for URL filtering and/or threat prevention, both of which provide support for unlimited users. The unlimited user support helps maintain a consistent annual cost structure while ensuring that new employees are protected as they are hired.

## 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 capabilities have received recommended status from NSS Labs based on the high block rate, strong performance and resistance to IPS evasion. 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 de-fragmentation is performed to ensure the utmost accuracy and protection despite any packet-level evasion techniques.




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

## Stream-based Malware Scanning

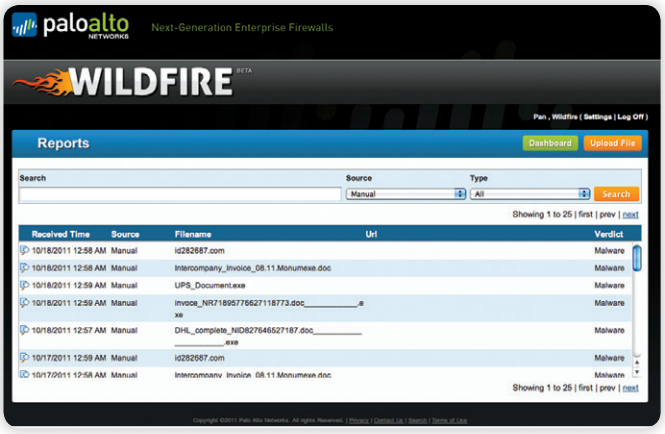
Prevention of known viruses and malware is performed through the use of stream-based scanning, a technique that begins scanning as soon as the first packets of the file are received as opposed to waiting until the entire file is loaded into memory to begin scanning. This means that performance and latency issues are minimized by receiving, scanning, and sending traffic to its intended destination immediately without having to first buffer and then scan the file.

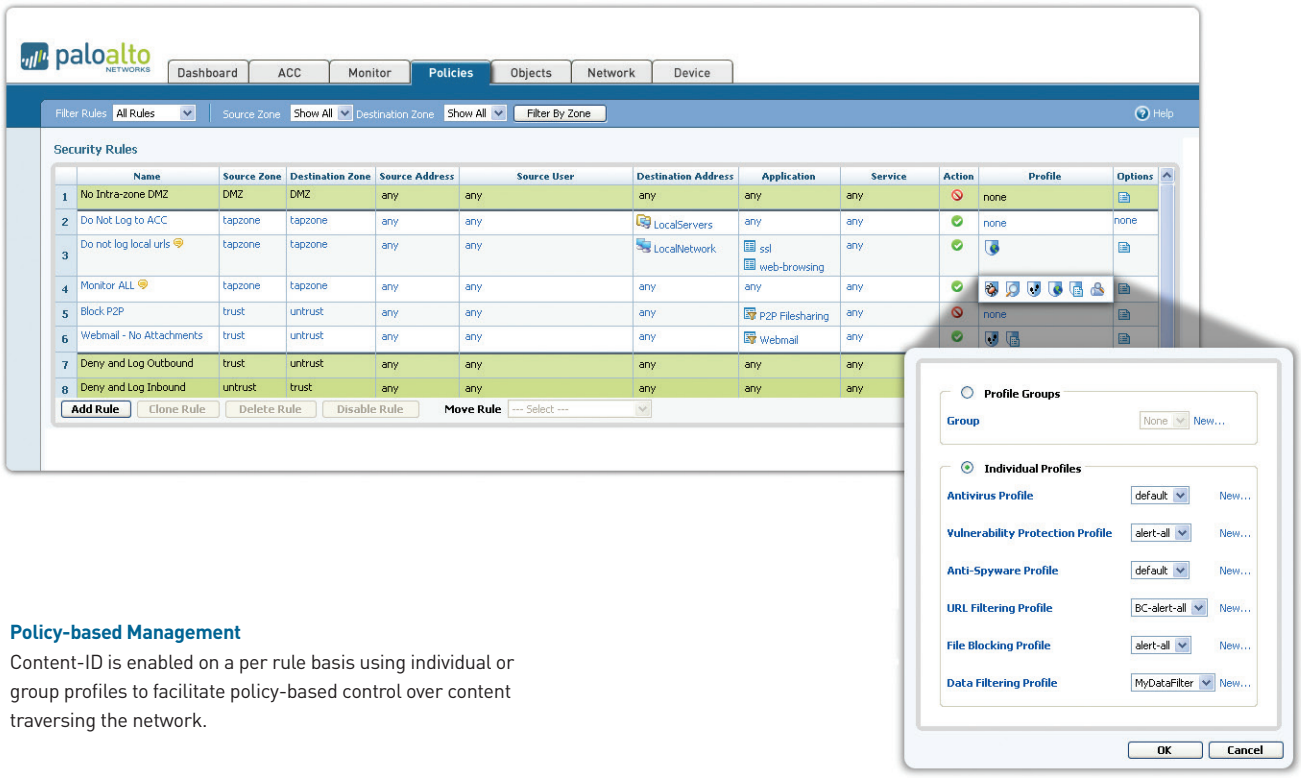
Palo Alto Networks maintains an independent database of millions of malware samples, with more than 50,000 samples analyzed daily. Virus and spyware signatures control a wide range of malware including PDF, HTML and Javascript viruses, spyware downloads, spyware phone home, trojans, key-loggers and botnets. Palo Alto Networks provides coverage for 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.

## WildFire: Modern Malware Prevention

Criminals have increasingly turned to customized and targeted malware to avoid traditional antivirus controls. Palo Alto Networks has addressed this challenge with WildFire, which identifies malware by observing the actual behavior of a suspect file in a virtualized environment instead of relying solely on pre-existing signatures.

- **Integration of Firewall and the Cloud** - WildFire makes use of a customer's on-premises firewalls in conjunction with Palo Alto Networks cloud-based analysis engine to deliver an ideal blend of protection and performance. The in-line firewall captures unknown files and performs in-line enforcement while maintaining high network throughput and low latency. The analysis of unknown files is offloaded to a secure cloud-based engine to identify unknown malware and subsequently deliver protections to all locations.
- **WildFire Virtualized Sandbox** - When the Palo Alto Networks firewall encounters an unknown file (initially portable executable files, and expanding to other file types in the future), the file can be submitted to the hosted WildFire virtualized sandbox. Submissions can be made manually or automatically based on policy. The sandbox provides virtual targets for the suspected malware where Palo Alto Networks can directly observe more than 100 malicious behaviors that can reveal the presence of malware.
- **Automated Signature Generator** – When a sample is identified as malware, the sample is then passed on to the signature generator, which automatically writes a signaturse for the sample and tests it for accuracy. Signatures are then delivered to all Palo Alto Networks customers as part of the malware signature updates. Customers with the WildFire subscription receive protections from newly discovered malware within an hour of the initial discovery anywhere in the world.
- **Deep Visibility and Analysis** – In addition to providing protection from modern malware, users can see a wealth of information about the detected malware in reports available on the WildFire Portal. This includes the ability to see all behaviors of the malware, the user that was targeted, the application that delivered the malware, and all URLs involved in delivery or phone-home of the malware.






### 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.

## URL Filtering

Complementing the threat prevention and application control capabilities is a fully integrated, on-box URL filtering database that enables security teams to to not only control end-user web surfing activities, but also combine URL context with application and user rules. 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 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 the 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. The page can include references to the username, IP address, the URL they are attempting to access and the URL category. 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 can use 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 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 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.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com