URL FILTERING

Enable Safe Web Access for All Users

URL Filtering enables safe web access. The cloud-based service uses a unique combination of static analysis and machine learning to identify as well as automatically block malicious sites and phishing pages. As a native component of the Palo Alto Networks Security Operating Platform, URL Filtering provides best-in-class web security with easy-to-use application- and user-based policies.

URL Filtering

- Safeguards your organization from malicious sites through a unique combination of static analysis and machine learning while addressing regulatory, compliance, and acceptable use.
- Immediately categorizes and blocks new malicious URLs with a powerful categorization engine enhanced by shared protections from the WildFire malware prevention service and our Unit 42 threat research.
- Extends your next-generation firewall policy with granular web control, including automatically triggering advanced security actions, such as selective SSL decryption for suspicious sites.

Enabling safe web access requires a natively integrated approach that extends your next-generation firewall policy with easy-to-set web controls that automatically detect, prevent, and control threats.

Safe Web Access Through Coordinated Protection

Palo Alto Networks URL Filtering service scans websites and analyzes their content using machine learning, with static and dynamic analysis, to accurately determine categories and risk ratings. URLs are classified into benign or malicious categories, which can easily be built into next-generation firewall policy for total control of web traffic. Newly categorized malicious URLs are immediately blocked upon discovery, requiring no analyst intervention.

Analytics are used to assign a risk rating to each site by examining additional layers of information, including domain history and reputation, host reputation, use of dynamic DNS, or the presence of high-risk content. URL categories and risk rating can be used together to create nuanced policies that block dangerous sites that may be used in phishing attacks, exploit kit delivery, or command and control, while still allowing employees the freedom to access web resources necessary for a business purpose.

URL Filtering works as part of the Security Operating Platform for an integrated approach to stopping threats at every opportunity. When an attack is launched against your network, URL Filtering works with your next-generation firewalls and Threat Prevention subscription to provide you with superior security. In addition to its own analysis, URL Filtering uses shared threat information from WildFire® malware prevention service and other sources, updating protections against malicious sites within seconds.

Extend Firewall Policy to Control Web Content

When it sees web traffic, your next-generation firewall uses the URL Filtering service to identify the URL category and apply consistent policy. In contrast to rules that are limited to either allowing or blocking all web behavior, multiple URL categories can be combined in policies, allowing for precise, exception-based enforcement, simplified management, and the flexibility to granularly control web traffic through a single policy table. You can use multiple URL categories in policies to, for example:

- Block all “high-risk” sites while allowing access to others but prevent download/upload of executable files or potentially dangerous file types for “medium-risk” URLs.

- Allow all “computer-and-internet-info” sites but block “recently-registered-domain” sites.
- Allow access to “freeware-and-shareware” sites but prevent file downloads from them; block them if they are “high-risk.”
- Identify and allow exceptions to general security policies for users who may belong to specific groups within Active Directory®—e.g., deny access to hacking sites for all users but those who belong to the security group.
- Allow access to personal websites and blogs but decrypt if SSL is used, and employ strict Threat Prevention profiles to block potential exploit kits embedded in forums and posts.

Create Policies Based on URL Categories	
Policies	**Description**
Selective SSL	Initiate SSL decryption based on URL categories.
Credential theft	Dictate which sites can receive corporate credentials and block, allow, or warn users submitting credentials to unauthorized sites.
Block high-risk file types	Prevent upload/download of executable files or potentially dangerous file types.
Enable stricter IPS profiles	Automatically employ strict vulnerability and anti-spyware profiles for specific URL categories to block phishing kits, exploit kits, and server- and client-side vulnerabilities.
User-based policies	Allow specific groups in your organization to access certain URL categories while blocking those categories for others.

Beyond simply blocking malicious sites, URL categories can be used to enable fine-grained security policies to protect users without slowing down the business.

Selective Web Traffic Decryption

You can establish policies to selectively decrypt SSL-secured web traffic to gain maximum visibility into potential threats while complying with data privacy regulations. Specific URL categories, such as social networking, web-based email, or content delivery networks, can be designated for SSL decryption while transactions to and from other types of sites, such as sites for governments, banking institutions, or healthcare providers, can be designated to remain encrypted. You can implement simple policy that enables SSL decryption for applicable content categories with high or medium risk ratings. Selective decryption enables optimal security posture while respecting confidential traffic parameters set by company policies or external regulations.

Machine Learning-Powered Detection

Machine learning and automation enable rapid, highly accurate web threat detection. Our systems automatically examine URLs for images, content, and language to determine benign and malicious status. We use text and language analysis to draw correlations between website copy, the context in which that copy is used, and URLs to precisely categorize websites. Images of websites are broken down pixel-by-pixel and compared to all previous examples using a sophisticated algorithm to assist in determining potential phishing sites. By examining each component of an individual page and applying multiple machine learning classifiers, we combine accuracy, speed, and continual adaptation in the face of changing attack techniques.

- **Content analysis:** Our URL crawlers scrutinize multiple website attributes for malicious indicators. Correlated domain data, the presence of forms, and the location of specific types of content are among the attributes our learning classifiers process. Every URL we analyze adds to our data library, continually informing and updating our ability to accurately identify websites that pose security threats.
- **Text analysis:** URL Filtering scans website text and its context to determine the most accurate category classification.
- **Image analysis:** To avoid detection, phishing pages increasingly use obfuscated JavaScript and images on webpages instead of actual text. By automatically analyzing the image content of each URL, we can compare website code with visual indicators to more accurately determine whether a URL poses a phishing threat.

Credential Phishing Prevention

Phishing is one of the most prevalent, dangerous, and malicious techniques available to adversaries aiming to steal legitimate user credentials. When stolen, genuine credentials provide attackers with “authorized” network access, which is less likely to trip alarms or alert administrators. This means more time for attackers to accomplish their objectives, such as stealing sensitive information or causing harm to an organization.

URL Filtering analyzes potential credential phishing pages, conclusively identifying and preventing access through the “phishing” URL category. Beyond identifying and preventing potential phishing threats from being delivered to users, URL Filtering offers unique capabilities to prevent users from unwittingly sending credentials to adversaries. Administrators can establish URL Filtering policy that dictates which sites should be allowed to receive corporate credentials. Leveraging the capabilities of User-ID™ technology on Palo Alto Networks next-generation firewalls, URL Filtering detects user credentials submitted into outgoing web forms and lets you set policy that can block the attempt, allow it, or notify the user they may be performing a dangerous action.

Customizable Categories

Although URL Filtering utilizes a defined set of categories, different organizations may have different needs around risk tolerance, compliance, regulation, or acceptable use. To meet organizational requirements and fine-tune security policies, administrators can establish custom categories by combining multiple existing categories to create new ones. For example, combining the "high-risk," "financial-services," and "recently-registered" categories would create a powerful new category, enabling policy to be enacted upon any site that meets these criteria.

Tight Controls Over Common Policy Evasion Tactics

URL Filtering policies can be enforced even when attacks use common evasion tactics, such as cached results and language translation sites. This is accomplished through:

- **Search engine-cached results prevention:** A common tactic employed to evade controls involves accessing cached results within the popular search engines. URL Filtering policies are applied to cached results when end users attempt to view the cached results of Google searches and internet archives.
- **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, Yandex, Yahoo, or Bing searches with the strictest safe search option set will be allowed, and all other searches can be blocked.

Customizable End-User Notifications

Each organization has different requirements for how best to inform users when they attempt to visit webpages that are blocked according to policy and the associated URL Filtering profile. Administrators can notify users of the violation using a custom block page, which can include references to username and IP address, the URL a user is attempting to access, and the page's URL category, in addition to a customized message from the administrator. To put some web activity ownership back in users' hands, administrators have two options:

- **URL Filtering continue:** When users accesses pages that may pose risks to the organization, URL Filtering can present a customized warning page, with a "Continue" button, to users. This presents an opportunity to educate users about the risks of their requested sites and allows them to proceed if they feel the risks are acceptable.
- **URL Filtering override:** This option requires users to correctly enter a configurable password to create a policy exception and continue. This allows users access to potentially critical sites with approval from the administrator.

URL Activity Reporting and Logging

IT departments can get visibility into URL Filtering and related web activity through a set of predefined or fully customized URL Filtering reports, 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.
- **URL activity reports:** A variety of top 50 reports display URL categories visited, URL users, websites visited, blocked categories, blocked users, blocked sites, and more.

Maximized Security and Minimized TCO

URL Filtering is enabled as a natively integrated subscription on Palo Alto Networks next-generation firewalls. Our unique platform approach eliminates the need for multiple, stand-alone security appliances and software products. By deploying URL Filtering functionality directly within existing network traffic policy, you can minimize operational expenditure through a radically simplified rule base and streamlined training costs. Unlimited user licenses with the URL Filtering subscription let you secure web activity for your entire user community while reducing the total cost of ownership and increasing the effectiveness of your security.

Licensing Information

URL Filtering is available through the Palo Alto Networks URL Filtering license, or as part of the Palo Alto Networks Subscriptions ELA or Palo Alto Networks VM-Series ELA.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

url-filtering-ds-012319