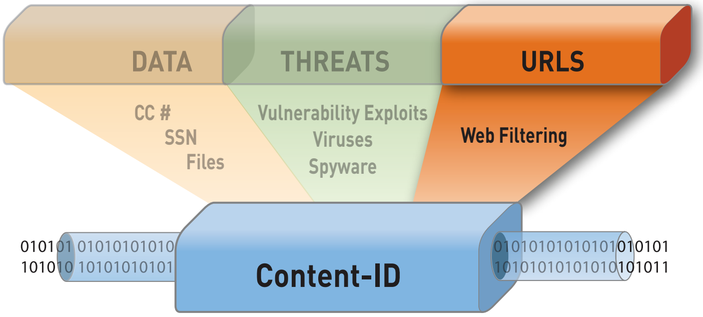
Integrated URL Filtering

Fully integrated URL filtering database enables policy control over web browsing activity, complementing the policy-based application visibility and control that the Palo Alto Networks next-generation firewalls deliver.

- Block access to non-desirable web sites to reduce security, legal and regulatory risks.
- Reduce malware incidents by prohibiting access to known malware and phishing download sites.
- Tailor web filtering control efforts with allow list, deny list and database customization.
- Facilitate SSL decryption policies such as "don't decrypt traffic to financial services sites" but "decrypt traffic to blog sites".



Today's Internet-savvy users are spending more and more time on their favorite web site or using the latest and greatest Internet application. This unfettered web surfing and application use exposes enterprises to security and business risks including propagation of threats, possible data loss, and lack of regulatory or internal policy compliance.

Stand-alone URL filtering solutions are insufficient control mechanisms because they are easily bypassed with external proxies (PHproxy, CGIproxy), circumventors (TOR, UltraSurf, Hamachi) and remote desktop access tools (Yoics!, RDP, SSH). Controlling users' application activity requires a multi-faceted approach that implements policies to control web activity and the applications that are commonly used to bypass traditional security mechanisms.

Palo Alto Networks' next-generation firewalls identify and controls more than 950 applications, irrespective of port, protocol or SSL encryption or evasive characteristic. Once identified, the application identity, not the port or protocol, becomes the basis of all security policies, resulting in the restoration of application control. Acting as the perfect complement to policy-based application control is an on-box URL filtering database that provides control over non-work related web activity. By addressing the lack of visibility and control from both the application and web perspective, enterprises are safeguarded from a full spectrum of legal, regulatory, productivity and resource utilization risks.

Policy-based Control Over Applications and Web Surfing

Tech-savvy users know how to get around URL filtering controls using applications such as TOR, Hamachi, UltraSurf, or external proxies. Palo Alto Networks identifies all of these applications and more, enabling policies to be set that block their use – a critical complimentary component to URL filtering. Once application control policies are enabled, security administrators can implement URL filtering policies to further control employee and network activity. Policies can be enabled using a combination of the following mechanisms:

- Select from 76 categories and more than 20 million URLs or create a custom list through block lists and allow lists with wildcard support.
- Specify users and groups via seamless integration with Active Directory, eDirectory, or LDAP.
- Source and destination IP address, source and destination security zone, and time-based schedule.
- Enable SSL decryption policies by allowing encrypted access to specific sites such as health, finance and shopping while decrypting traffic to all other sites such as blogs, forums, and entertainment.

Customizable URL Database and Categories

To accommodate the rapidly expanding number of URLs, as well as regional and industry-specific URLs, the 20 million on-box URL database can be augmented to suit the traffic patterns of the local user community. If a URL is detected that is not categorized by the local URL database, the firewall can request the category from a hosted 180 million URL database. The URL is then cached locally in a separate 1 million URL capacity database. In addition to database customization, administrators can create custom URL categories to further tailor the URL controls to suit their specific needs.

Customizable End-User Notification

Each enterprise has different requirements regarding how 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. The page can include references to the username, IP address, the URL attempting to be accessed and the category of the URL. In order to place some of the web activity ownership back in the users hands, administrators have two powerful options.

- URL filtering continue: When a user accesses a page that potentially violates URL filtering policy, a block page warning with a “Continue” button can be presented to the user, allowing them to proceed if they feel the site is acceptable.
- URL filtering override: Requires a user to correctly enter a password in order to bypass the block page and continue surfing.

URL Activity Reporting and Logging

A set of pre-defined 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, web sites visited, and a detailed report of all URLs visited over a specified period of time.
- URL activity reportss: A variety of top 50 reports that display URL categories visited, URL users, web sites visited, blocked categories, blocked users, blocked sites and more.
- Real-time logging: Logs can be filtered through an easy-to-use query tool that uses log fields and regular expressions to analyze traffic, threat or configuration incidents. Log filters can be saved and exported and for more in-depth analysis and archival, logs can also be sent to a syslog server.

Deployment Flexibility

The unlimited user license behind each URL filtering subscription and the high performance nature of the Palo Alto Networks firewalls means that enterprise customers can deploy a single appliance to control web activity for an entire user community without worrying about cost variations associated with user-based licensing.

paloalto NETWORKS

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Sales 866.320.4788
408.738.7700
www.paloaltonetworks.com