February 23, 2021

by Hillstone Marketing

The Key Benefits of URL Filtering

What are the key benefits of URL filtering and why do you need it? Many employees rely on the internet for information and services needed to do their respective jobs, but web sites can harbor harmful content or behaviors, like drive-by downloads, phishing and malware. In addition, certain sites focused on activities like gaming, social media and other personal pursuits can impact worker productivity and tie up corporate network resources.

URL filtering can also help reduce resource usage by blocking or limiting the viewing of online videos, for example. In addition, liability can be avoided by blocking access to inappropriate sites (porn, gambling, gaming, etc.) and regulatory compliance can be improved by exempting certain encrypted connections (banking, healthcare, etc.).

In its first generations, URL filtering was simply a tool to keep employees from accessing non-work-related sites. However, URL filtering has evolved to help protect against the rapidly changing threat landscape, and to interwork with other technologies to provide accurate and efficient identification of risky web sites.

But How Does URL Filtering Work?

At its most basic level, URL filtering matches outbound web traffic against a built-in URL database to determine whether to allow or disallow access to web sites based on parameters set by the admin. The database is typically segmented into broad categories, like financial, healthcare, gaming, malicious, etc.

Admins can then choose to allow or disallow traffic destined to given categories via policies. Alternatively, administrators can block individual websites that are known to be questionable in terms of worker productivity or malware. Compliance can be maintained by providing special handling for traffic to financial or healthcare web sites, for example. In addition, DNS filtering is often supported, which allows admins to block entire domains.

In this way, URL filtering reduces risk from a variety of web-borne threats, improves regulatory compliance, and boosts worker productivity.

Taking URL Filtering to the Next Level

Of course, a built-in URL database can't possibly keep up with the rapid creation of web sites, even if the list is updated regularly. According to one source, about 380 new sites per minute are produced globally – or more than 500,000 per day!

In response, some network security vendors, like Hillstone Networks, offer a cloud-based real-time URL categorization database. Hillstone's cloud URL filtering database, for example, includes more than 140 million URLs (and counting) with 64 categories, 8 of which are security related. Hillstone next-gen firewalls and IPS products also allow the admin to set up highly detailed actions, like filtering Java Applets, ActiveX or cookies, or blocking HTTP post actions. Together, these capabilities increase the accuracy and effectiveness of URL filtering.

Machine learning and artificial intelligence add even more sophistication to the process by analyzing and automatically responding to new potential threats. Through these technologies, URL filtering becomes even more proactive and effective in defending the network.

A Comprehensive Approach to Network Security

As important as URL filtering is for network protection, however, it is only one component of a comprehensive security strategy. URL filtering is, in fact, often deployed as a part of another security technology. For example, Hillstone's S-Series Network Intrusion Prevention System (NIPS) appliances include URL filtering, which combines with deep packet inspection, protocol anomaly analysis and signature analysis to block threats.

Next-gen firewalls, like Hillstone A-Series, E-Series, X-Series datacenter NGFW and CloudEdge virtual NGFW, include URL filtering as well and provide even more comprehensive detection and prevention of threats and attacks. NGFWs can provide a broad spectrum of defense mechanisms, up to and including at the application layer, to meet real-world network security needs.

Advanced NGFWs, like the A-Series, include multiple other technologies to detect and protect against attacks and threats. In addition to URL filtering, Hillstone NGFWs incorporate anti-spam, cloud sandboxing, botnet C&C prevention, IPS, IP reputation, anti-virus and many other techniques.

A unified threat detection and analytics engine coordinates across all the security mechanisms, including URL filtering, to increase overall efficiency, reduce network latency, and support a comprehensive security posture. For instance, if botnet C&C prevention detects communications to a command center, or if the cloud sandbox identifies a potential threat, that information can be instantly forwarded to URL filtering and other technologies, which in turn can quickly block access to and communication with the offending URL or IP address.

As mentioned, URL filtering is an important tool in a comprehensive security strategy. If you'd like to learn more, please reach out to us. Our friendly and knowledgeable team is happy to help.

Share this page...

Hillstone on YouTube

Categories

- Event
- Industry News
- Network Security
- Product Release
- Products
- Uncategorized
- Vulnerability Notification

Archives

- March 2021
- February 2021
- January 2021
- December 2020
- November 2020
- October 2020
- September 2020
- August 2020
- July 2020
- June 2020
- May 2020
- March 2020
- February 2020
- January 2020
- December 2019
- October 2019
- September 2019
- August 2019
- July 2019
- June 2019
- May 2019
- April 2019
- March 2019
- January 2019
- December 2018
- November 2018
- October 2018
- September 2018
- August 2018
- July 2018
- June 2018
- May 2018
- April 2018
- March 2018
- February 2018
- January 2018
- October 2017
- June 2017

0 SHARES