



TLS Versions: North-South and East-West Web Traffic Analysis

What We Found After Studying 275 Billion
HTTP and HTTPS Live Network Flows

FEBRUARY 2020



Introduction

It's a simple question without an easy answer: What encryption technologies are organizations seeing in their networks, both in north-south and east-west traffic? While a simple web search found multiple surveys and reports that describe versions of SSL/TLS used in the public internet, many of these findings conflate HTTPS with TLS traffic.. We were unable, however, to find any hard data to answer our question about internal enterprise traffic. So, we set out to find the answer. The results are detailed below in this research report.

Why is this important? The wide adoption of SSL/TLS — not only for public internet traffic, but for internal east-west traffic as well — underscores the criticality for inspecting encrypted traffic. East-west traffic visibility is needed for multiple reasons: Detection of laterally moving threats (threat actors are adopting the use of encryption in their attacks); compliance with governance standards that mandate data protection; accurate performance measurements; and finally, faster troubleshooting. All of these require inspection of encrypted traffic.

STEVE PORCELLO

As a former incident responder, Steve uses his experiences to educate organizations on Gigamon's network-based detection and response solution, ThreatINSIGHT.

BASSAM KHAN

Bassam leads product, solutions and technical marketing teams to ensure customer challenges are addressed in Gigamon strategy, products and communications.

Research Methodology

We based our research on 275 billion flows from several dozen enterprises across various industries to ensure a representative sample size. The data was averaged for a four-month collection period to produce high reliability in the results.

For the purposes of this report, several definitions and assumptions were applied regarding the measurement of encrypted versus non-encrypted network traffic. Those were kept consistent for all measurements included in the data set.

Note: We plan to repeat this research in the future to determine changes in data and trends.

TRAFFIC FLOW

We measured network traffic by adding the packet flow, which is a sequence of traffic from a source to a destination, which may be a host or a multicast/broadcast domain. Conceptually, a flow is analogous to a phone call session; however, there are often multiple flows over the lifetime of a session.

DATA COLLECTION

Data collection for this research was performed with the capture and analysis of network packets flowing in and out (north-south traffic) and across (east-west traffic) each organization. Only TCP traffic over the HTTP and HTTPS protocols was analyzed.

Gigamon ThreatINSIGHT's visibility into enterprise traffic enabled us to gather this data. ThreatINSIGHT is a network-based detection and response solution whose sensors are typically deployed at both the organization's edge network, to track north-south traffic, and its core network, to track east-west activities. This deployment model provides threat investigators with a 360-degree view of malware activities by correlating how it entered the organization and how it traversed internally. For the purposes of this research, the deployment model resulted in an accurate representation of all web-based (HTTP/HTTPS) encrypted and non-encrypted traffic. Non-web traffic, such as SMTP and FTPS, was filtered out.

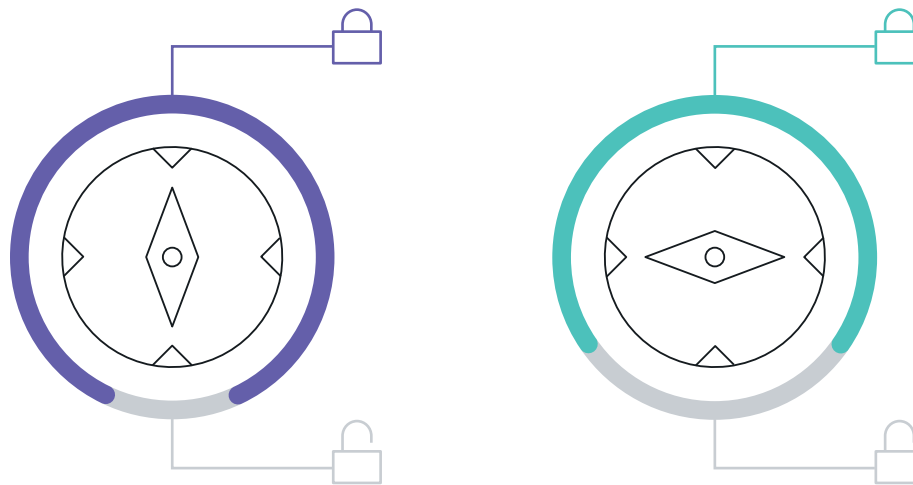
Research Methodology

DATA DESCRIPTION

The following is a breakdown the type of data we worked with:

Total volume: 274,743,312,991 flows

- 106,061,628,564 north-south flows
- 168,681,684,427 east-west flows



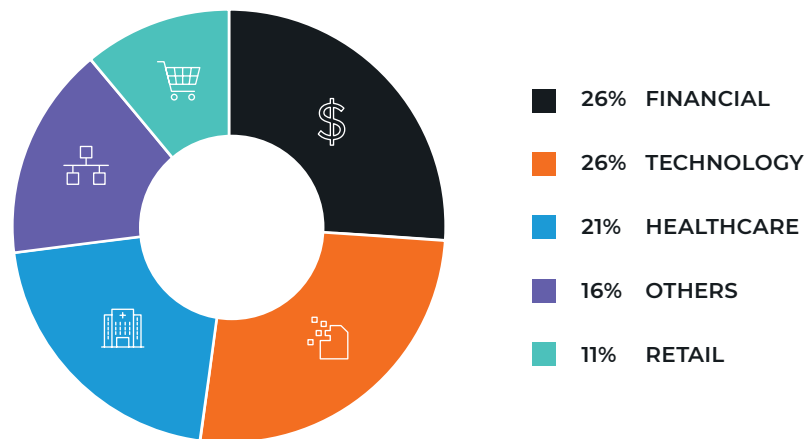
Period of collection:

- Weeks 22–42 of 2019, primarily during the months of June, July, August and September. By averaging over this long time period, we factored out spikes and fluctuations in the data.
- For this time range, the flow was aggregated on an hourly basis per organization. For flows spanning multiple hours, we measured the end timestamp of the flow.

Research Methodology

Organization profile:

- About 50 percent of the organizations are in the Fortune 1000
- On the whole, these organizations have mature security teams and practices, as indicated by their deployment of advanced tools for threat detection, investigation and response based on network metadata
- While the organizations span a wide range of industries, the representative data weighed heavily toward financial institutions, technology and healthcare



DATA OBFUSCATION

Customer data privacy is of the utmost importance to Gigamon, so we analyzed only network metadata (versus actual data) for this report. While we found several areas of this report that could have benefited from additional customer details, we chose to err on the side of caution in regard to privacy and chose not include them in this report.

Even with the obfuscation, the findings are highly valuable in guiding the industry on how to better protect their organizations.

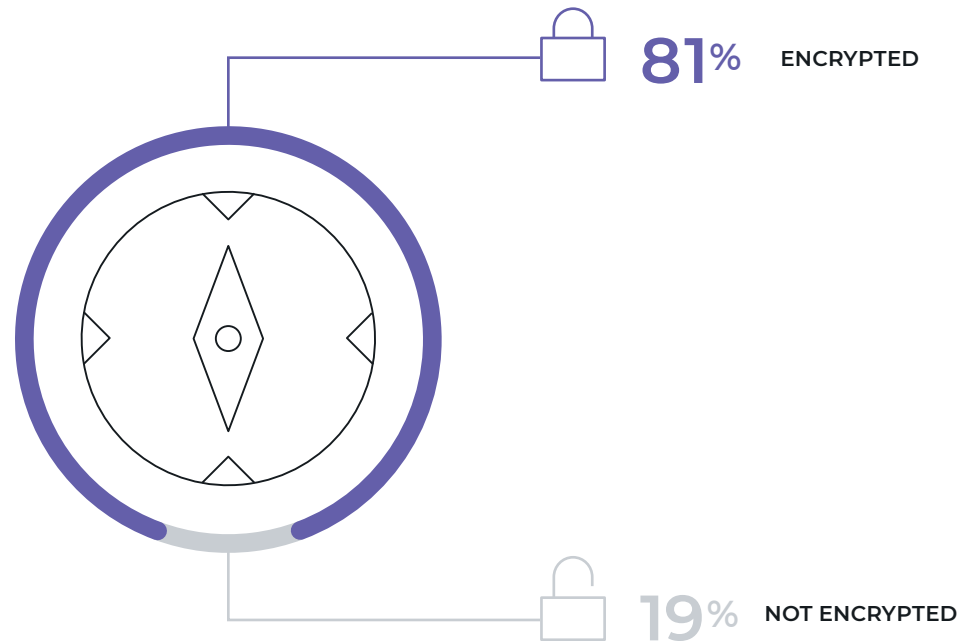
Findings and Discussion



81 Percent of North-South Traffic is Encrypted, 19 Percent is not

While it may not be surprising that the majority of north-south traffic is encrypted, the flip side is that 20 percent of public internet sites are **not** encrypted. In other words, your employees are interfacing with web applications over plain text, and that accounts for roughly one-fifth of all of organizations' internet-facing traffic. There are several dozens of hops along the users' connection routes, and anyone listening in on any of those devices can collect, or worse, manipulate, any data being transferred. This statistic can be useful for educating employees to best practices for online safety.

This 81 percent statistic also underscores the importance of decrypting and inspecting encrypted traffic. While it may not be surprising that the majority of north-south traffic is encrypted, the flip side is that almost 20 percent of public internet sites are **not** encrypted.

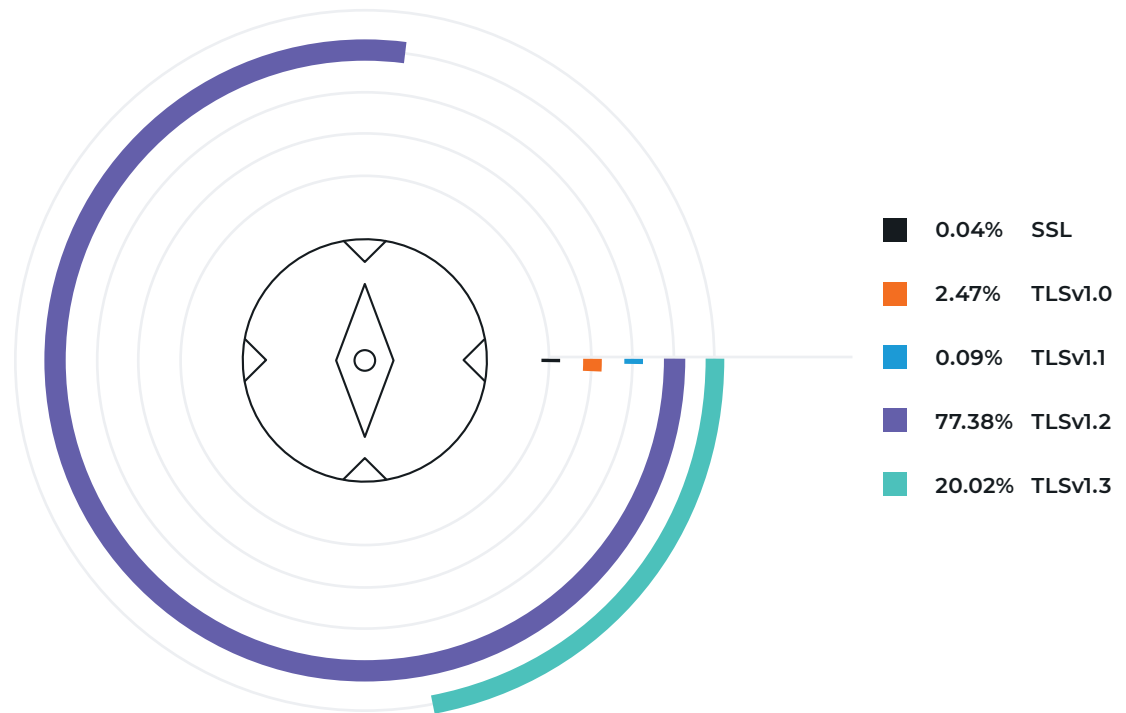


Findings and Discussion



TLS 1.3 is off to a Strong Start in North-South Traffic

TLS 1.3, released in August of 2018, is gaining momentum. About 20 percent of corporate internet traffic is now on TLS 1.3. This appears high at the first glance, but that's because top web services (Google and Facebook, for example) and content delivery networks (CDNs) are now on TLS 1.3 and the most common web browsers (Chrome, Firefox, Microsoft Edge, Safari) now also support TLS 1.3.

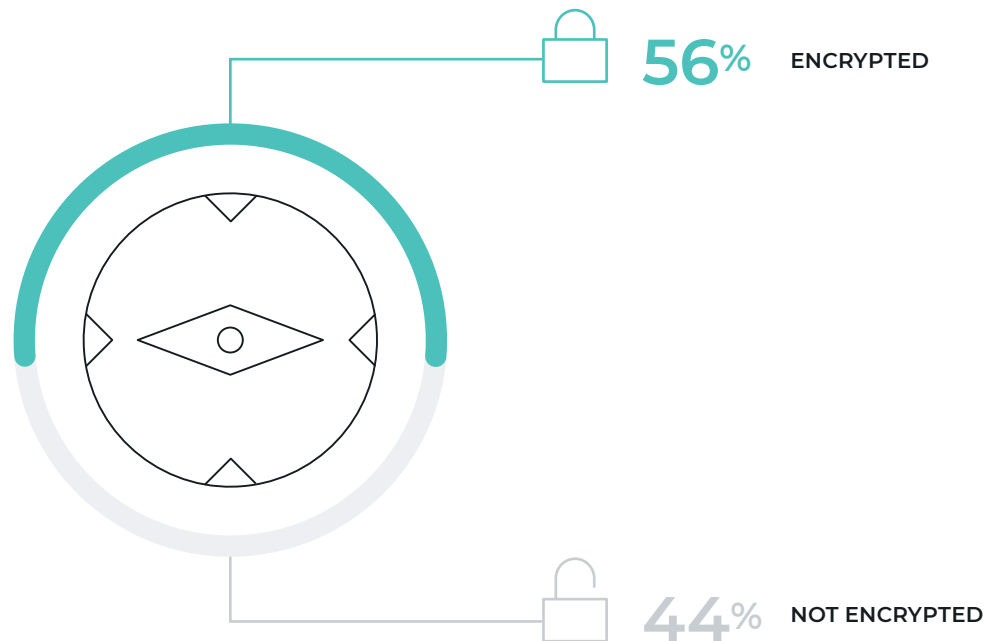


Findings and Discussion



56 Percent of East-West Traffic is Encrypted, 44 Percent is Not

The good news is that just over half of all internal traffic is encrypted, but that also means about half of all lateral traffic is not encrypted. While most headlines tout cyber espionage and state-sponsored attacks, two out of five security incidents come from inside the organization. According to recent research, organizations report that 42 percent of IT security incidents occur as a result of their employees' actions, and 74 percent originate from their extended enterprise (employees, customers, suppliers).¹ Encrypting all feasible east-west traffic is an opportunity for organizations to improve their security posture.



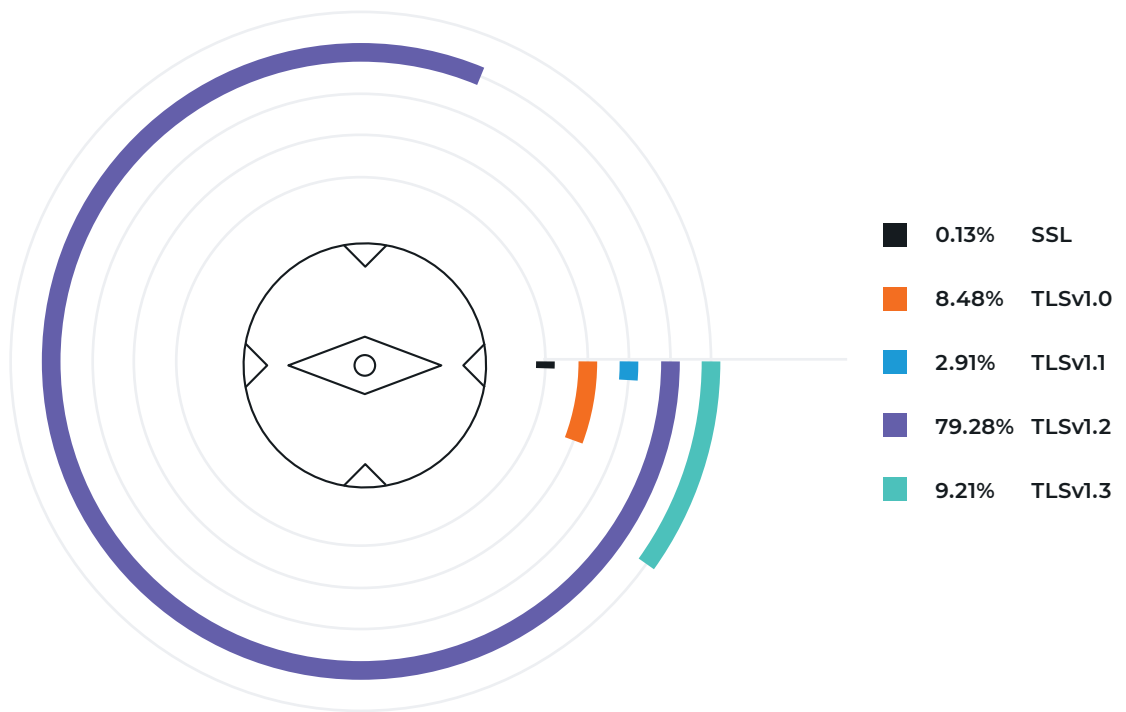
Findings and Discussion



TLS 1.2 Dominates East-West Traffic, but Outdated Protocols are Still Being Used

While the prominent use of TLS 1.2 isn't surprising, what is interesting is the prevalence of TLS 1.0 at 8.48 percent of all internal traffic. This could represent a risk to some organizations, particularly since TLS 1.0 is not approved for PCI, and IT would need to understand and risk-manage anything still using these highly deprecated protocols.

As we continue this research in future months, it will be interesting to see the trend with these statistics.



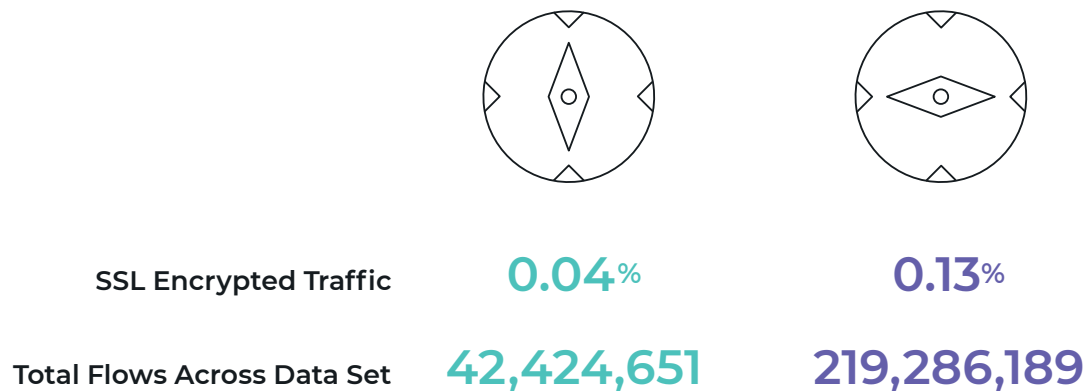
Findings and Discussion



SSL Lives – Securing Like it's 1999

While the volume of SSL traffic is not huge, the mere existence of live traffic on such an insecure protocol is significant, if not alarming. Netscape developed SSL 1.0 to secure the internet of 1995. There were significant issues with that version, so Netscape released two more versions that year. In 1999, the PCI council recommended deprecating SSL altogether and moving to TLS 1.0. While SSL v3 and TLS 1.0 are not interoperable, the latter was largely based on the former.

The existence of SSL may represent a misconfiguration, and its use is a risk indicator simply because it's so poorly supported by most monitoring tools. If seen in large quantities from a single source, it is definitely something that needs to be investigated because it could indicate an attempt to avoid security monitoring.



Recommendations

The objective of this report is to provide real-world metrics of SSL/TLS usage. If you currently inspect all of your encrypted traffic, we hope these statistics are a helpful baseline for planning and reporting purposes. If you are not currently inspecting encrypted traffic, maybe these findings will nudge your organization toward taking action.

Here is a basic set of guidelines on decryption and inspection:



Know your traffic's volume and composition

First, before deploying any SSL/TLS decryption solution, be aware of the total volume of traffic in your network and the amount of traffic that is SSL/TLS encrypted. A good free tool is NTOPNG, which can give valuable insight into your network. Understanding what traffic exists on your network is critical when deciding how and where to decrypt network traffic.



Know what traffic needs to be decrypted

Either you're hosting on-premises web applications that are accessed internally or externally, or you want to decrypt all the traffic leaving your network. Each case requires different techniques for on-premises web applications. In the first scenario, you'll need a private key for decryption. In the second, for outbound traffic you'll need to use man-in-the-middle (MITM) decryption.



Determine your solution's limitations

Different solutions offer different decryption capacity for inbound or outbound traffic. It's important to know how much traffic a solution can decrypt based on the active number of connections and volume of SSL/TLS traffic.



Have an inspection plan

Once you have traffic decrypted, where do you need to steer that traffic? Does just one tool need to see decrypted traffic, or multiple tools? The number of tools that require the decrypted traffic and the locations of these tools certainly play a role in the decision to decrypt.



Understand the impact of decryption on network devices

Many security tools and firewalls offer a decryption solution, but that sometimes impairs their primary function. In these cases, enabling SSL/TLS decryption can cause high CPU usage, degrading the tool's ability to inspect or block traffic. According to NSS Labs Test Reports, there was a 92 percent drop in the average connection rate of the products that perform decryption, with connection degradation from 84 percent to 99 percent.²



Plan for traffic growth

Decryption may be easy to configure for your current setup, but what happens when your traffic volume grows? Ask yourself how easy it would be to scale your decryption solution over time, and what would be the budget impact? Tip: Estimate the impact if your encrypted traffic increases X percent.



Research potential decryption platforms

Do research before deploying decryption solutions. Different solutions offer varied performance with different ciphers. Some solutions are easier to deploy or scale than others. We recommend you read the U.S. National Security Agency's "Managing Risk From the Transport Layer Security Inspection"² security advisory on TLS decryption and that you thoroughly research available solutions and associated pros and cons.



The Don'ts

While seeing all decrypted traffic may be good for security, decrypting financial and health data violates privacy laws. The solution must have the ability to distinguish data that needs to be decrypted from data that shouldn't be decrypted. Lastly, no matter how much a solution is tested in a lab environment, be aware that the production environment is different, and eliminate the possibility of outages with the ability to bypass in the event of a catastrophe.

Closing

In closing, enterprises are using a variety of encryption technologies for both north-south and east-west traffic, some of it obsolete and risky. We hope we have provided you with reasons and some high-level means to begin inspecting your TLS traffic. If you need further justification, we recommend the U.S. National Security Agency (NSA) [guidelines for decryption](#). For organizations that choose not to decrypt and inspect for whatever reason, it is still important to understand and communicate the risks with the organization.

REFERENCES

- 1 [“Insider Threat: 74% of Security Incidents Come from the Extended Enterprise, Not Hacking Groups.” Clearswift, 2017.](#)
- 2 Read Managing Risk from the Transport Layer Security Inspection [here](#), or on [NSA's site](#).

Contact Us

If you found this report to be useful, we encourage you to spread the word. If there are questions, changes or future research requests or would like to receive the next iteration of this research, we would love to hear from you: please email TLSResearch@gigamon.com or request a demo <https://www.gigamon.com/lp/free-trial/request-live-demo.html>.

To hear about how Gigamon helps track, decrypt and inspect TLS traffic, contact us at TLSResearch@gigamon.com.

Gigamon®