URL FILTERING WITH PAN-DB

Enable Safe Web Access for All Users

URL Filtering with PAN-DB enables safe web access, protecting users from dangerous websites, malware sites, credential-phishing pages and attacks attempting to leverage web browsing to deliver threats. The service is a native component of the Next-Generation Security Platform, providing best-in-class security without adding operational burden.

URL Filtering with PAN-DB:

- Prevent attacks that leverage the web as an attack vector, including phishing links in emails, phishing sites, HTTP-based command and control, malware sites, and pages that carry exploit kits.
- Automated updates for newly discovered attacks with updates from the Palo Alto Networks® WildFire™ cloud-based threat analysis service every five minutes, blocking malicious URLs as they are discovered.
- Enable SSL decryption with granular policy that balances the inspection of potentially harmful content, while allowing sites with sensitive, personal information to remain encrypted.
- Enable granular policy control for web browsing activity as an extension of your application-based policies.
- Maintain web performance by combining fast cloud URL lookups with a local cache to ensure rapid web browsing while increasing the accuracy and relevancy of categorization.

The web is one of the most common attack vectors for threat delivery, exposing organizations to security risks, including malware propagation, credential theft and data loss. URL filtering is a crucial component of an organization's threat prevention strategy.

The web can be a dangerous place. Uncontrolled web surfing or email link clicking can quickly lead to a security incident. Stand-alone URL filtering solutions don't have the right mechanisms to adequately control web browsing or prevent 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.

Controlling web application activity requires a natively integrated approach that implements rules for web browsing as a natural extension of existing network traffic policy, enabling control of web browsing activity and any inherent threats, including applications commonly used to bypass traditional security mechanisms.

Coordinated Protection Across the Attack Lifecycle

PAN-DB works as part of Palo Alto Networks Next-Generation Security Platform to provide an integrated approach to stopping threats at every opportunity. Policies, traffic, threat logs and protections are automatically coordinated to stop attacks before compromise occurs.

Palo Alto Networks Next-Generation Firewall (NGFW) natively classifies all traffic by application, including web applications, and ties that traffic to the user, regardless of physical location or IP address, and then inspects all allowed traffic and web content for threats. The application, content and user — the business elements that run your organization — are then used as the basis of all security policies. By addressing traffic visibility and control from both the application and web content perspective, your organization is safeguarded from a full spectrum of regulatory, compliance, appropriate use and security risks.

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

Extend Firewall Policy to Control Web Content

As an extension to the application visibility and control enabled by App-ID™ application identification technology, URL categories can be used as match criteria for web traffic within your firewall policies. When web traffic is seen, your NGFW, with the help of PAN-DB, identifies the URL category and applies policy just as it does for all other application traffic. Instead of creating rules that are limited to either allowing all or blocking all web behavior, the URL category acts as a granular matching mechanism, allowing for precise exception-based behavior, simplified management, and the flexibility to granularly control web traffic through a single policy table. Examples of how URL categories can be used in policies include:

- Prevent file download/upload for URL categories that represent higher risk (e.g., allow access to personal email, but prevent upload/download of executable files or other potentially dangerous file types from such sites to limit malware propagation).
- Identify and allow exceptions to general security policies for users who may belong to specific groups within Active Directory® (e.g., deny access to hacking sites for all users, yet allow access to users who belong to the security group).
- Allow access to personal websites and blogs, but decrypt if SSL is used, and employ strict Threat Prevention profiles to block potential exploit kits embedded in forums and posts.

Prevent Credential Phishing Attempts

Phishing attacks are some of the most prevalent, dangerous and malicious techniques available to adversaries aiming to steal legitimate user credentials. When stolen, genuine credentials provide attackers with "authorized" access to the network, which is less likely to trip any alarms or alert administrators, which, in turn, means more time for attackers to accomplish their objectives, potentially stealing sensitive information or causing harm to an organization.

PAN-DB analyzes potential credential phishing attempts through static and dynamic analysis, as well as advanced machine learning models, conclusively identifying and preventing them through the "phishing" URL category. Additionally, the PAN-DB phishing category is informed about indicators of compromise from a variety of sources, including third-party feeds; Unit 42, the Palo Alto Networks threat research team; and WildFire.

Beyond identifying and preventing potential credential phishing threats from being delivered to users, PAN-DB offers unique capabilities to prevent credentials from being unwittingly sent to adversaries by users. Leveraging the User-ID™ user identification technology capabilities of the Next-Generation Firewall, PAN-DB detects user credentials submitted into outgoing web forms, and enables policy to be set that can block the attempt, allow it, or notify the user they may be undertaking a dangerous action.

Selectively Decrypt Web Traffic

Establish policies to selectively decrypt SSL secured web traffic to gain maximum visibility into potential threats while complying with data privacy regulations. Specific URL categories, such as social networking, web-based email or content delivery networks, can be designated for SSL decryption, while transactions to and from such sites as government, banking institutions or healthcare providers can be designated to remain encrypted. Selective decryption enables optimal security posture while respecting confidential traffic parameters set by company policies or external regulations.

Tighten Controls Over Common Policy Evasion Tactics

URL Filtering policies can be enforced even when common evasion tactics, such as cached results and language translation sites, are used.

- **Search engine-cached results prevention:** A common tactic to evade controls is to access cached results within the popular search engines. URL Filtering policies are applied to cached results when end users attempt to view the cached results of Google® search and internet archive.
- **Translation site filtering:** URL Filtering policies are applied to URLs that are entered into translation sites, such as Google Translate, as a means of bypassing policies.

Safe Search Enforcement

Safe Search Enforcement allows you to prevent inappropriate content from appearing in users' search results. When this feature is enabled, only Google, Yahoo® or Bing searches with the strictest safe search option set will be allowed; all other searches can be blocked.

Customizable URL Database and Categories

To account for each organization's unique traffic patterns, on-device caches are used to store the most recently accessed URLs. Devices also automatically query a master cloud-based database for URL category information when a URL is found that is not in the cache already. Lookup results are automatically inserted into the cache for future activity. Additionally, administrators can create custom URL categories to suit their specific needs or to create specific categorizations for internally hosted websites or domains.

Customizable End-User Notification

Each organization has different requirements on how best to inform end users that they are attempting to visit a web page that is blocked, according to the corporate policy and associated URL Filtering profile. To accomplish this goal, administrators can use a custom block page to notify end users of the policy violation, which can include references to the username, IP address, the URL they are attempting to access, and its URL category, in addition to a customized message from the administrator. In order to place some of the web activity ownership back in the user's hands, administrators have two options:

- **URL Filtering continue:** When a user accesses a page that may pose a risk to the organization, a customized warning page with a "Continue" button can be presented to the user. This presents an opportunity to educate the user about the risks of the requested site and allows them to proceed if they feel the risk is acceptable.
- **URL Filtering override:** Requires a user to correctly enter a configurable password in order to create a policy exception and continue. This allows a user access to a potentially critical site with approval from the administrator.

URL Activity Reporting and Logging

A set of predefined or fully customized URL Filtering reports provides IT departments with visibility into URL Filtering and related web activity including:

- **User activity reports:** An individual user activity report shows applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period of time.
- **URL activity reports:** A variety of top 50 reports that display URL categories visited, URL users, websites visited, blocked categories, blocked users, blocked sites and more.
- **Real-time logging:** Logs can be filtered through the easy-to-use log monitoring function of the firewall administrator user interface, which uses log fields and regular expressions to analyze traffic, threat or configuration events. Log filters can be saved and exported, and for more in-depth analysis and archival, logs can also be sent to a syslog server.

Cost-Effective Deployment

Because URL Filtering with PAN-DB is enabled as a natively integrated subscription on the Palo Alto Networks Next-Generation Security Platform, it provides a scalable answer to deploying secure web gateway functionality directly within your existing network traffic policy. This architecture provides protection from web-borne threats that is automatically coordinated with our other prevention technologies to block threats at every opportunity.

The unlimited user license behind each URL Filtering subscription and the high-performance nature of the Palo Alto Networks Next-Generation Firewall means that customers can secure web activity for an entire user community while reducing operational expenditures through streamlined policy and reporting. Our unique platform approach eliminates the need for multiple, stand-alone security appliances and software products, and can reduce the total cost of ownership for organizations while increasing effectiveness, by simplifying their security infrastructure.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com