AT A GLANCE
URL FILTERING

It's no secret the web can be a dangerous place – with organizations increasingly assailed by web-based threats, including malware, phishing attacks and exploit kits. As a result, URL filtering has become a crucial component of an organization's threat prevention strategy to protect users and data.

Palo Alto Networks® URL Filtering with PAN-DB subscription service provides secure web browsing and URL access by allowing administrators to block dangerous sites that deliver malware, attempt to circumvent security controls, or are designed to steal legitimate user credentials through phishing attempts.

PAN-DB works natively with Palo Alto Networks Next-Generation Firewall to extend existing network traffic policies to web browsing activity. This enables granular control of web traffic through a single policy table, allowing for precise exception-based behavior while simplifying management. URL Filtering policies can also be enforced even when common evasion tactics, such as cached results and language translation sites, are used. Combining fast cloud URL lookups with a local cache (instead of a big database download) ensures rapid web browsing while increasing both the accuracy and relevance of the categorization.

URL Filtering and Next-Generation Security Platform

Today's stand-alone URL filtering solutions don't have the right mechanisms to prevent web-based threats because they have insufficient application visibility, can't coordinate action, and lack meaningful integration with other network defense systems to protect against the different attack stages and threat vectors.

When an attack is launched against your network, URL Filtering works with your Palo Alto Networks Next-Generation Firewall and Threat Prevention subscription to provide additional blocking capabilities. In addition to its own analysis, PAN-DB utilizes information from WildFire™ cloud-based threat analysis service, updating PAN-DB protections for malicious sites every five minutes.

Our ability to reprogram the security posture across the network, endpoint and cloud counters new threats in real time, providing organizations with superior protection against the sophistication of modern attacks. Our unique platform approach eliminates the need for multiple stand-alone security appliances and software products. Moreover, it can reduce the total cost of ownership for organizations while increasing effectiveness by simplifying their security infrastructure.

For effective and coordinated protection, we recommend deploying URL Filtering with PAN-DB, Threat Prevention and WildFire.

URL Filtering Highlights

Reduce the risk of infection from dangerous websites and protect users and data from malware, credential-phishing pages and those that carry exploit kits

- Keep protections synchronized with the latest threat intelligence through our cloud-based URL categorization for phishing, malware and undesired content
- PAN-DB works as part of Palo Alto Networks Next-Generation Security Platform to provide an integrated approach to stopping threats at every opportunity
- Enable granular policy control for web browsing activity as an extension of your application-based policies
- Full visibility and threat inspection into normally opaque web traffic through granular control over SSL decryption

AT A GLANCE
URL FILTERING

YOU NEED	WE OFFER
Protection against malicious sites exposing your people and data to malware and exploit kits	Safely enable access to the web, and discover and block access to modern threats, such as exploit kits and phishing pages. Further control your risk by blocking suspicious file types, such as portable executables (PEs), from being downloaded from URLs within specific categories with assigned risk. Establish policies to prevent file downloads, identify and allow exceptions, and employ strict threat prevention profiles to block potential exploit kits.
Protection from credential phishing	Behind Palo Alto Networks URL Filtering is sophisticated analysis technology that inspects webpages to determine whether the content and purpose is malicious in nature, including understanding how credentials are used. This technology informs our phishing URL category and protects users from becoming victims of credential-phishing attacks.
Coordinated protection to prevent threats at every opportunity	Policies, traffic, threat logs and protections provided are automatically coordinated to stop attacks before compromise occurs, through native integration of PAN-DB with Palo Alto Networks Next-Generation Firewall, Threat Prevention and WildFire. PAN-DB receives updates from WildFire every five minutes, with malicious URLs associated with new malware and other threat intelligence, ensure your strongest security posture at all times.
Granular, on-box SSL decryption	Palo Alto Networks firewalls include on-box SSL decryption, which extends to the web through URL Filtering. By using PAN-DB URL categories to selectively decrypt web traffic, we provide you with the visibility and seamless inspection you need to maintain security while protecting users' personal privacy and data integrity.
To comply with acceptable use policies	Granular URL categorization of web content enables you to control the interaction of your users with online content that is adequate and appropriate. We also provide customizable alerts and notification pages when users navigate to sites often used by attackers, such as dynamic DNS, parked domains and unknown sites, helping educate users and reduce the risk of infection from dangerous websites.

"OUR PRIME REQUIREMENT WAS TO BLOCK RANSOMWARE AND OTHER ADVANCED CYBERTHREATS. WITH SO MUCH MORE SSL TRAFFIC EXPECTED, WE ALSO WANTED GREATER VISIBILITY OF ALL TRAFFIC, AND WE NEEDED BETTER URL FILTERING THAT WE COULD BASE ON INDIVIDUAL USERS, NOT JUST IP ADDRESSES. PALO ALTO NETWORKS MET ALL OUR SECURITY NEEDS ON A SINGLE PLATFORM THAT OFFERED EASY INTEGRATION WITH ACTIVE DIRECTORY AND SIMPLE ADMINISTRATION."

— Bojan Vujanovic
Network Administrator, DELTA HOLDING