HTTPS Content Inspection: 7 Things Your Firewall Absolutely MUST Do

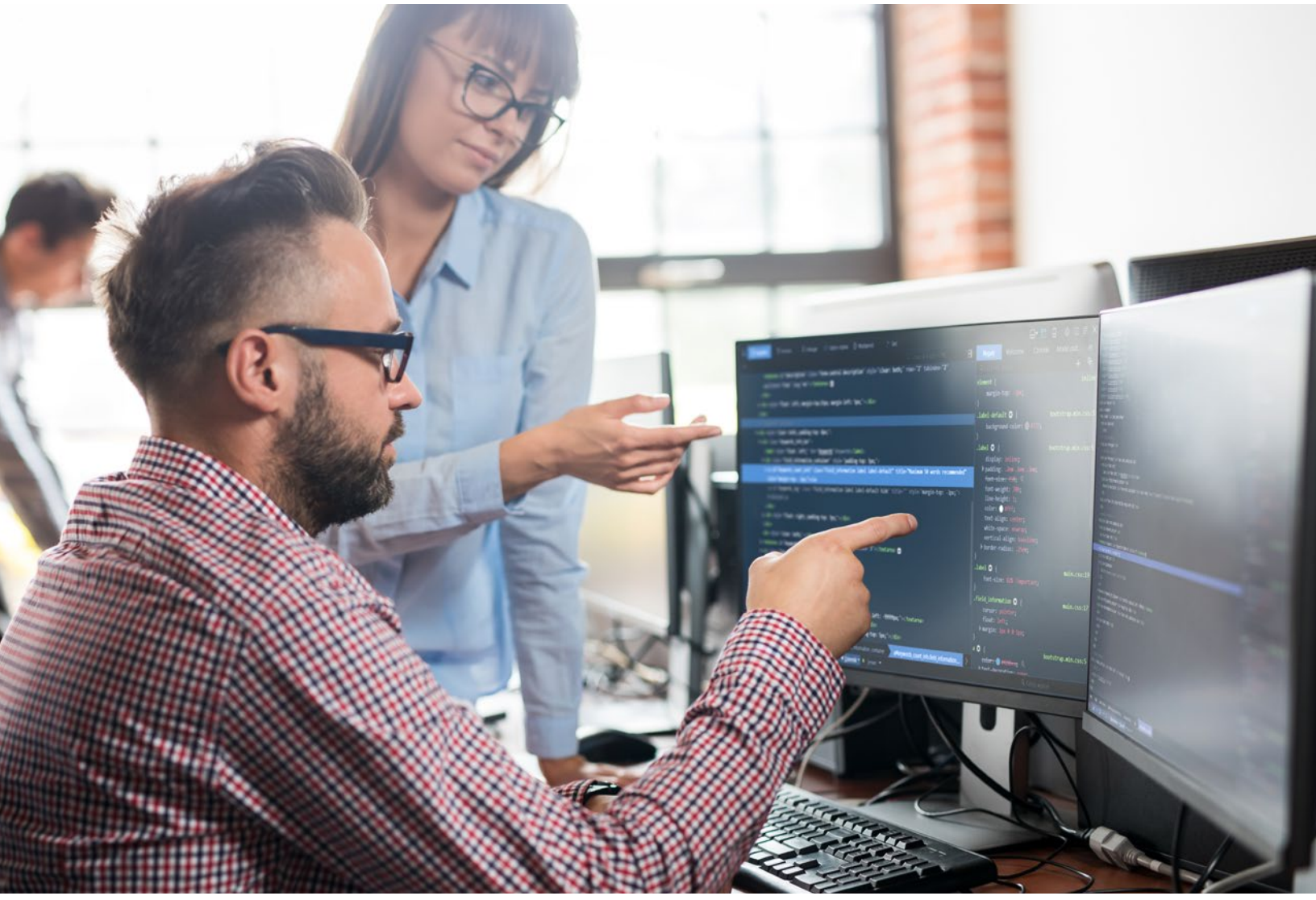


Table of Contents

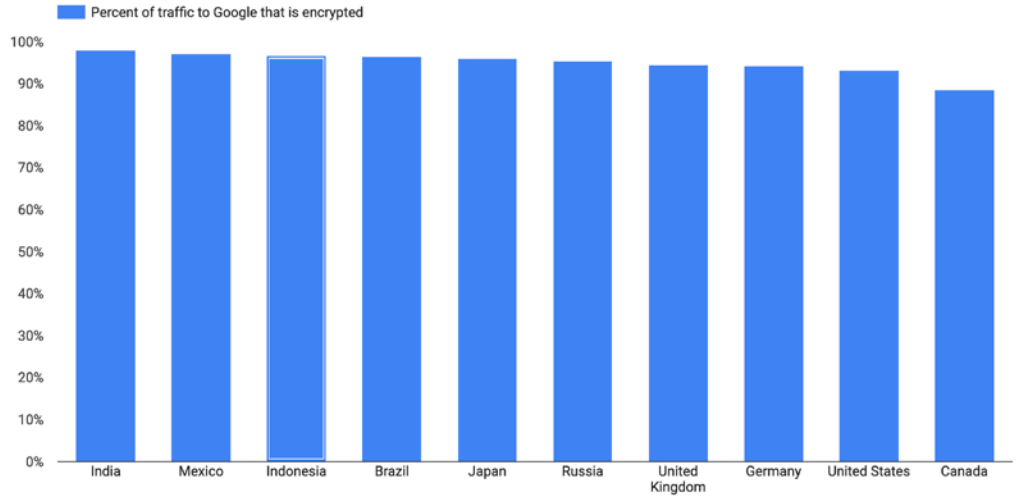
INTRODUCTION

Web traffic has changed dramatically over the last decade. Years ago, visiting a site normally meant accessing the content over HTTP. The problem is that in HTTP, the data is not encrypted and can be easily intercepted by attackers as it is passed between systems. To keep this data private, the majority of websites today require access by HTTPS, which encrypts communications between systems using SSL/TLS (Secure Socket Layer/Transport Layer Security). **Without HTTPS, any data passed between systems is susceptible to compromise and theft.**

Though HTTPS is intended to secure your communications, attackers increasingly use HTTPS to hide malware, command and control (C&C) channels, and nefarious activity. **Attackers know that legacy firewalls, like those commonly seen in the midsize enterprise, are rarely able to inspect this encrypted traffic.** Ransomware strains like Cryptowall and Locky demonstrated the scope of damage possible when threats are allowed to lurk in the shadows of encrypted network traffic, and botnets heavily rely on HTTPS to disguise their communications. For this reason, HTTPS inspection is vital for ensuring security in the modern workplace.

HTTPS Traffic by the Numbers

Once only accounting for a small percentage of traffic, today HTTPS pervades the Internet. As part of their "HTTPS encryption on the web" transparency report, Google found that half of the pages an average user accesses are over HTTPS, and 95% of a user's time is spent on HTTPS pages. For the average user, the use of HTTPS and the appearance of an icon indicating a secure connection in the corner of the browser instills a sense that you are transacting with a trustworthy party. This fact is not lost on hackers, however, as research shows that nearly half of the phishing sites discovered in 2018 used HTTPS to appear legitimate and encrypt their deeds. Let's Encrypt, which provides free SSL/TLS certificates to anyone who wants to use HTTPS on their own site, has lowered the barrier for attackers who formerly would have had to purchase a certificate. As a result, without the ability to inspect this traffic, many businesses have fallen victim to malware and other attacks as the result of risky clicks made on pages their users thought were safe.



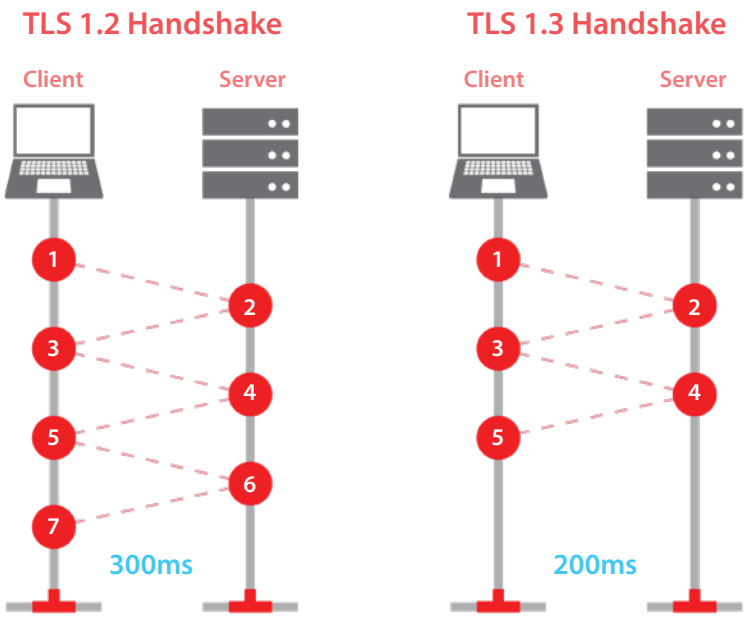
Hiding in Plain Sight: Encrypted Traffic Obscures Serious Threats

Today, **67% of all malware uses encrypted communication channels to disguise their attack.** More alarmingly, **72% of malware hidden is zero day**, meaning it has never been seen in the wild before.[2] This suggests that not only do threat actors hide their attacks using encryption, but they tend to use more sophisticated malware through these encrypted channels. Removing malware before it enters the network is one part of a layered defense strategy. In this whitepaper, we will look at seven essential features of a firewall solution for inspecting and securing encrypted traffic.

1. Inspect TLS 1.3

The latest version of the TLS protocol, TLS 1.3, improves on the privacy and performance of HTTPS communications but complicates the process of HTTPS inspection for many firewall vendors. From a security perspective, TLS 1.3 removes support for outdated protocols and ciphers, much of which had remained in previous versions for compatibility purposes. These were heavily exploited by Logjam, FREAK, Lucky13, BEAST, and POODLE, which necessitated their removal. TLS 1.3 also removes support for the commonly used RSA key exchange and other non-Perfect Forward Secrecy (PFS) cipher suites, which are known to be inadequate for security today.

TLS 1.3 adoption has grown since initial release in August of 2018, and we expect this to accelerate in the short term. Simply put, **if your firewall can't inspect TLS 1.3, you will be left with a blind spot growing ever larger.** Thankfully, TLS 1.3 content inspection is fully supported in the latest version of the WatchGuard Fireware OS.



1. https://transparencyreport.google.com/https?hl=en
2. WatchGuard Internet Security Report - Q1 - 2020

2. Inspect by Category

Not all web traffic is created equal, and let's face it, some areas of the Internet are riskier than others. Look for a solution that allows you to easily determine which traffic to inspect, based on the category of the domain. This way you can avoid inspecting traffic generated as an employee checks their bank balance and be confident that any traffic to NSFW (not suitable for work) pages is well inspected. Categories should be predefined, but the solution should also provide the flexibility to choose what to do when uncategorized domains are encountered.

3. Accelerate Inspection

Delivering high performance and throughput for HTTPS inspection on a multi-function security appliance is a challenge. Many vendors will publish impressive inspection throughput figures, but these are for basic inspection only. The type and number of security applications active on the firewall can dramatically reduce the throughput of the device. Third-party competitive tests have shown activating HTTPS inspection on some firewall platforms results in performance degradation of over 90% in some cases.

4. Provide Predefined and Curated Exception Lists

Creating and managing exceptions lists to dictate which domains can be inspected can be a time-consuming and tedious process. Failure to do so, however, could leave your company vulnerable and your traffic bogged down. Look for solutions that provide a predefined and well-curated list of exceptions as a foundation. This list should include domains for services such as Dropbox, Skype, Microsoft Office, Okta, and many other applications and services you use. It should also be regularly updated to stay ahead of the latest threats.

5. Import Certificates Signed by a Microsoft CA Server

To examine HTTPS traffic requested by a user on your network, you must configure your Firebox to decrypt the information and then encrypt it with a certificate signed by a CA that each network client trusts. If your organization already has a PKI (Public Key Infrastructure) set up with a trusted CA, you should be able to import a certificate that is signed by your organization's internal CA to your firewall. This avoids having to import each previous certificate and allows you to quickly bring the firewall into the chain of trust.

6. Reject Out-dated and Insecure Protocols

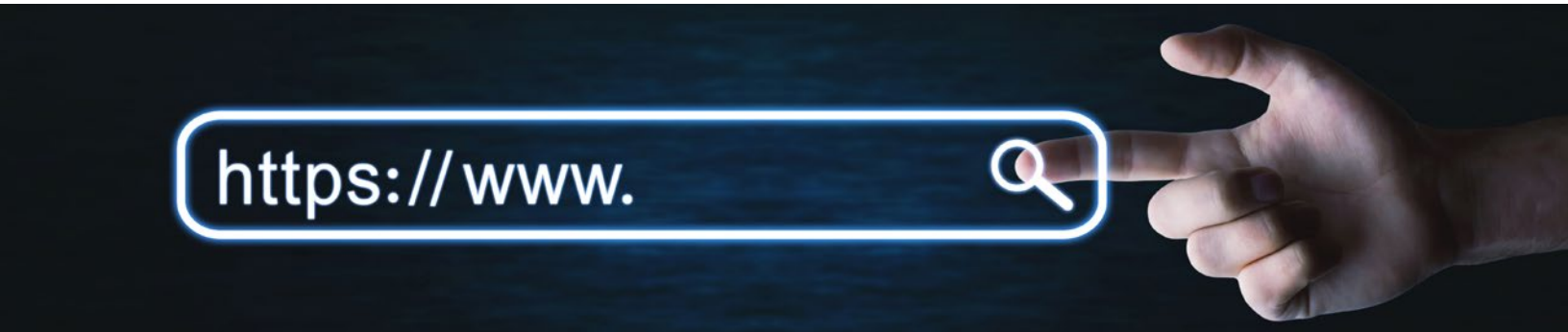
By default, HTTPS content inspection should not support weaker, broken protocols like SSLv2 and SSLv3. Unfortunately, many HTTPS content inspection platforms still use these protocols, leaving organizations under threat by well-known and easily exploited vulnerabilities. When a client requests a connection based on an outdated protocol, it should be immediately denied, and no further negotiation to a different protocol should be possible.

It should also be possible to determine if a certificate is expired or is not signed by a trusted certification authority using the Online Certificate Status Protocol (OCSP) to validate the original server certificate.

7. SSL/TLS Offloading

To reduce the burden on your internal clients, there may be instances where you want to avoid encrypting the content as it proceeds into your network. SSL/TLS offloading allows the firewall to perform content inspection and pass on the inspected traffic to the intended destination without unnecessary steps. This reduces the CPU load on the firewall and removes the burden of TLS/SSL encryption and decryption from your internal web server.

Although this approach will be appropriate for certain use cases and organizations, it does introduce a security risk, as now those inside your organization could see your unencrypted traffic.



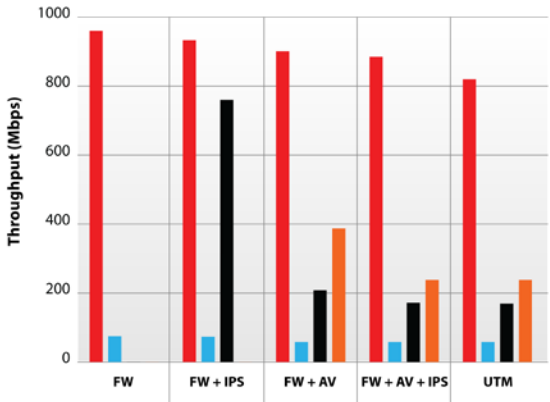
HTTPS Content Inspection with WatchGuard Firebox

At WatchGuard, we don't view HTTPS content inspection as a "nice to have" feature – it's a security essential. That's why HTTPS Content Inspection is a standard feature in every WatchGuard Firebox. WatchGuard Firebox uses in-line proxies to decrypt TLS traffic to preform what is effectively man-in-the-middle-style (MitM) inspection of SSL/TLS sessions. With Deep Packet Inspection (DPI), the entire stack of WatchGuard anti-malware, content filtering, botnet detection, and intrusion prevention services (IPS) can be brought to bear on attacks attempting to hide in encrypted channels.

Built on AES-NI-capable Intel chipsets, WatchGuard Firebox M Series appliances offload some cryptographic function to the hardware for accelerated encryption and decryption. This architecture enables WatchGuard to deliver best-in-class performance for HTTPS inspection and is the reason why the Firebox consistently outperforms competitors in third-party performance testing.

Unified Threat Management Throughput (Mpbs)

Security Features Enabled with Stateful HTTPS Traffic

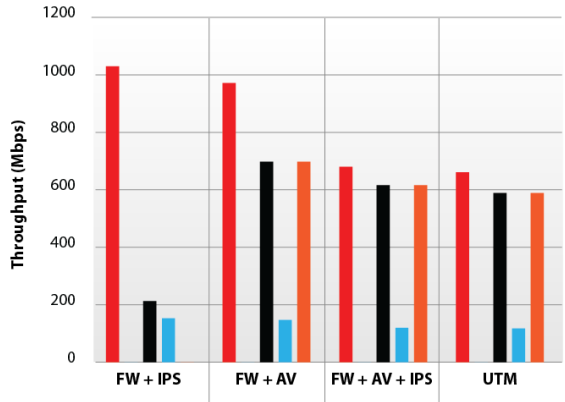


	FW	FW + IPS	FW + AV	FW + AV + IPS	UTM
WatchGuard Firebox M370	960	933	901	885	820
SonicWALL NSA 2600	75	73	58	58	58
Fortinet FortiGate 100E	N/A	760	208	172	169
Sophos XG 210	N/A	N/A	387	238	238

Source: Miercom July 2017

WatchGuard Firebox M270 Unified Threat Management

Competitive Security Features HTTPS Throughput (Mbps)



	FW + IPS	FW + AV	FW + AV + IPS	UTM
WatchGuard Firebox M270	1030	972	680	661
SonicWALL NSA 2600	153	147	120	118
Fortinet FortiGate 100E	213	698	616	589
Sophos XG 210	N/A	698	616	589
Cisco Meraki MX84	N/A	N/A	N/A	N/A

Source: Miercom August 2018

To inspect encrypted HTTPS traffic, administrators make our Firebox part of a client's (Windows, Android, and macOS) trust chain by adding a digital certificate that makes their Firebox a Trusted Root Certificate Authority (CA). This allows the Firebox to inspect all the client's encrypted traffic, without breaking HTTPS security or the expected user experience.

The Firebox also can use the Online Certificate Status Protocol (OCSP) to validate the original server certificate. If a certificate is expired or is not signed by a well-known certification authority that the Firebox trusts, it marks it as invalid before providing it to the browser.

ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by over 18,000 security resellers and service providers to protect 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com