URL Filtering

Applications	URLs	Known Threats	Unknown Threats
• Identify and control all applications, across all ports, all the time.	• **Control traffic sources and destinations based on risk**	• Stop exploits, malware, spying tools, and dangerous files.	• Automatically identify and block new and evolving threats.

An integrated approach to risk reduction

Fully integrated URL filtering database enables granular control over web browsing activity, complementing safe application enablement policies.

- Safely enable web usage with the same policy control mechanisms that are applied to applications—allow, allow and scan, apply QoS, block, and more.
- Reduce malware incidents by blocking access to known malware and phishing download sites.
- Tailor web filtering control efforts with white lists (allow), black lists (block), custom categories and database customization.
- Facilitate SSL decryption policies such as "don't decrypt traffic to financial services sites" but "decrypt traffic to blog sites".

Tech-savvy users are spending more and more time on their favorite website or using the latest and greatest web application. This unfettered web surfing and application use exposes organizations to security and business risks including propagation of threats, possible data loss, and lack of regulatory or internal policy compliance.

Stand-alone URL filtering solutions are insufficient control mechanisms because they are easily bypassed with external proxies (PHproxy, CGIproxy), translation sites (Google Translate, Bing Translator), search engine caches (Google Search, Internet Archive), circumventors (Tor, UltraSurf, Hamachi) and remote desktop access tools (GoToMyPC, RDP, SSH). Controlling users' application activity requires a integrated approach that implements policies to control web activity and the applications that are commonly used to bypass traditional security mechanisms.

Palo Alto Networks® next-generation firewalls natively classifies all traffic, inclusive of applications, threats and web content, then ties that traffic to the user, regardless of location or device type. The application, content and user, the business elements that run your business, are then used as the basis of all security policies. By addressing the lack of visibility and control from both the application and web content perspective, your organization is safeguarded from a full spectrum of legal, regulatory, productivity, and resource utilization risks.

paloalto NETWORKS®

the network security company™

Flexible, Policy-based Control

As a complement to the application visibility and control enabled by App-ID™, URL categories can be used as a match criteria for policies. Instead of creating policies that are limited to either allowing all or blocking all behavior, the URL category as a match criteria allows for exception-based behavior, resulting in increased flexibility yet more granular policy enforcement. Examples of how using URL categories can be used in policies include:

- Identify and allow exceptions to general security policies for users who may belong to multiple groups within Active Directory (e.g. deny access to malware and hacking sites for all users, yet allow access to users that belong to the security group).

- Allow access to streaming media category, but apply QoS to control bandwidth consumption.

- Prevent file download/upload for URL categories that represent higher risk (e.g. allow access to unknown sites, but prevent upload/download of executable files from unknown sites to limit malware propagation).

- Apply SSL decryption policies that allow encrypted access to finance and shopping categories but decrypt and inspect traffic to all other URL categories.

Tighten controls over common policy evasion tactics

URL filtering policies can be enforced even when common evasion tactics such as cached results and language translation sites are used.

- **Search engine cached results prevention:** a common tactic to evade controls is to access cached results within the popular search engines. URL filtering policies will be applied to cached results when end-users attempt to view the cached results of Google Search and Internet Archive.

- **Translation site filtering:** URL filtering policies are applied to URLs that are entered into translation sites such as Google Translate as a means of bypassing policies.

Safe Search Enforcement

Safe Search Enforcement allows you to prevent inappropriate content from appearing in users' search results. When this feature is enabled, only Google, Yahoo or Bing searches with the strictest Safe Search option set will be allowed; all other searches will be blocked.

Customizable URL Database and Categories

To account for each organization's unique traffic patterns, on-device caches are used to store the most recently accessed URLs. Devices can also automatically query a master cloud-based database for URL category information when an unknown URL is found. Lookup results are automatically inserted into the cache for future activity. Additionally, administrators can create custom URL categories to suit their specific needs.

Customizable End-User Notification

Each organization has different requirements on how best to inform end-users that they are attempting to visit a web page that is blocked according to the corporate policy and associated URL filtering profile. To accomplish this goal, administrators can use a custom block page to notify end users of the policy violation. The custom block 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 have two powerful options:

- **URL filtering continue:** when a user accesses a page that potentially violates URL filtering policy, a block page warning with a "Continue" button can be presented to the user, allowing them to proceed if they feel the site is acceptable.

- **URL filtering override:** requires a user to correctly enter a password in order to bypass the block page and continue surfing.

URL Activity Reporting and Logging

A set of pre-defined or fully customized URL filtering reports provides IT departments with visibility into URL filtering and related web activity including:

- **User activity reports:** an individual user activity report shows applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period of time.

- **URL activity reports:** a variety of top 50 reports that display URL categories visited, URL users, websites visited, blocked categories, blocked users, blocked sites and more.

- **Real-time logging:** logs can be filtered through an easy-to-use query tool that uses log fields and regular expressions to analyze traffic, threat or configuration incidents. Log filters can be saved and exported and for more in-depth analysis and archival, logs can also be sent to a syslog server.

Deployment Flexibility

The unlimited user license behind each URL filtering subscription and the high performance nature of the Palo Alto Networks next-generation firewall means that customers can deploy a single appliance to control web activity for an entire user community without worrying about cost variations associated with user-based licensing.