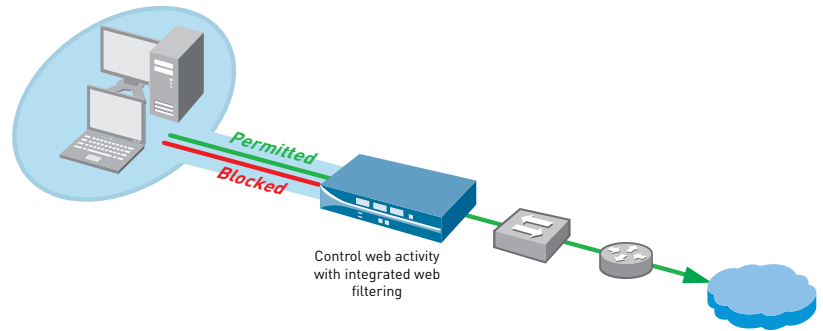


Integrated URL Filtering

An integrated URL filtering database helps control 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.
- Facilitate SSL decryption policies such as “don’t decrypt traffic to financial services sites” but “decrypt traffic to blog sites”.



Today, enterprise users are more Internet-savvy than ever. More and more, they’re spending time on their favorite web site or they’re using the latest and greatest evasive Internet application. The result of users’ unfettered Internet usage exposes enterprises to significant security and business risks including propagation of threats, possible data loss, and lack of regulatory or internal policy compliance. Controlling users’ web activity requires a multi-faceted approach that implements policies for both Internet and application activity.

The Palo Alto Network’s next generation firewalls provide enterprise customers with visibility into the applications traversing the network irrespective of port/protocol, SSL or evasive tactic employed. Acting as the perfect complement to policy-based application control is an on-box URL filtering database that enables IT departments to control access to web sites that are in violation of corporate policies.

Combining application identification and control with comprehensive URL filtering delivers new found powers of control to the IT department. Application visibility means that administrators see the exact application that is traversing the firewall, not just the port or the protocol. Once the application is identified, policy controls can be tied to specific users through the transparent integration with Microsoft’s Active Directory (AD). With a fully integrated URL filtering database, administrators can apply granular web browsing policies, complementing the application visibility and control policies and safeguarding the enterprise from a full spectrum of legal, regulatory, productivity and resource risks.

URL Activity Reporting and Logging

Using a set of pre-defined or fully customizable URL filtering reports, IT departments can generate reports on URL filtering results and related web activity including:

- **Top 50 URL Users:** shows the top users that are hitting URL filtering categories that have been configured to block or alert.
- **Top 50 URL Users Behavior:** shows the top 50 users and category combinations.
- **URL Categories:** displays the number of sessions that accessed web sites in the top 50 URL categories.
- **Web Sites:** shows the number of sessions that accessed the top 50 web sites in URL filter categories that were blocked or generated alerts.
- **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.

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.

Policy-based Control: Applications and URLs

Control of applications is just as important as controlling the URLs that users are allowed to use as many applications are designed to specifically bypass traditional URL filtering solutions. Applications such as Hopster, UltraSurf, Tor, PHPProxy, and many others allow user browsing behavior to go undetected by traditional solutions. Palo Alto Networks identifies all of these applications and more, enabling policies to be set that block them from being used – a critical complimentary component to URL filtering. Using a Palo Alto Networks firewall, enterprise IT departments can implement URL filtering policies 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.
- 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.

Deployment Flexibility

The unlimited user license behind each URL filtering subscription and the high performance of the PA-2000 and PA-4000 Series means that enterprise customers gain an advantage of being able to deploy a single appliance to control web activity for an entire user community without worrying about user-based licensing.

URL FILTERING ORDERING INFORMATION

PA-4060 URL filtering subscription
 PA-4050 URL filtering subscription
 PA-4020 URL filtering subscription
 PA-2050 URL filtering subscription
 PA-2020 URL filtering subscription

YEAR 1 PART NUMBER

PAN-PA-4060-URL2
 PAN-PA-4050-URL2
 PAN-PA-4020-URL2
 PAN-PA-2050-URL2
 PAN-PA-2020-URL2

RENEWAL PART NUMBER

PAN-PA-4050-URL2-R
 PAN-PA-4050-URL2-R
 PAN-PA-4020-URL2-R
 PAN-PA-2050-URL2-R
 PAN-PA-2020-URL2-R



Palo Alto Networks
 232 E. Java Drive
 Sunnyvale, CA. 94089
 Sales 866.207.0077
 www.paloaltonetworks.com

Copyright ©2008, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

840-000005-00A