Business Benefits

- **Eliminate security silos and keep users safe.** As a native component of the Next-Generation Firewall, URL Filtering provides best-in-class web security for campuses, branches, or mobile users or wherever they reside, eliminating hard-to-manage legacy solutions.
- **Minimize operational expenditure.** Deployed directly in your existing network traffic policy, URL Filtering functionality simplifies rule sets and streamlines administration for security teams.
- **Block new malicious sites.** URL Filtering categorizes and blocks never-before-seen malicious URLs in milliseconds, before they have a chance to infect your network and end users.
- **Prevent known malicious websites.** Safeguard your organization against known web-based threats, including phishing, malware, exploit kits, and command and control (C2).
- **Safeguard against phishing.** Layers of prevention protect your organization from known and brand-new phishing sites with the ability to stop credential phishing in real time.
- **Support regulatory compliance and acceptable use.** Ensure your organization maintains compliance with internal, industry, and government regulatory policies.

URL Filtering

Stop phishing, credential abuse, and command and control

The Web Is the Most Common Source of Cyberattacks

Malicious webpages expose employees to phishing and credential theft, malware infection, and ransomware. Attackers use automation to dynamically generate thousands of malicious new URLs daily, overwhelming legacy protections such as standalone proxies or web filtering tools, which simply can't keep up. In the minutes it takes to identify, classify, and protect against malicious websites, an infection can spread far enough to put a whole organization at risk. Point products that don't integrate with the rest of your security stack mean more policy sets to manage, and they can slow down your adoption of new business applications while requiring extra resources to maintain.

Safe Web Access Through Integrated Protection

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. Beyond simply allowing and blocking websites, Palo Alto Networks URL Filtering uses machine learning to identify and prevent new and unknown attacks inline, blocking threats before your users can even access them.

The service analyzes URLs and classifies them into benign or malicious categories, which you can easily build into your Next-Generation Firewall policy for total control of web traffic. These categories trigger complementary capabilities across the Next-Generation Firewall platform, enabling additional layers of protection, such as targeted SSL decryption and advanced logging. Alongside its own analysis, URL Filtering uses shared threat information from WildFire® malware prevention service and other sources to automatically update protections against malicious sites.

Key Capabilities

Machine Learning-Powered Prevention

The URL Filtering subscription stops new threats before your users can access them. Enabling machine learning directly on your Next-Generation Firewall, it stops never-before-seen phishing and JavaScript attacks inline, preventing them from being unleashed on your organization. It identifies and prevents malicious URLs instantly, before they have a chance to infect your organization.

Total Control of Web Content

Web policy is simply an extension of your firewall policy. Your Next-Generation Firewall uses URL Filtering to identify URL categories, assign risk ratings, and apply consistent policy. Multiple URL categories and risk ratings can be combined in nuanced policies, allowing for precise, exception-based enforcement, simplified management, and granular control of web traffic through a single policy table. You can block dangerous sites that may be used in phishing attacks, exploit kit delivery, or C2 while still allowing employees the freedom to access web resources they need for business purposes.

Selective Web Traffic Decryption

Targeted decryption helps you further reduce risk. You can establish policies to selectively decrypt TLS/SSL-encrypted web traffic, maximizing your visibility into potential threats while keeping you compliant with data privacy regulations. Specific URL categories, such as social networking, web-based email, or content delivery networks, can be designated for decryption, while transactions to and from other types of sites, such as those of governments, banking institutions, or healthcare providers, can be designated to remain encrypted. You can implement simple policies that enable 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.

Credential Phishing Prevention

Protect user logins and passwords in real time. URL Filtering analyzes potential credential phishing pages, conclusively identifying them and preventing access through the "phishing" URL category. In an industry first, URL Filtering detects and prevents in-progress phishing attacks, preventing credential theft, by controlling sites to which users can submit corporate credentials based on the site's URL category—all with zero false positives. This enables you to block users from submitting credentials to untrusted sites while still allowing them to submit credentials to corporate and sanctioned sites.

Customizable Categories

Tailor categories and policies to organizational needs. 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 your organizational requirements and fine-tune security policies, your administrators can establish custom categories by combining multiple existing categories to create new ones. For example, combining the "high-risk," "financial-services," and "newly-registered-domain" categories would create a powerful new category, enabling policy to be enacted upon any site that meets these criteria.

Analysis of Cached Results and Translation Site Filtering

Maintain tight control 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:** URL Filtering policies are applied when end users attempt to view the cached results of web searches and internet archives.
- **Translation site filtering:** URL Filtering policies are applied to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.

Safe Search Enforcement

For strict control over search results, Safe Search Enforcement allows you to prevent inappropriate content from appearing in users' search results. With this feature enabled, only Google, Yandex, Yahoo, or Bing searches with the strictest safe search options set will be allowed, and all other searches can be blocked.

Customizable End User Notifications

Each organization has a different approach to informing users when they attempt to visit webpages that are blocked according to policy and the associated URL Filtering profile. Administrators can notify users of a 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 control options when users attempt to access risky pages:

- **Continue** displays a customized warning page with a "Continue" button. 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.
- **Override** requires users to enter a configurable password to create a policy exception and continue. This allows users to access potentially critical sites with approval from the administrator.

The Power of Palo Alto Networks Security Subscriptions

Advancing Prevention for Web Security

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity.

Seamlessly integrated with our industry-leading Next-Generation Firewall platform, our cloud-delivered security subscriptions coordinate intelligence and provide protections across all attack vectors, providing best-in-class functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats.

Benefit from URL Filtering or any of our security subscriptions:

- **Threat Prevention:** Go beyond a traditional intrusion prevention system (IPS) to automatically prevent all known threats across all traffic in a single pass.
- **WildFire:** Ensure files are safe with automatic detection and prevention of unknown malware with industry-leading cloud-based analysis.
- **DNS Security:** Disrupt attacks that use DNS for C2 and data theft without requiring any changes to your infrastructure.
- **IoT Security:** Protect Internet of Things (IoT) and OT devices across your organizations with the industry's first turnkey IoT security solution.
- **GlobalProtect™ network security for endpoints:** Extend Next-Generation Firewall capabilities to your remote users to provide consistent SaaS Security everywhere in your environment.

Operational Benefits

The URL Filtering subscription enables you to:

- **Benefit from shared intelligence.** Take advantage of best-in-class web security with easy-to-use application- and user-based policies, and tight integration with Threat Prevention and WildFire.
- **Maintain total control over web traffic.** Use URL categories to automatically trigger advanced security actions, such as selective TLS/SSL decryption for suspicious sites.
- **Automate your security.** Policy is applied to URL categories automatically, requiring no analyst intervention.
- **Gain insight into user and URL activity.** IT departments can get visibility into URL Filtering and related web activity through a set of predefined or fully customized URL Filtering reports.

	URL Filtering	Advanced URL Filtering
URL filtering database	✓	✓
ML-powered web categorization	✓	✓
Reputation/Risk ratings	✓	✓
Domain history analysis	✓	✓
Multi-category support	✓	✓
Criteria matching	✓	✓
Multi-language support	✓	✓
Automatic updates across all NGFWs	✓	✓
Inline ML-based URL analysis	—	✓
Inline instant prevention of malicious URLs	—	✓
Self-improving AI	—	✓
Anti-evasion measures	—	✓

Table 1: 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
Blocking high-risk file types	Prevent upload/download of executable files or potentially dangerous file types
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.

Table 2: Privacy and Licensing Summary	
Privacy with URL Filtering Subscription	
Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.
Licensing and Requirements	
Requirements	To use Palo Alto Networks URL Filtering subscription, you will need: • Palo Alto Networks Next-Generation Firewalls running PAN-OS 8.1 or later • Palo Alto Networks Threat Prevention license
Recommended Environment	Palo Alto Networks Next-Generation Firewalls deployed in any internet-facing location, as threats involving phishing, credential theft, and C2 require external connectivity.
URL Filtering License	URL Filtering requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks Next-Generation Firewalls. It is also available as part of the Palo Alto Networks Subscription ELA, VM-Series ELA, or Prisma Access.

paloalto NETWORKS

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