Content identification

Content identification infuses next-generation firewalls with capabilities not possible in legacy, port-based firewalls. The user and application visibility and control of App-ID™ and User -ID™, coupled with the content inspection enabled by Content-ID, empowers IT teams to regain control over application traffic and related content.

Enterprises of all sizes are at risk from a variety of increasingly sophisticated threats that have evolved to avoid many of the industry's traditional security measures. Content-ID™ technology delivers a new approach based on the complete analysis of all allowed traffic, using multiple advanced threat prevention technologies in a single, unified engine.

Content-ID is based on a single-pass architecture, which is a unique combination of software and hardware that was designed from the ground up to integrate multiple threat prevention technologies (IPS, anti-malware, URL filtering, etc.) into a single stream-based approach that simplifies management, streamlines processing, and maximizes performance

Application identification eliminates threat vectors through the tight control of all types of applications. This capability immediately reduces the attack surface of the network, after which all allowed traffic is analyzed for exploits, malware, dangerous URLs, and dangerous or restricted files or content. Content identification 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.

Threat prevention

Enterprise networks are facing a rapidly evolving threat landscape full of modern applications, exploits, malware, and attack strategies that can avoid 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. Also, enterprises are exposed to targeted and customized malware, which may pass undetected through traditional anti-malware solutions.

To be effective threat prevention needs to be applied in full application and protocol context – across all traffic and ports – to ensure that threats are detected and blocked, despite evasion attempts. Content-ID provides fully integrated protection from vulnerability exploits, malware and malware-generated command and control traffic.

Palo Alto Networks Content-ID addresses these challenges with unique threat prevention capabilities not found in traditional 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 any evasion, tunneling, or circumvention techniques that are used. No threat prevention solution will be effective if it does not have visibility into the traffic. Palo Alto Networks ensures that visibility through the identification and control of all traffic, using the following tools and techniques:

- **Application decoders.** Content-ID leverages the more than 100 application and protocol decoders in App-ID to look for threats hidden within application data streams. This tool enables the firewall to detect and prevent threats tunneled within approved applications that would bypass traditional IPS or proxy solutions.

- **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 C2 activity and vulnerability exploits in a single pass.

- **Vulnerability attack protection (IPS).** IPS functionality blocks vulnerability exploits, buffer overflows, and port scans. Additional capabilities, like blocking invalid or malformed packets, IP defragmentation and TCP reassembly, protect you from the evasion and obfuscation methods used by attackers Robust routines for traffic normalization and defragmentation are joined by protocol-anomaly, behavior-anomaly, and heuristic detection mechanisms to provide protection from the widest range of both known and unknown threats.

- **Cloud-based intelligence.** For unknown content, WildFire provides rapid analysis and a verdict that the firewall can leverage.

- **SSL decryption.** More and more web traffic connections are encrypted with SSL by default, which can provide some protection to end users, but SSL 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 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.

- **File and Data Filtering** – The data filtering features in Content-ID enable you to implement policies that reduce the risks associated with the transfer of unauthorized files and data, such as file blocking by type; data filtering to control the transfer of sensitive data patterns, including credit card and Social Security numbers in application content or attachments; and file transfer function control that provides control over file transfer functionality within an individual application, allowing application use while preventing undesired inbound or outbound file transfers.

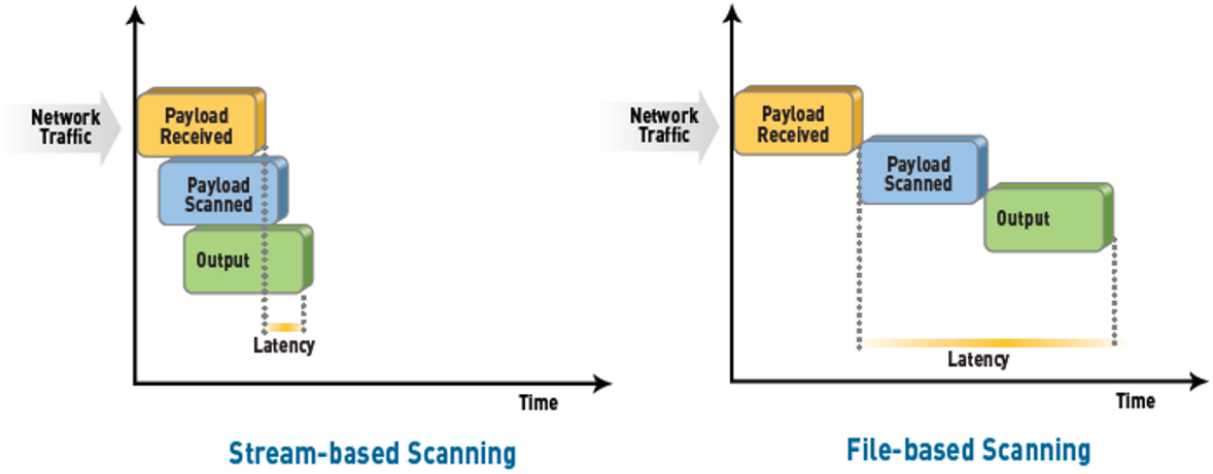
- **Anti-Malware**– Known malware as well as future variations of known malware are detected by a stream-based engine that blocks in-line at very high speeds.
- **Command and Control**– Content-ID can stop malware outbound communications, passively analyze DNS queries, and will identify the unique patterns of botnets. It can identify infected users, and prevent secondary downloads and data from leaving your enterprise.
- **URL Filtering** – Content-ID connects to an integrated URL Filtering database and allows you to more easily and effectively enforce policies for Web browsing. The feature also reduces malware incidents by blocking access to known malware and phishing download sites.

Stream-based malware scanning

Prevention of known 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. Stream-based scanning minimizes performance and latency issues by receiving, scanning, and sending traffic to its intended destination immediately without having to first buffer and then scan the file (see Figure 2-11).

Figure 2-11

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



Intrusion prevention

Content-ID protects networks from all types of vulnerability exploits, buffer overflows, DoS attacks, and port scans that lead to the compromise of confidential and sensitive enterprise information. IPS mechanisms in Content-ID 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 are performed to ensure the utmost accuracy and protection despite any packet-level evasion techniques.

File and data filtering

File and data filtering takes advantage of in-depth application inspection and enables enforcement of policies that reduce the risk of unauthorized information transfer or malware propagation. File and data filtering capabilities in Content-ID include:

- **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 numbers and Social Security numbers in application content or attachments.
- **File transfer function control.** Control the file transfer functionality within an individual application, which allows application use while preventing undesired inbound or outbound file transfer.