AccessEnforcer®

HTTPS Web Filter Overview

calyptix®
SECURITY

Introduction

A web filter is essential to protecting small businesses and their employees from malicious websites and distracting web content. To stay safe, productive, and compliant online, every organization needs to block certain websites.

This critical task has become more difficult in recent years. Websites have moved to the encrypted HTTPS standard by the thousands. This is great news for security on the web, but it also complicates the task of filtering web content.

The HTTPS standard encrypts data transmitted between a host and server. This renders the data almost useless to attackers. It also prevents eavesdropping and man-in-the-middle attacks – and makes it difficult for web filters to inspect the traffic.

Dozens of security products offer HTTPS web filtering (also known as HTTPS interception, SSL inspection, TLS filtering, and many other names). Unfortunately, this feature is poorly designed in many products and often harms users' security (more about this inside).

In this report:

- 4 Reasons You Need an HTTPS Filter
- Why Many HTTPS Filters are Bad
- AccessEnforcer HTTPS Web Filter Overview

4 Reasons You Need an HTTPS Web Filter

#1. Increase staff productivity

Years ago, HTTPS was mostly used for online transactions, online banking, and other sensitive sessions. However, thousands of websites that do not handle sensitive data have adopted HTTPS. Many of them are often viewed as time wasters in the small business community.

Facebook, Twitter, YouTube, and hundreds of other sites that many businesses would prefer to block use HTTPS by default. For a small business, the most practical way to prevent some or all employees from wasting time on these sites is to use a reliable HTTPS web filter.

#2. Block malicious sites

Millions of websites are dangerous. Through drive-by-downloads, session hijacking, spoofing, and other tactics, they can inject malware onto the user's system or trick users into supplying sensitive information.

These techniques work on HTTP sites, and they work on HTTPS sites as well. An HTTPS filter helps protect businesses from these hazards.

#3. Block offensive web content

Websites with offensive or inappropriate content abound on the web. Nothing prevents them from using HTTPS. The only way an organization can remain free of this disruptive material is to use a web filter that can manage both HTTP and HTTPS sites.

#4. Comply with regulations

Education, healthcare, and retail are three industries among many that are required to have enhanced network security. Some standards, such as the Children's Internet Protection Act (CIPA), require organizations to filter web content. Any industry that requires HTTP filtering is all but certain to require HTTPS filtering as well.

Many HTTPS Filters are Bad for Security

Not all web filters are equal. The way they handle traffic and enforce policies can have a significant impact on performance – and security.

In March 2017, an alert from U.S. CERT (under the Department of Homeland Security) warned U.S. businesses about HTTPS inspection products that harm security.[1] The alert followed the release of a major study that found nearly all such products severely undermined connection security.

In The Security Impact of HTTPS Interception, researchers from Mozilla, Google, and other tech organizations studied two product categories: client-side antivirus and "middleboxes" (such as UTM firewalls). Their analysis was thorough and their findings were clear.

"As a class, interception products drastically reduce connection security....many introduce severe vulnerabilities," according to the report (underlining added).[2]

[1] US CERT: HTTPS Interception Weakens TLS Security: https://www.us-cert.gov/ncas/alerts/TA17-075A

[2] The Security Impact of HTTPS Interception (pg. 13; pg. 1): https://jhalderm.com/pub/papers/interception-ndss17.pdf

What’s Wrong with HTTPS Inspection?

Most products that filter HTTPS traffic act as a proxy. When users visit HTTPS websites, the product terminates the browser’s TLS session, inspects the web content, and creates a new TLS connection. The new connection is created by sending a Client Hello message to the destination server.

This hello message shows the TLS version and features supported by the security product’s TLS client. This includes ordered lists of cipher suites, compression methods, and extensions – all of which can contain additional parameters such as elliptic curves and signature algorithms.

Here’s the problem: nearly all of the security products included weak or deeply flawed TLS options in the Client Hello message.

The options were almost always worse than those allowed by the user’s web browser – meaning the user’s connection would have been more secure without the product’s help. Researchers also found widespread support for broken ciphers and a failure to verify the certificates of destination servers.[3]

“The default settings for eleven of the twelve corporate middleboxes we evaluated expose connections to known attacks, and five introduce severe vulnerabilities,” according to the report. “Similarly, 18 of the 20 client-side security products we tested reduce connection security, and half introduce severe vulnerabilities.” [4]

[3] The Security Impact of HTTPS Interception (pg. 1): https://jhalderm.com/pub/papers/interception-ndss17.pdf

[4] The Security Impact of HTTPS Interception (pg. 1-2): https://jhalderm.com/pub/papers/interception-ndss17.pdf

AccessEnforcer HTTPS Web Filter is Different

Most security products filter HTTPS traffic using the method described above – i.e. they break the encryption, inspect the traffic, and create another TLS connection with the destination server to forward the traffic.

The HTTPS Web Filter in AccessEnforcer UTM Firewall does not break the encryption. Instead, it uses a proprietary method of analyzing web server certificate fields to determine if a connection is allowed. The browser's encryption is not affected, and the firewall is also not bogged down with a resource intensive process.

The result is a web filter that doesn't bog down your network or harm your security.

Settings for the HTTPS Filter

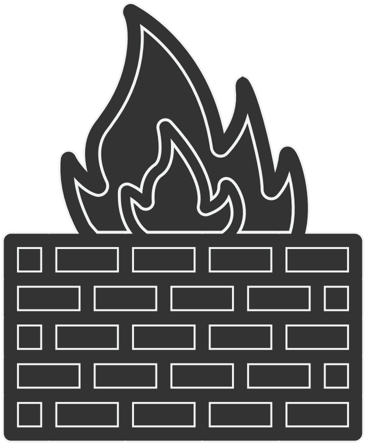
AccessEnforcer filters HTTPS sites in a single click. Assuming the organization has filtering policies for HTTP traffic, a click on a single checkbox automatically applies the same policies to HTTPS traffic. When the HTTPS filter is active, the following policies will apply to HTTPS traffic:

- URL whitelist
- URL blacklist
- Web filter exemptions

The HTTPS filter has three options for how it enforces policies:

- Disabled – the HTTPS filter is off.
- Monitor – the filter will log HTTPS traffic, but it will not enforce policies.
- Enforce – the filter will log and enforce policies on HTTPS traffic.

For protocols, AccessEnforcer monitors HTTPS requests that use TLS 1.0 and later on port 443.



Compared to Other Firewalls

Some firewall vendors can block HTTPS sites, but none can match the benefits of the web filter in AccessEnforcer UTM Firewall:

- **Faster Activation -** some filters require complicated and time-consuming configurations to enable HTTPS filtering. AccessEnforcer does it in one click.
- **Faster Connection Speeds -** many web filters decrypt HTTPS traffic to inspect it before filtering. This demands a tremendous amount of resources from the device and can slow connection speeds. AccessEnforcer filters HTTPS traffic without decryption, so the network stays fast.
- **Stronger Chain of Security -** security products that break the chain of encryption almost always create a less-secure connection with the destination sever once content inspection is complete.

This can invite severe vulnerabilities into the connection and enable a man-in-the-middle attack.

AccessEnforcer filters HTTPS traffic without breaking the chain of encryption – giving you a safer connection online.

HTTPS Web Filter Comes Standard

The HTTPS Filter is included as part of standard service with AccessEnforcer. In fact, standard service includes every feature we offer.

Additional standard features include:

- Intrusion detection and prevention (IDS/IPS)
- Quality of service (QoS)
- Web filtering
- Email filtering
- Automatic firmware updates
- Automatic security updates
- Unlimited network users
- Unlimited virtual private networks (VPNs)
- GUI-based management

Protect your business with simple, powerful security with AccessEnforcer UTM Firewall.

Request Pricing & Learn More

704.900.0422

sales@calyptix.com

calyptix® SECURITY