AT A GLANCE
URL FILTERING

It's no secret: the web can be a dangerous place. Uncontrolled web surfing or email link clicking can quickly lead to infection, possible data loss, and potential compliance violations. Stand-alone URL filtering deployments don't have the right mechanisms to adequately control web browsing or prevent threats because they have insufficient application visibility, can't coordinate actions, and lack meaningful integration with other solutions to protect against the different attack stages and threat vectors.

The integration of URL Filtering (PAN-DB) with WildFire™ threat intelligence service, and all other components of the Palo Alto Networks® Next-Generation Security Platform, gives organizations the assurance that their networks, endpoints and cloud services are protected by the latest threat intelligence on malware and phishing at all times.

Secure web access and protection against malware and phishing sites is a high priority to organizations today. The integration of URL Filtering (PAN-DB) into the single-pass architecture of the Palo Alto Networks next-generation firewall and WildFire automatically enhances your company's security posture and keeps it up to date. Combining fast cloud URL lookups with a local cache (instead of a big database download) significantly reduces latency and increases both the accuracy and relevance of the categorization.

Constantly updated global threat intelligence allows for fast identification and prevention of undesired content and malicious sites.

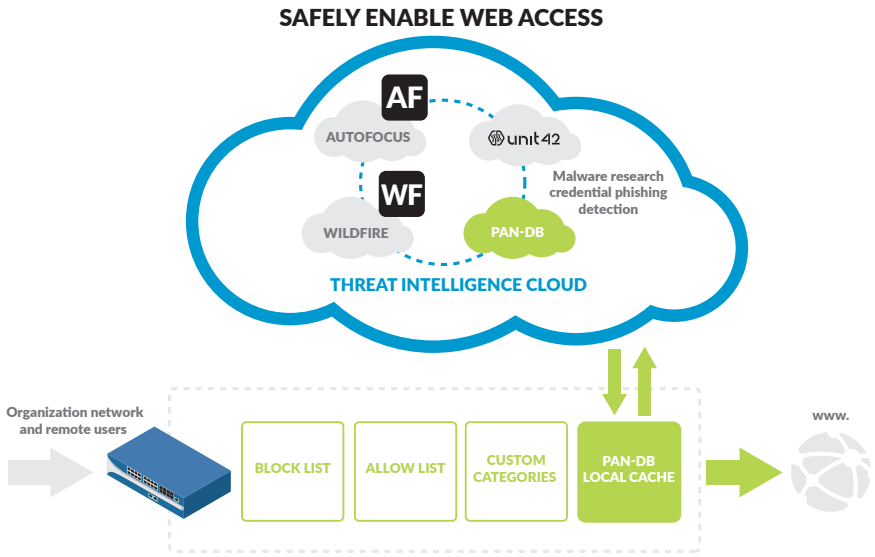
URL Filtering and the Next-Generation Security Platform

Palo Alto Networks natively integrated technologies support open communication, orchestration and visibility. Our ability to reprogram the security posture across the network, endpoint and cloud counter 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 and 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 PAN-DB URL Filtering with Threat Prevention and WildFire.

URL Filtering Highlights

- Reduce the risk of infection from dangerous websites and protect users and data from malware and credential-phishing pages
- Protection across the attack lifecycle through integration with WildFire and the Next-Generation Security Platform
- Keep protections synchronized with the latest threat intelligence through our cloud-based URL categorization for phishing, malware and undesired content
- 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
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 the Next-Generation Firewall, Threat Prevention and WildFire services. URL Filtering stops attacks that leverage the web as an attack vector, including phishing emails, drive-by downloads, and HTTP-based command and control.
Protection against malicious sites that deliver malware to unsuspecting users	PAN-DB, our cloud URL database, receives updates from WildFire every 15 minutes with malicious URLs associated with new malware and other threat intelligence that get categorized as such to provide protection against web-based malware delivery. Further control your risk by blocking suspicious file types, such as portable executables (PE files), from being downloaded from URLs within specific categories with assigned risk.
Protection from credential phishing	Behind Palo Alto Networks URL Filtering is sophisticated analysis technology that inspects web pages 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.
Granular, on-box SSL decryption	Palo Alto Networks next-generation 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 your risk management plan	Granular URL categorization of web content to allow 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.