Advanced URL Filtering

Ensure Safe Access to the Web with the Industry's First Solution to Stop Unknown Web-Based Attacks in Real Time and Prevent 40% More Threats Than Traditional Web Filtering Solutions

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 hundreds of 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 deep learning. Now, you can automatically detect and prevent new malicious and targeted web-based threats instantly. Welcome to real-time protection.

Palo Alto Networks Advanced URL Filtering

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

Advanced URL Filtering uses Palo Alto Networks patent-pending Precision AI™ technology inline to analyze URL strings and web content 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 various form factors, 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 Palo Alto Networks industry-leading malware prevention service Advanced WildFire® and other Cloud-Delivered Security Services to automatically update protections against malicious sites. Advanced URL Filtering delivers:

- **Superior protection against web-based attacks** with a URL database to stop known threats and an ML-powered, cloud-delivered web security engine that categorizes and blocks new and even cloaked malicious URLs in real time, preventing 40% more threats.
- **Industry-leading phishing protections** that combat the latest and most sophisticated phishing techniques to stop the most common cause 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.

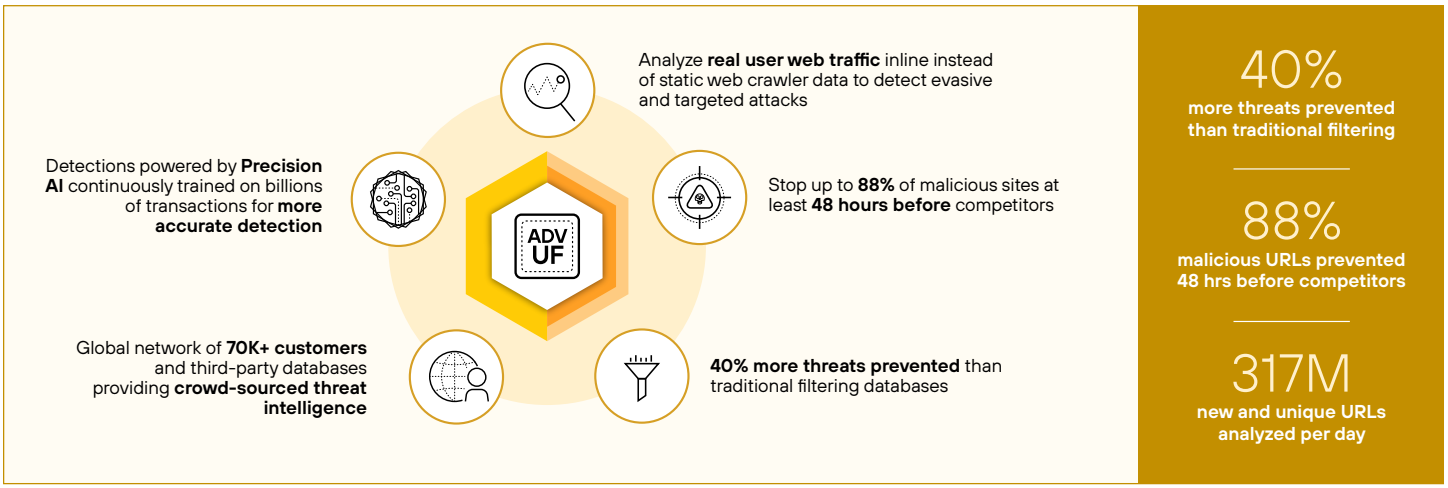

Figure 1: Palo Alto Networks Advanced URL Filtering

Business Benefits

- **Powered by Precision AI**: Advanced URL Filtering leverages the three core AI technologies—machine learning, deep learning, and generative AI—and pairs them with high-fidelity threat data to better detect and prevent rapidly evolving phishing attacks, all in real time.
- **Inline protection**: Protection from new and unknown web-based attacks in less than 100 milliseconds to prevent patient zero.
- **Detect evasive and targeted attacks**: Increase detection of evasive and targeted attacks by detecting real web traffic and not web crawler data.
- **Cloud-native service**: Designed to expand and scale capabilities over time.
- **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$12.85 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

Powered by Precision AI

Palo Alto Networks harnesses the full potential of AI with its Precision AI technology. From machine learning to deep learning and generative AI, Advanced URL Filtering, along with other Palo Alto Networks Cloud-Delivered Security Services, takes the best of each technology and integrates it to better detect and prevent rapidly evolving threats. Key attributes of Precision AI consist of AI-powered security models, high-fidelity data, and action in real time.

1. *The Total Economic Impact™ Of Palo Alto Networks Cloud-Delivered Security Services*, Forrester Consulting, November 2023.

AI-Powered Security Models

To be effective in cybersecurity, Precision AI must be as close to 100% accurate as possible to find malicious activity and avoid alerting on false positives. However, this becomes extremely challenging given the evasive and sophisticated nature of today's threat actors, who use various tools and techniques to obfuscate their threats from security scanners. To successfully identify threats and combat attackers' techniques, security-specific combinations of AI technologies are required. From its inception, Advanced URL Filtering has used machine learning to analyze structured data and identify malicious web traffic. Thereafter, deep learning was integrated to analyze larger volumes of unstructured data that enabled security models to better predict evasive and never-before-seen threats. And now, with the mass adoption of generative AI by threat actors, security models are trained on threat samples generated by AI to also identify AI-generated attacks.

High-Fidelity Data

AI is only as effective as the data it trains on. Palo Alto Networks Precision AI leverages rich and diverse threat data to continuously train its security models, giving Advanced URL Filtering comprehensive insights into the never-before-seen phishing attacks seen every day. Data sources include threat intelligence collected from over 70,000 global customers, third-party databases, and real user web traffic.

Real-Time Action

Given the speed at which today's threat actors operate, security can no longer solely rely on threat signature databases, which can only prevent known threats. Instead, security must operate in real time. Analysis must occur inline and be done on real network traffic to see through evasion techniques and to identify net new threats. Additionally, security must utilize the power and scalability of the cloud to deliver a verdict instantly and prevent anything malicious before patient zero is infected.

With Precision AI, Advanced URL Filtering helps customers stay ahead of today's adversaries. Its inline AI-powered models continuously train on rich and diverse threat data to gain insights on new and advanced phishing techniques. These insights make Advanced URL Filtering the industry's first web security engine to stop unknown phishing attacks in real time, allowing Palo Alto Networks to deliver 40% more phishing protection than traditional filtering databases.

Inline Protection from New Malicious Webpages

At Palo Alto Networks, we identify 347,000 new malicious pages every day. With so many new threats, practically every one of them has never been seen before when it hits your network. In addition, 40% of malicious URLs come from legitimate domains, 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 required.

Advanced URL Filtering takes web protection to the next level with the ability to detect and block new threats in real time, preventing patient zero. Inline AI-powered security models delivered from the cloud perform real-time analysis of live web traffic instead of web crawler data, categorizing and blocking malicious URLs in milliseconds—before they have a chance to infect your organization. Our security models are continuously trained, ensuring the most up-to-date detection intelligence against new and emerging web-based threats. Meanwhile, our extensive cloud-based architecture ensures you can take advantage of the latest innovative detection modules on the fly without going through a painful update process.

Antievasion

Modern adversaries have evolved to avoid security measures, and now 90% of phishing kits sold on the dark web include at least one type of evasive technique. These techniques include cloaking, CAPTCHA challenges, meddler-in-the-middle phishing, SaaS-hosted phishing, and much more, capitalizing 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 live web content, 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. In fact, studies have shown that 91% of security incidents are caused by phishing,[2] while 84% of organizations in 2022 were successfully phished.[3]

Phishing is a constant threat, and thanks to hacker-friendly resources such as phishing as a service, automation, and black hat AI tools (WormGPT, FraudGPT, etc.), attackers are able to generate and distribute a vast number of new phishing pages with ease. With Advanced URL Filtering, you're protected from millions of known phishing pages, but it's also critical to detect new and never-before-seen phishing pages instantly and accurately before they can claim their first victim. We continuously add new and innovative AI-powered detection capabilities to prevent the latest sophisticated techniques used by attackers and provide the most comprehensive phishing protection available, including:

- Inline AI-powered web content analysis for real-time zero-day detection.
- Industry's first real-time credential theft prevention.
- ML-based image analysis.
- Static and dynamic analysis.
- Deep recursive analysis.
- Deep learning convolutional neural networks (CNN) model.
- Appended attack detection.
- ML-powered domain analysis.
- Deobfuscating JavaScript engine to stop data exfiltration attempts.
- Phishing redirection chain analysis.
- Fake CAPTCHA interaction analysis.

Total Control of Web Traffic

Web policy is simply an extension of your security policies. Your Palo Alto Networks NGFW or Prisma Access 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 the web resources they need for business purposes.

2. "91% of all cyber attacks begin with a phishing email to an unexpected victim," Deloitte, January 9, 2020.
3. *2023 State of the Phish*, Proofpoint, May 19, 2023.

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 or Prisma Access. Our Cloud-Delivered Security Services reduce the need for standalone solutions, saving US$12.85 million over three years and reducing risk by 50%.[4] Using a platform where each security capability enhances the next, you can see ROI in less than six months.[5]

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 and Prisma Access platforms, our Cloud-Delivered Security Services 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 Advanced URL Filtering or any of our security subscriptions.

Table 1: Palo Alto Networks Cloud-Delivered Security Services

Product	Description
Advanced Threat Prevention	Stop known and unknown exploits, malware, spyware, and command-and-control (C2) threats with the industry's first prevention of zero-day attacks, stopping 60% more zero-day injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
Advanced WildFire	Ensure safe access to files with the industry's largest malware prevention engine, stopping up to 22% more unknown malware and turning detection into prevention 180X faster than competitors.
Advanced URL Filtering	Ensure safe access to the web and prevent 40% more threats in real time than traditional filtering databases with the industry's first prevention of known and unknown phishing attacks, stopping up to 88% of malicious URLs at least 48 hours before competitors.
Advanced DNS Security	Protect your DNS traffic and stop advanced DNS-layer threats, including DNS hijacking, all in real time with 2X more DNS-layer threat coverage than competitors.
NG-CASB	Discover and control all SaaS consumption in your network with visibility into 60K+ SaaS apps and protect your data with 28+ API integrations.
IoT/OT Security	Secure your blind spots and protect every connected device unique to your vertical with the industry's most comprehensive Zero Trust solution for IoT devices, discovering 90% of devices within 48 hours.
AI Access Security™	Enable the safe use of GenAI apps with real-time visibility of 600+ GenAI apps, access control, and data protection.

4. *The Total Economic Impact™ Of Palo Alto Networks Cloud-Delivered Security Services*, November 2023.
5. Ibid.

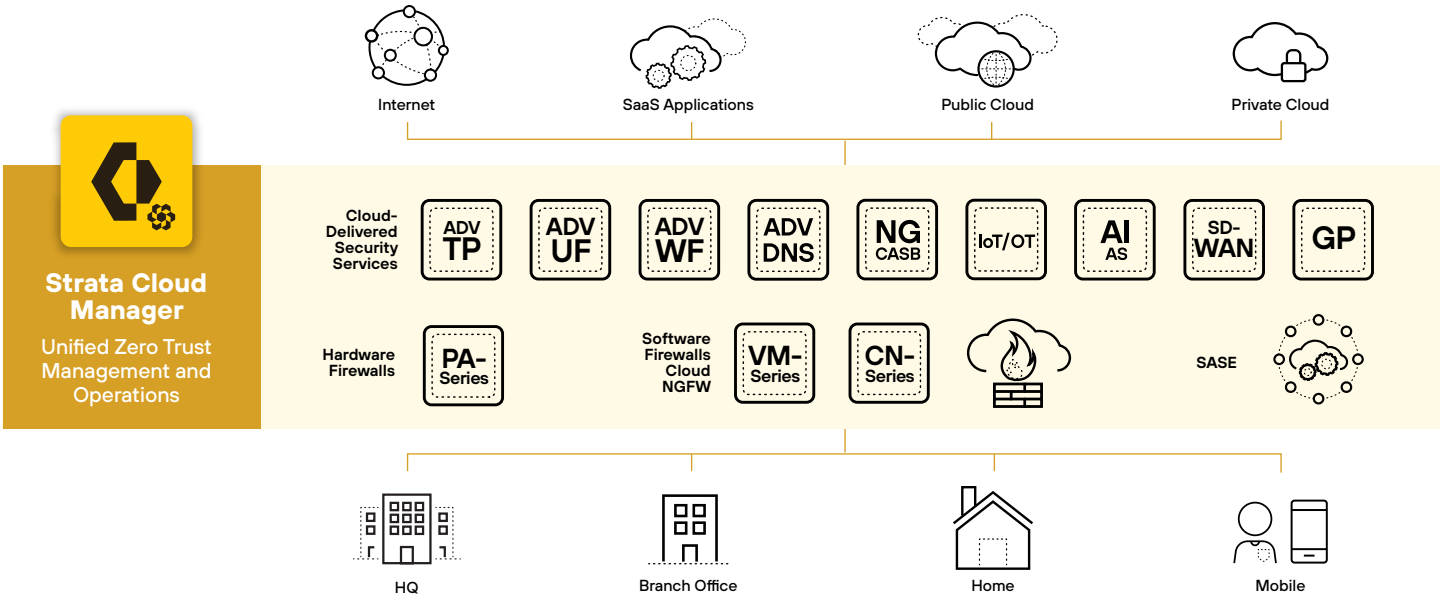

Figure 2: Palo Alto Networks Strata Security Platform

Table 2: Advanced URL Filtering Features

Feature	Description
Precision AI	Use of machine learning, deep learning, and generative AI to train security models for more accurate detection of advanced and never-before-seen DNS-layer threats, including those generated by AI.
Real-Time Web Protection	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).
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, safety, and includes more than 70 benign and malicious content categories, with more continuously being added.
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 aren't confirmed malicious.
Multicategory 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 or creating a category exception list.
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 with zero false positives.
Phishing Image Detection	Uses ML models to analyze images in webpages to determine whether they're 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 2: 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 Advanced 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 Advanced 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 Advanced URL Filtering reports.

Table 3: 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'll need Palo Alto Networks Next-Generation Firewalls running PAN-OS® 9.0 or later. Real-time web analysis is only supported on PAN-OS 10.2 Nebula and later.
Recommended Environment	Use Advanced URL Filtering with Palo Alto Networks Next-Generation Firewalls deployed in any internet-facing location, as ransomware, 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 can also be available as part of an Enterprise Licensing Agreement or Software NGFW Credits.

Resources

- Advanced URL Filtering Privacy datasheet
- Advanced URL Filtering webpage

About This Datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

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

strata_ds_advanced-url-filtering_100324