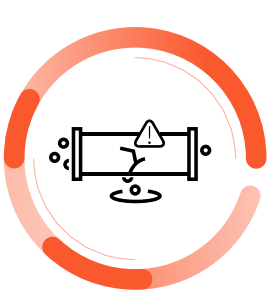
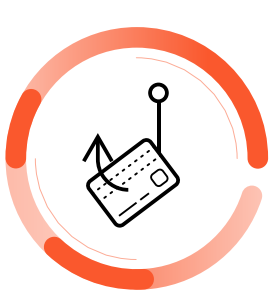
Enhance Your Web Security with Advanced URL Filtering

As applications move to the cloud and people work from anywhere, it is more important than ever to secure your access to the web. Modern web-based threats like phishing are rapidly evolving, making them more evasive and unknown to existing security solutions. Organizations need a solution that can successfully prevent today's new and evasive web-based threats, all in real time.



90%
of data breaches were caused by phishing[1]



93%
of organizations were successfully phished in 2021[2]

$14.8M
Average cost of a phishing attack[2]

Today's security solutions struggle to keep up with the evolution of today's web-based threats simply because attackers are using more evasive techniques to bypass security and relying on traditional URL filtering databases is no longer sufficient since it can't protect against unknown threats.

Palo Alto Networks Advanced URL Filtering Prevents Attacks Others Don't

Palo Alto Networks Advanced URL Filtering subscription provides best-in-class web protection for the modern enterprise. Advanced URL Filtering combines it's renowned malicious URL database capabilities with the industry's first real-time web protection engine powered by deep learning, allowing you to prevent new and evasive web-based attacks in real time.

40%
more threats prevented than traditional web filtering databases[3]

12M+
web-based threats prevented per day[3]

76%
of threats discovered up to 24 hours before other vendors[3]

The Power of Deep Learning

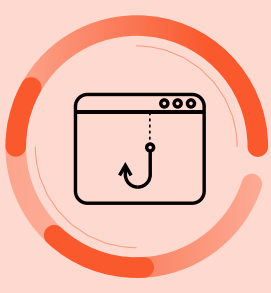
Today's web security solutions rely heavily on traditional URL filtering databases that have the ability to block known malicious URLs, but lack the capabilities to prevent the new and evasive web-based threats we see today. In order to protect your organization from modern web-based attacks, solutions need to be able to analyze live customer traffic as it enters their network, and prevent any threats in real time.

Palo Alto Networks Advanced URL Filtering subscription is the only web security solution in the industry that uses deep learning capabilities to prevent unknown attacks in real time. With the power of deep learning, Advanced URL Filtering has the analysis capabilities and processing power to analyze large volumes of real world threat data inline, and enforce real-time protection against evasive attacks.

Enable Selective SSL Decryption

99%
of the browsing time on Chrome is spent on HTTPS pages[4]

48%
of sites have inadequate security[5]



83%
of phishing sites use SSL[6]

What if an encrypted site displays suspicious characteristics (for example, the domain was previously associated with malware) yet isn't overtly malicious? Put Advanced URL Filtering to work.

Implement a policy that automatically enables SSL decryption for certain sites or categories of sites such as personal blogs, file sharing sites and high-risk sites. Selective decryption enables an optimal security policy while respecting confidential traffic parameters.

Protect Against New and Evasive Threats

90% of today's phishing kits include evasive techniques[7]

127% growth of malicious web pages since 2019[8]

56M new malicious web pages in created 2021[3]

Modern web-based attacks such as phishing have largely adopted evasive techniques to successfully breach organizations. Attackers use evasive techniques such as cloaking, hiding behind CAPTCHAs and targeted attacks, to render today's security solutions ineffective. With Advanced URL Filtering, customers can benefit from detections powered by deep learning to defeat evasion techniques used in modern phishing attacks.

Leverage Security Risk Profiles

Low Risk

- Only benign history
- Previously malicious but have displayed benign activity for at least 90 days

Medium Risk

- Previously malicious but have displayed benign activity for at least 60 days

High Risk

- Previously malicious but have displayed benign activity for at least 30 days
- Hosted on bulletproof ISPs or using an ASN that has known malicious content
- Websites sharing a domain with a known malicious website
- Websites in "Unknown"

While we recommend blocking malicious categories, including malware, command-and-control, grayware, and phishing on day one, many URLs fall in the gray area between benign and malicious. Simply blocking all of them can seriously hinder business productivity. With Advanced URL Filtering, you can use risk ratings to reduce your attack surface by providing targeted decryption and enforcement for sites that pose varying levels of risk but are not confirmed malicious. Increased enforcement on URLs that may be scored as high or medium risk. For more information on how to optimize your Advanced URL Filtering subscription, we recommend you follow these best practices.

Learn more about how Advanced URL Filtering can protect your organization from new and evasive web-based threats today.

1. https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
2. https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study
3. (PAN Eng data)
4. https://transparencyreport.google.com/https/overview?hl=en
5. https://www.ssllabs.com/ssl-pulse/
6. https://www.keyfactor.com/blog/https-phishing-attacks-how-hackers-use-ssl-certificates-to-feign-trust/
7. https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service
8. https://www.paloaltonetworks.com/resources/datasheets/advanced-url-filtering