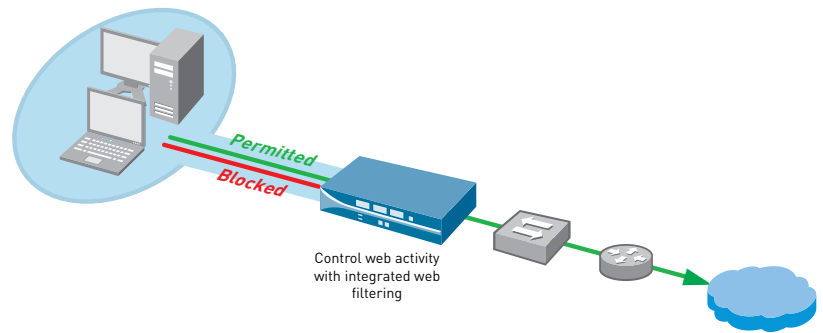


Integrated URL Filtering

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-work related 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 finance sites” but “decrypt traffic to blog and forum sites”.



Integrated into every Palo Alto Networks next-generation firewall is a complete URL filtering database that enables IT departments to monitor and control employee web surfing activities through granular security policies. Combining a comprehensive URL filtering database with granular application visibility and control delivers new found powers of control to the IT department.

The application visibility delivered by App-ID means that administrators are provided with the exact application that is traversing the firewall, irrespective of port, protocol, SSL encryption or evasive tactic employed. Once the application is identified, appropriate policy controls can be implemented.

With a fully integrated URL filtering database, administrators can then apply more 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 filtering visibility and policy controls can be tied to specific users through the transparent integration with Microsoft’s Active Directory (AD) with additional insight provided through customizable reporting and logging.

URL Activity Reporting and Logging

Using a set of pre-defined or fully customizable URL filtering reports, IT departments can generate summaries of 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 User Behavior:** shows the top 50 user 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 logs** can be filtered through an easy-to-use query tool 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. These variables can be used in providing links to trouble-ticketing systems if desired so the user can submit a request for review when they don't agree with the category rating.

Policy-based Control

Policy-based application usage control and URL filtering means that enterprise IT departments can set detailed policies to control a wide-range of non-work related activities and protect the network from a wide range of associated risks. URL filtering policies can be created using a combination of the following mechanisms:

- Select from 54 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, 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 platforms 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

PART NUMBER

Future
 PAN-PA-4050-URL
 PAN-PA-4020-URL

 PAN-PA-2050-URL
 PAN-PA-2020-URL

RENEWAL PART NUMBER

Future
 PAN-PA-4050-URL-R
 PAN-PA-4020-URL-R

 PAN-PA-2050-URL-R
 PAN-PA-2020-URL-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, FlashMatch, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. in the United States. 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.