Advanced URL Filtering

Best-in-Class Web Protection

Safeguarding the Web in Real Time

As applications move to the cloud and people work from anywhere, it's becoming more important—and more difficult—to secure the web. Web-based attacks like phishing and fileless attacks are coming at higher volume, greater speed, and increased sophistication, yet many web security solutions only depend on databases of known malicious webpages that are quickly overrun by the thousands of new threats created every day.

Palo Alto Networks Advanced URL Filtering provides best-in-class web protection for the modern enterprise. Bringing together the best of both worlds, Advanced URL Filtering combines our renowned malicious URL database capabilities with the industry's first real-time web protection engine powered by machine learning (ML). Now, you can automatically detect and prevent new malicious and targeted web-based threats instantly. Welcome to real-time protection.

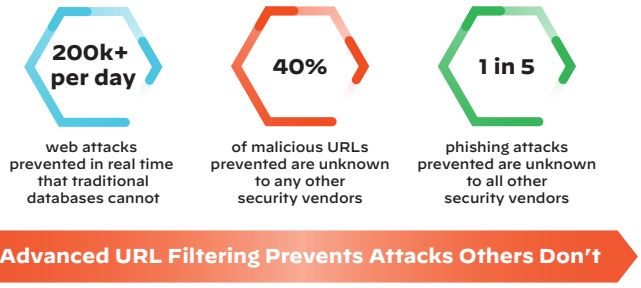

Figure 1: Advanced URL Filtering detects the most damaging web-based attacks aimed at enterprises networks today

The Advanced URL Filtering Difference

Built in the cloud, Advanced URL Filtering is a subscription service that works natively with your Palo Alto Networks Next-Generation Firewall (NGFW) to secure web access against threats such as phishing, malware, and command-and-control (C2).

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

- **Superior protection against web-based attacks** with the combined power of our URL database stopping known threats and our industry-first inline web protection engine categorizing as well as blocking new malicious URLs in real time, even when content is cloaked from crawlers. Advanced URL Filtering prevents more than 200,000 attacks per day that traditional databases cannot, in real time.
- **Industry-leading phishing protections** that tackle the most common causes of breaches.
- **Total control of your web traffic** through fine-grained controls and policy settings that enable you to automate security actions based on users, risk ratings, and content categories.
- **Maximum operational efficiency** by enabling web protection through the Palo Alto Networks platform.

Business Benefits

- **Block new malicious sites.** Advanced URL Filtering categorizes and blocks never-before-seen malicious URLs in milliseconds, before they have a chance to infect your network and end users.
- **Leverage consistent security policies and capabilities.** Deploy Advanced URL Filtering with hardware appliances, on virtual environments, or in the cloud with the same set of policies and security consistently applied.
- **Eliminate security silos and keep users safe.** We can help you attain proper security posture 30% faster compared to point solutions.
- **Minimize operational expenditure.** Palo Alto Networks cloud-delivered security services reduce the need for standalone solutions, saving US$9.9 million over three years.[1]
- **Safeguard against phishing.** Layers of prevention protect your organization from known and brand-new phishing sites by stopping credential phishing in real time.
- **Support regulatory compliance and acceptable use.** Ensure your organization stays compliant with internal, industry, and government regulatory policies.

Key Capabilities

Real-Time Protection from New Malicious Webpages

At Palo Alto Networks, we saw more than 56 million new malicious webpages in 2020, an increase in volume of more than 84% compared to 2019. With so many new threats, practically every one of them has never been seen before when it hits your network.

1. "The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN," Forrester, January 2021, https://start.paloaltonetworks.com/2021-forrester-tei-report-network-security.html.

In addition, 40% of malicious URLs come from legitimate domains,[2] as adversaries look to embed threats in websites that have largely been deemed trustworthy. URLs change from benign to malicious frequently, and unless your solution is constantly analyzing them, that leaves you exposed. Modern organizations can no longer depend solely on static or slow-to-update databases to keep pace. A new approach is necessary.

Advanced URL Filtering takes web protection to the next level with the ability to detect and block new threats before your users can access them. Cloud-based inline ML analyzes real web traffic, categorizing and blocking malicious URLs in milliseconds—before they have a chance to infect your organization. Our ML models are retrained frequently, ensuring the most up-to-date detection intelligence against new web-based threats. Meanwhile, our extensible cloud-based architecture ensures you can take advantage of the latest innovative detection modules on the fly without going through a painful update process.

It's time to move beyond the overreliance on offline crawling and databases that take too long to update. Advanced URL Filtering takes that step, delivering the industry's first inline web protection engine capable of detecting never-before-seen web-based threats and preventing them in real time.

Anti-Evasion

Modern adversaries have evolved to avoid security measures, and now 87% of phishing kits sold on the dark web include at least one type of evasive technique. The most common of these techniques, called cloaking, capitalizes on the fact that many web security solutions rely solely on offline crawling of webpage content to determine whether a threat exists. Attackers may actively block connections from specific IP addresses and hosts they know to be security companies or reroute them to benign content.

Advanced URL Filtering goes beyond webpage crawling to analyze URL strings in live web traffic, disrupting attackers and identifying the true nature of malicious sites hiding behind evasive techniques.

Phishing Protection

One of the oldest tricks in the book, phishing continues to pose a challenge for enterprise organizations. A new phishing site launches every 20 seconds,[3] and phishing constitutes more than 80% of reported security incidents[4] as well as 22% of successful breaches.[5]

Phishing is a constant threat, with new phishing sites able to be set up and taken down in minutes. With Advanced URL Filtering, you're protected from millions of known phishing pages, but it's also critical to detect new phishing pages instantly and accurately, before they can claim their first victim. We incorporate layers of innovative detection capabilities to provide the most comprehensive phishing protection available, including:

- Inline ML-based URL analysis for real-time detection of never-before-seen phishing attacks
- The industry's only real-time credential theft prevention
- ML-based image analysis
- Newly registered domain analysis
- Advanced JavaScript detection for phishing and malware
- Phishing redirection chain analysis
- Fake CAPTCHA interaction analysis

Total Control of Web Traffic

Web policy is simply an extension of your firewall policy. Your Palo Alto Networks NGFW uses Advanced 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 set. 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.

Operational Efficiency

Reduce the total cost of your security stack and maximize operational efficiency by enabling web protection through the Palo Alto Networks platform. Because of its cloud architecture, Advanced URL Filtering eliminates the need to deploy and manage additional appliances for web protection—you simply turn it on through the NGFW. Our cloud-delivered security services reduce the need for standalone solutions, saving US$9.9 million over three years and reducing risk by 45%.[6] Using a platform where each security capability enhances the next, you can achieve proper security posture 30% faster compared to point solutions.

The Power of Palo Alto Networks Security Subscriptions

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 NGFW platform, our cloud-delivered security subscriptions coordinate intelligence

2. "2019 Webroot Threat Report," Webroot, February 22, 2019, https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf.
3. "Mobile Threat Landscape Report 2020," Wandera, accessed May 6, 2021, https://www.wandera.com/mobile-threat-landscape.
4. "Top cybersecurity facts, figures and statistics," CSO from IDG, March 9, 2020, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.
5. "2020 Data Breach Investigation Report," Verizon, accessed May 3, 2021, https://enterprise.verizon.com/resources/reports/dbir.
6. Forrester Total Economic Impact study.

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 Advanced URL Filtering or any of our security subscriptions including:

- **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 organization with the industry's first turnkey IoT security solution.
- **GlobalProtect™**: Extend NGFW capabilities to your remote users to provide consistent security everywhere in your environment.

Operational Benefits

The Advanced 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, alongside 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.** Save time as policy is applied to URL categories automatically, requiring no analyst intervention.
- **Gain insight into user and URL activity.** Enable your IT department to gain visibility into URL filtering and related web activity through a set of predefined or fully customized reports.

Table 1: Advanced URL Filtering Features

Feature	Description
Inline Real-Time Web Threat Prevention	Uses cloud-based inline ML to analyze real web traffic, categorizing and blocking malicious URLs in real time. ML models are retrained frequently, ensuring protection against new and evolving never-before-seen threats (e.g., phishing, exploits, fraud, C2).
Anti-Evasion Measures	Protects against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding.
URL Database	Maintains hundreds of millions of known malicious and benign URLs categorized through a combination of static, dynamic, machine learning, and human analysis.
Content Categories	Classifies websites based on site content, features, and safety, and includes more than 70 benign and malicious content categories.
Risk Ratings	Scores URLs on a variety of factors to determine risk. These security-focused URL categories can help you reduce your attack surface by providing targeted decryption and enforcement for sites that pose varying levels of risk but are not confirmed malicious.
Multi-Category Support	Categorizes a URL with up to four categories, allowing for flexible policy and the creation of custom categories.
Custom Categories	Lets you tailor categories and policies to your organization's needs. Although Advanced 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 requirements and fine-tune policies, administrators can create new custom categories by combining multiple existing categories.
Real-Time Credential Theft Protection	Detects and prevents credential theft by controlling sites to which users can submit corporate credentials based on the site's URL category. This allows you to block users from submitting credentials to untrusted sites in real time while still allowing users to only submit credentials to corporate and sanctioned sites.
Phishing Image Detection	Uses ML models to analyze images in webpages to determine whether they are imitating brands commonly used in phishing attempts.
Criteria Matching	Allows you to designate multiple policy action types based on URL categories or criteria. Beyond simply blocking or allowing sites, policy examples may include selective SSL decryption, advanced logging, blocking downloads, or preventing credential submission.

Table 1: Advanced URL Filtering Features (continued)	
Feature	**Description**
Selective SSL Decryption	Helps you further reduce risk with targeted decryption. Policies can be established to selectively decrypt TLS/SSL-encrypted web traffic, maximizing visibility into potential threats while keeping you compliant with data privacy regulations. Specific URL categories (e.g., social networking, web-based email, content delivery networks) can be designated for decryption while transactions to and from other types of sites (e.g., those of governments, banking institutions, 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.
Translation Site Filtering	Applies URL Filtering policies to URLs that are entered into language translation websites (e.g., Google Translate) as a means of bypassing policies.
Search Engine Cached Results Prevention	Applies URL Filtering policies when end users attempt to view the cached results of web searches and internet archives.
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	Enables administrators to notify users of a violation using a custom block page. These pages may include options to present a warning and allow the user to continue or require a configurable password that creates a policy exception.
Multilingual Support	Supports crawling and analysis in 41 languages.
Reporting	Provides visibility into Advanced URL Filtering and related web activity through a set of predefined or fully customized URL Filtering reports.

Table 2: Privacy and Licensing Summary	
Privacy with Advanced 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 the Palo Alto Networks Advanced URL Filtering subscription, you will need Palo Alto Networks Next-Generation Firewalls running PAN-OS 9.0 or later.
Recommended Environment	Use Advanced URL Filtering with Palo Alto Networks Next-Generation Firewalls deployed in any internet-facing location, as malware, grayware, phishing, credential theft, and C2 require external connectivity.
Advanced URL Filtering License	Advanced 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 FirewallFlex.

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