SOPHOS
Cybersecurity evolved.

Has encryption made your current firewall irrelevant?

Five TLS inspection capabilities you need in your next firewall

A Sophos Whitepaper. June 2021

Five TLS inspection capabilities you need in your next firewall

The rapid increase in encrypted network traffic, coupled with the inability of most next-gen firewalls to inspect this traffic, has created a perfect security storm – one with dire consequences.

Over 90% of traffic on most networks is encrypted and it passes through the average firewall completely unfiltered. This is not due to a lack of desire to inspect it. Rather, it's because most firewalls simply aren't up to the task. And even if the firewall can inspect encrypted traffic, all too often their TLS inspection solution is poorly implemented, breaking many websites and delivering a poor user experience.

Unsurprisingly, hackers are catching on to this enormous blind spot in organizational security. They are starting to take advantage of this weakness to get threats onto networks and keep them there.

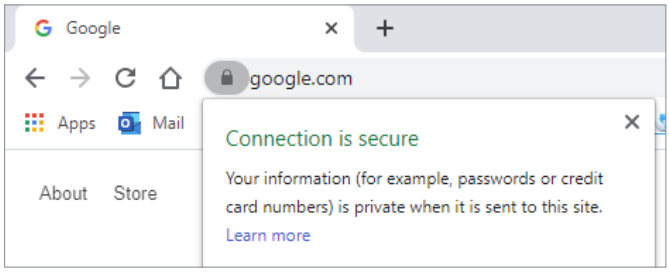
Read this paper to learn about how encryption has made most next-gen firewalls irrelevant, the challenges with TSL inspection, and the five SSL inspection capabilities you need to close this security gap.

Encryption provides privacy not security

People often believe that encrypted internet connections are "secure." But "secure" from what, exactly?

Transport Layer Security, or TLS, is the encryption standard used on the internet today. The terms SSL and TLS are often used interchangeably. In fact, SSL is an old standard that has been since eclipsed by TLS. However, SSL remains the more common term. Just know that most people mean TLS when they say SSL.

TLS is designed to provide confidentiality and authenticity by encrypting the communication between two parties and verifying that the server is who it claims to be, based on its certificate and who issued it.



The lock symbol in your browser indicates the connection is encrypted – for privacy.

What TLS encryption does NOT do is secure, or provide assurance of, the content of the web page. A site hosting malware payloads can have a perfectly valid encrypted and 'secure' connection.

When someone claims their connection to a web server is secure, they really just mean it's secure from eavesdropping (although even that may not be the case). This is why it's is so important to inspect encrypted traffic

TLS inspection is not easy

The challenge with TLS inspection is that TLS is a very complex protocol. Different certificates must be exchanged and the cipher suites to be used need to be negotiated in order to determine how the connection should be encrypted. Compounding matters further, there are several TLS versions, and many applications and web services do things differently.

As a result, it's very possible, despite having rigorous standards, for things to be incompatible. This presents enormous challenges for any security solution that attempts to inject itself into the process in order to inspect and secure the content that is exchanged.

The importance of TLS 1.3 and dispelling some myths

The good news is that the latest TLS standard, TLS 1.3, offers a number of advantages over its predecessors in the area of performance, privacy, and addressing vulnerabilities.

TLS 1.3 adoption on servers is still in the early days, but all major browsers now support this standard. However, due to the complexities and R&D effort required to implement it, many firewalls with TLS inspection on the market today don't fully support 1.3. Instead they force a downgrade to TLS 1.2. This opens those connections up for exploitation and attack due to legacy vulnerabilities.

As with many new technologies, there are a number of myths or common misunderstandings around inspecting TLS 1.3. These include claims that flat-out declare that TLS 1.3 cannot be inspected. This is false. While it's true that passive TLS inspection, which was done on the side-lines, is no longer possible, with the participation of a cooperating endpoint – as you have on a corporate network – inspection is still entirely possible.

Another claim is that by inspecting encrypted traffic flows, you're somehow making them less secure. This is true if you downgrade a TLS 1.3 connection to TLS 1.2, as many TLS inspection solutions do today. The vulnerabilities in TLS 1.2 opens the door to possible exploitation by a malicious man-in-the-middle (MITM) attack. TLS 1.3 has been designed to address these vulnerabilities so inspecting this traffic without downgrading the connection does not introduce risk.

And lastly, some will claim that certificate pinning makes TLS inspection impossible. While this is true for some applications with hard-coded certificates, most applications use a certificate pinning approach that respects the resigning certificate and will continue to work with SSL inspection solutions.

The importance of certificate validation

Certificate validation Is a fundamental component of TLS as it enables the client (or inspection device like your firewall) to prove the identity of the server that the communication is coming from.

However for certificate validation to work it needs to be implemented properly. If not, firewalls, and the endpoints they are connected to, can be fooled into thinking they are talking to a server they are not, opening the door for a malicious MITM attack.

Balancing performance, privacy, and protection

In addition to all the technical complexities with TLS encrypted traffic flows, there are policy and regulatory constraints that need to be considered and respected as well. Plus trusted corporate application traffic and streaming media can make up a good portion of TLS encrypted traffic that may not require inspection.

The bottom line is that not all encrypted traffic can or should be treated the same. It's a balancing act: you have to balance privacy, security, compliance, and performance. Some jurisdictions may dictate the balance, while in others, you're left to your own devices to come up with a suitable balance for your organization.

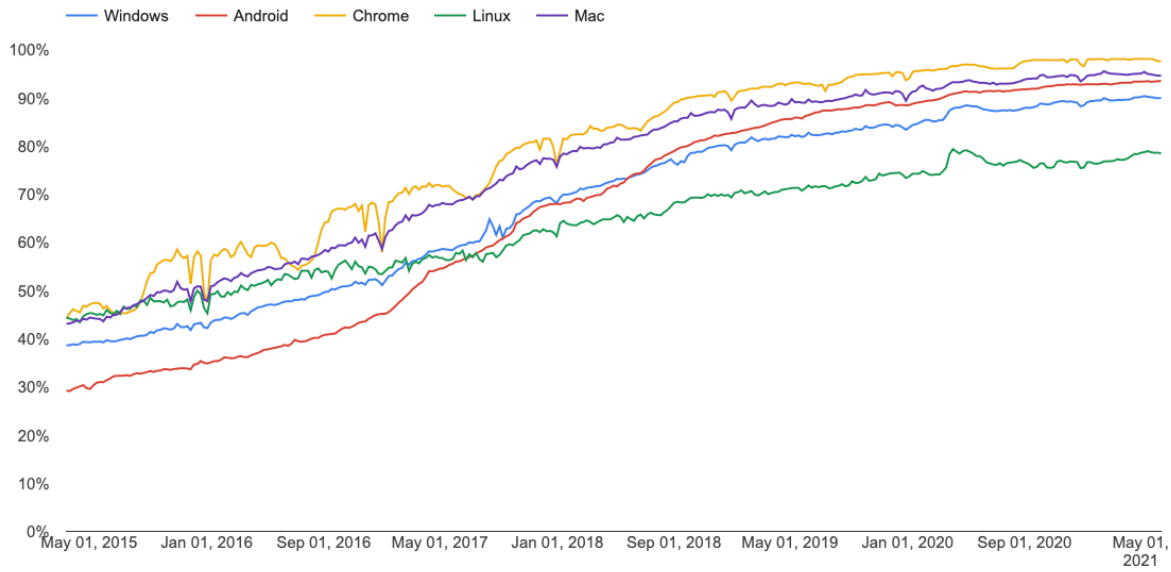
Unfortunately, the limitations in TLS inspection solutions in most firewalls on the market today force organizations to adopt a very unbalanced approach: security and compliance needs are sacrificed in the struggle to provide essential performance and interoperability.

Encrypted traffic volume is approaching 100%

Most internet connections are now fully encrypted. In fact, on most platforms, over 90% of web sessions are now encrypted according to the Google Transparency Report, a dramatic increase from about 60% just two years ago.

Google Transparency Report

Percentage of pages loaded over HTTPS in Chrome by platform



The volume of encrypted traffic is up dramatically in the last two years and trending towards 100%.

Has encryption rendered your firewall irrelevant?

This dramatic growth in encrypted traffic has created an enormous security blind spot for most organizations. Their current firewalls are simply not up to the task of inspecting this volume of encrypted sessions. In effect, TLS encryption has made most firewalls irrelevant as they no longer have insight into the majority of traffic passing through the network.

The real danger is the threats hiding in encrypted traffic

With the explosive growth in TLS encryption in recent years, it's probably no surprise that hackers and attackers are catching onto this trend and leveraging it to help get malware on your network undetected – and keep it there.

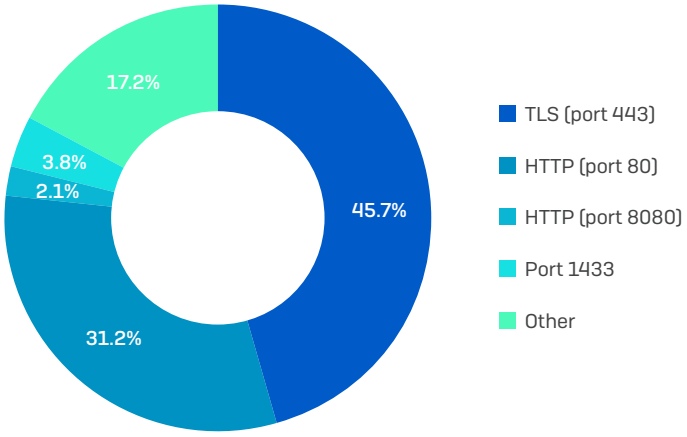
In particular, we've seen an increase in the use of TLS in ransomware attacks over the past year, especially in manually-deployed ransomware—in part because of attackers' use of modular tools that leverage encryption. But the majority of malicious TLS traffic is from initial-compromise malware: loaders, droppers and document-based installers reaching back to secured web pages to retrieve their installation packages.

Nearly all threats are now entering the network over encrypted connections.

Once a threat gets on the network, it will use every trick in the book to remain undetected. Using TLS allows commands sent to the client from control servers to remain undetected while also hiding the information collected from the network as well as any further payloads downloaded to the compromised host.

Not surprisingly, there has been a dramatic growth over the past year in malware using TLS to conceal its communications. In 2020, 23 percent of malware we detected communicating with a remote system over the Internet were using TLS; today, it is nearly 46 percent.

Malware C2 communications, TLS vs. other, Q1 2021

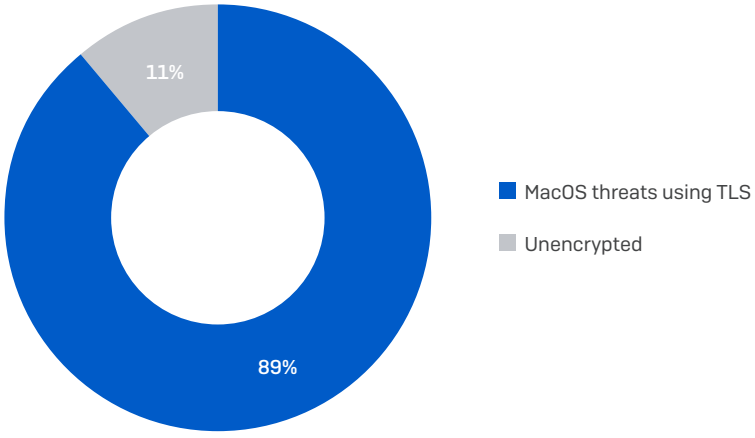


A breakdown of malware outbound communications

There's also a significant fraction of TLS communications that use an Internet Protocol port other than 443—such as malware using a Tor or SOCKS proxy over a non-standard port number.

Hackers are also starting to host malicious content on legitimate sharing services like Discord, Github, and Google Cloud that utilize TLS encryption to ensure the privacy of the content. This provides perfect obfuscation for malware, enabling threats to get into most networks undetected.

It's not just threats that are utilizing encryption to remain undetected; potentially unwanted applications like spyware, adware, and browser toolbars, as well as peer-to-peer file sharing clients and proxy avoidance tools also use encryption to evade firewall detection. This is particularly true on the macOS platform where over 89 percent of macOS threats with C2 communications used TLS to call home or retrieve additional harmful code.



Most Organizations Are Powerless to Act

As we've seen, TLS inspection is complex and resource intensive and with over 90% of network traffic now encrypted, few firewalls are up to the task of inspecting it.

The reality is that most firewalls today lack proper TLS inspection capabilities. They are unable to intelligently determine what should and shouldn't be inspected, and can't possibly handle the enormous load of decrypting everything. In addition, their packet processing and deep-packet-inspection (DPI) engines are not architected to handle TLS inspection efficiently. Furthermore, poor inspection implementations that don't support the latest standards result in downgraded security, which in turn opens organizations up to vulnerabilities while also creating a very poor user conditions.

The rapid increase in encrypted network traffic coupled with the inability of most next-gen firewalls to inspect this traffic has created a perfect storm in network security.

Five Things to Look for in Your Next Firewall

To minimize the risk from encrypted network traffic, ensure that your next firewall includes these top five TLS Inspection capabilities:

1. A modern high-performance streaming inspection engine that supports the latest standards such as TLS 1.3 and works effectively across all ports/protocols to identify risky traffic and threats.
2. Intelligent pre-packaged exclusion lists that are dynamically updated to avoid breaking the internet for sites and services that don't support or don't require decryption.
3. Dashboard visibility of your encrypted traffic flows and possible issues from non-compatible sites and services allowing you to add on-the-fly exceptions before they become a problem.
4. Robust certificate validation able to handle invalid, self-signed, revoked, or untrusted certificates to avoid potential malicious Man-in-the-Middle (MITM) attacks.
5. Policy tools that allow you to address user privacy, organizational security, and network performance to strike the perfect balance for your needs.

Sophos Firewall – Designed for the Modern Encrypted Internet

Sophos Firewall's all-new Xstream architecture and XGS Series appliances offer the best TLS inspection solution available in a Firewall - enabling you to eliminate your TLS encryption blind-spot without impacting performance. You get:

- High performance – a redesigned lightweight streaming engine with high connection capacity
- Unmatched dashboard visibility into your encrypted traffic flows and any errors with the option to add exclusions with just two clicks
- Top security, supporting TLS 1.3 and all modern cipher suites with robust certificate validation
- Inspection of all traffic, being application and port agnostic
- An extensive built-in exclusion list to ensure optimal performance and a great user experience with extensive interoperability to avoid breaking the internet
- Powerful policy tools, offering the perfect balance of performance, privacy, and protection

To learn more, read the XG Firewall Solution Brief or start an instant online demo at www.sophos.com/firewall.

Try it now for free

Try Sophos Firewall online for free
sophos.com/demo

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

21-06-17 EN (DD)

SOPHOS