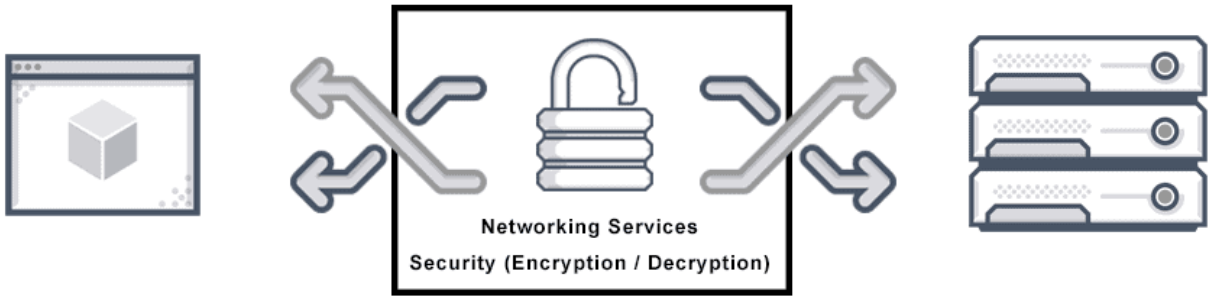

1

Addressing Security Visibility with TLS 1.3

Whitepaper

by

Haltdos

haltdos

TLS Visibility Issue

It is estimated that about 90 percent of enterprise web traffic is encrypted using some version of SSL/TLS. TLS (Transport Layer Security) is a tunnelling protocol that encapsulates application payload like DNS, HTTP, FTP, SIP, SMTP and others. TLS helps protect data traveling over the internet, secures our communications, and helps prevent eavesdropping and tampering attacks. The first version of TLS, 1.0, was released in 1999. Since then, three more versions of TLS have been released, the most recent, TLS 1.3, in 2018. To improve communications security on the internet, designers have changed protocols to strengthen security and better protect the secrecy of historical traffic, even if the servers' long-term secret keys are compromised. This process known as forward secrecy has made it more difficult for enterprises to implement network visibility strategies.

Need for Decryption

In any data center scenario there is both North-South and East-West traffic. The North-South traffic can be inbound, where external users are coming to your data center (DMZ). The other scenario is where your internal users are going out, accessing content on the web. The majority of the traffic in the data center is East-West. This is the communication between internal users and applications, as well as between applications.

Today, the majority of web traffic uses TLS 1.2, which was the most current version of TLS until TLS 1.3 was introduced in August 2018. TLS 1.3 adoption rate is on the rise as more web services and enterprise networks embrace the technology (the four top web browsers – Chrome, Firefox, IE, Edge support TLS 1.3 by default).

What benefits security teams, also benefits attackers. Attackers are now using encryption to transport malicious traffic applications exploits into and out of the enterprise environment, and encrypting the threat. According to Gartner, about 50 percent of malware attacks are encrypted. In 2020, about 60 percent of organizations are failing to effectively decrypt this traffic. This huge gap leaves enterprises extremely vulnerable to attacks and exploitations.

Typically, there are two decryption considerations: passive out-of-band and active inline (i.e. man-in-the-middle). Out-of-band is not applicable when using ephemeral or perfect forward secrecy (PFS) encryption (which TLS 1.3 enforces with restricted cipher suites support), and is limited to inbound deployments where private keys are available. This creates challenges to enterprise networks as it hides valuable metadata, blinding current security monitoring tools to the content so they are unable to detect threats. Consequently, this raises questions about how enterprise can meet security, operational, and regulatory requirements for critical services while using modern protocols such as TLS 1.3.

According to the Forrester report "Maintain Security Visibility in the TLS 1.3 Era, July 2020," "you have only a few years to prepare your security tools for TLS 1.3 and DNS-over-HTTPS." To protect your network and organization, it's critical to start acting now and prepare for the widespread adoption of TLS 1.3 and DNS over HTTPs.

Do it Once but do it Well

That's the recommendation from the NSA cybersecurity information report 2019 when decrypting and encrypting in enterprise networks. In order to minimize risks in breaking and inspecting TLS traffic, inspection should only be conducted once within the enterprise network. Redundant TLS inspection, wherein a client-server traffic flow is decrypted, inspected and re-encrypted multiple times should not be performed. Inspecting multiple times can greatly complicate diagnosing network issues with TLS traffic. Further, it obscures certificates when trying to ascertain whether a server should be trusted and adds unwanted latency to the network.

Sandwich Deployment Model

In order to bring TLS 1.3 visibility, we propose a Sandwich deployment model where one or more security devices are sandwiched between two SSL inspection layers.

The upper layer is client facing SSL/TLS decryption layer that decrypts incoming encrypted user traffic before sending traffic downstream. The lower layer of SSL inspection is meant for encrypting (previously decrypted) traffic before sending to web servers.
The architecture ensures adherence to compliance with end-to-end encryption using affordable off-the-shelf SSL / TLS offloading solutions like Application Delivery Controllers (ADC). For reliability, each layer can be built using two SSL inspection devices configured in HA mode (Active-Active or Active-Passive).

Between these two SSL inspection layers, various security solution can be implemented. Apart from the obvious benefit of avoiding multiple decryption and re-encryption, each solution implemented in the sandwich model will be able to run at its maximum throughput capacity and enhanced level of security inspection.

Let's look at some use cases that benefits from this deployment model:

Getting Decrypted SPAN traffic

Administrators can add a Layer 2 switch between the SSL / TLS inspection layers and take decrypted traffic feed over SPAN / TAP interface of the switch. This traffic feed can then be used by advanced analytics solutions in Security Operation Center (SOC) for enhanced visibility, correlation and attack detection.

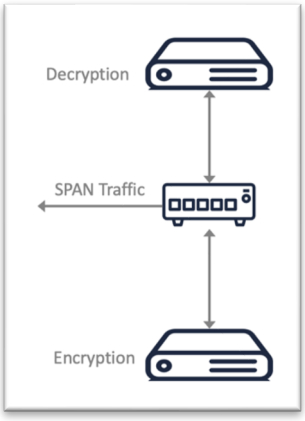

Fig 1: Generating decrypted SPAN traffic with Sandwich Model

Certificate Management

Updating SSL certificate bound to FQDN need only to be installed on the upper SSL inspection layer instead of all intermediate network and security devices thereby saving certificate upgradation challenges.

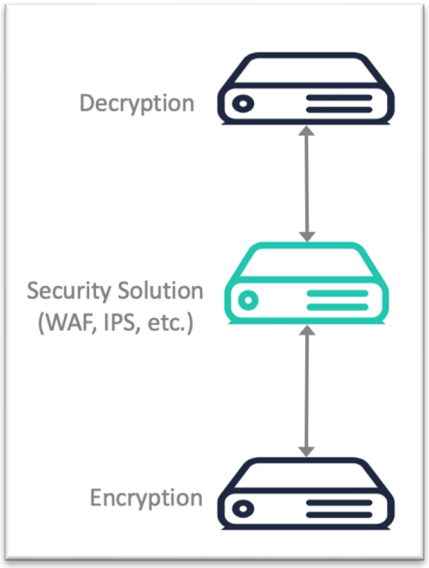

Fig 2: Implementing Security Solution with Sandwich Model

Improving Performance of Web Application Firewalls

SSL / TLS handshake is CPU intensive and can reduce performance of security devices by 40% in terms of throughput, especially when handling burst traffic. With dedicated SSL layers performing encryption / decryption, solutions like Web Application Firewalls, API Gateways, IPS/IDS can perform enhanced inspection without any overhead.

Approach Benefits

Low Overhead, Reduced Latency

Decrypting once and feeding multiple security tools simplifies operations and the security stack. The InfoSec team doesn't have to employ multiple devices for decrypting and encrypting that lead to complexity, difficulty in troubleshooting and increased latency.

Regain Visibility & Control

By gaining complete visibility into encrypted traffic including TLS 1.3, InfoSec and NetOps teams, as well as security tools, are empowered with unparallel visibility to analyse and detect threats.

Increased Performance

By offloading decryption from security tools and providing decrypted traffic, the performance of the tools is significantly enhanced to inspect threats without dropping packets as well as prolonging the life of the tools. Furthermore, latency is reduced by minimizing the number of times needing to decrypt and re-encrypt. Furthermore, by offloading decryption from overburdened security tools,

organizations are able to protect and extend current investment and spend less on purchasing new tools.

Interoperability

With dedicated inline decryption and encryption devices, existing security solutions and older versions of application would not require any change when migrating between SSL and TLS versions. Policies required to support legacy clients can also be configured per-application basis without any operational overheads.

Conclusion

TLS 1.3 has thrown up visibility challenges for security administrators. Technology innovation, necessarily does not need to be a complex design feature. Security administrators can deploy simplified solutions to address their security requirements.

This whitepaper addresses a simple approach to a Secure network architecture design addressing TLS 1.3 visibility challenges using off-the-shelf solution.