Whitepaper

Improve Network Visibility with Advanced Inline SSL/TLS Decryption Solutions

Overview

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are vital Internet technologies. Countless applications are protected by SSL/TLS encryption, such as web browsing, email, e-commerce, voice-over-IP, online banking, instant messaging, remote health, and file storage. Users expect their data to be secure. SSL and its later variant TLS are how most companies encrypt that data. In fact, Gartner now estimates that 80 percent of enterprise traffic will be encrypted by 2019.[1]

Unfortunately, many security and performance monitoring tools used by enterprises today do not have visibility inside encrypted sessions. If you do not have a line of sight into these encrypted sessions, how can you ensure that content is safe? You simply cannot protect against what you cannot see. Moreover, monitoring application performance and network usage patterns becomes impossible if you cannot determine which applications are running over the network.

Because encrypted traffic is so hard to inspect, advanced malware increasingly hides inside SSL/TLS sessions, confident security tools will not block its traffic. These attacks include:

- Malware sent over file transfer capabilities in IM and email, which is protected from inspection by SSL/TLS.
- Malicious use of encryption for data exfiltration by insiders.
- Malware distributed over social media, which utilize SSL/TLS to encrypt and shield communications from third-party inspections.
- Malicious use of SSL to exfiltrate information, infiltrate corporate networks or perform Distributed Denial of Service (DDoS) attacks using known SSL vulnerabilities to flood servers.
- Malware to command and control servers via SSL/TLS.

A recent Trustwave security report estimates that 36 percent of malware uses encryption.[2] The sad fact is that the very technology that makes the Internet secure has become a significant threat vector.

This whitepaper examines the benefits and challenges of some of the most common approaches available today to inspect encrypted traffic and introduces innovative new technology from Gigamon that delivers an advanced inline SSL/TLS solution to foster network visibility.

Today's Point Solutions Come at a High Cost

The growing security threat posed by uninspected SSL/TLS sessions increases the urgency for inspecting SSL/TLS traffic. SSL/TLS decryption is required for a variety of applications:

- Malware Detection: Once malware exploits a host, it can use SSL/TLS encrypted transactions to communicate with a command and control server.
- Data Loss Prevention: Whether initiated by malware or a user from inside the corporate firewall, confidential data and files can be encrypted and leaked using SSL/TLS connections.
- Application Performance Monitoring: Key business applications use SSL/TLS to ensure authentication, but this obscures data required for proper monitoring.
- Cloud Services Monitoring: Secure services running in the cloud, including Web applications, all look the same at the TCP layer and it is not until the SSL/TLS sessions are decrypted that they can be differentiated and monitored.

However, decrypting SSL/TLS is a tremendous processing burden for monitoring tools that do it themselves; this greatly inhibits tool performance and increases the cost of monitoring.

Faced with a landscape of dynamic and expanding threats, many organizations are compelled to take a multi-tiered approach to security, utilizing both inline and out-of-band security appliances to protect critical information assets. Whereas an inline approach places the security appliance in the path of data traffic at critical locations needing protection, the out-of-band approach makes a copy of that traffic to perform the necessary inspection.

[1]Gartner "Predictions 2017: Network and Gateway Security," December 13, 2016. https://www.gartner.com/doc/3542117/predicts--network-gateway-security
[2]Trustwave Global Security Report, https://www2.trustwave.com/2017-Trustwave-Global-Security-Report.html

A multi-tiered security deployment may span web application firewalls (WAFs), malware detection, intrusion detection or prevention systems (IDS/IPS), data loss prevention (DLP) and other network security devices that inspect various components of network traffic in real time. This can become very complex very quickly.

That is because these security solutions depend on relevant, consistent and accurate streams of network traffic to identify threats and stop attacks. Clearly, as visibility for security and operations management depends on live network traffic feeds, the traditional method of connecting traffic-based appliances directly to the network is no longer sustainable for the modern, agile enterprise. This lack of visibility is exacerbated by:

- The growth in enterprise traffic being carried over SSL/TLS connections and the increased number of locations in the infrastructure, from which data must be acquired for security inspection.
- The increasing bandwidth of core networks, caused by both the increased speed of the links from 1G, to 10G, 40G, and 100G.
- The introduction of flatter core architectures – especially leaf-spine architectures – which means that we have much greater network bisection bandwidth, translating into a greater bottleneck bandwidth for the network.
- The need to inspect east-west traffic patterns arising from the growth in virtualized and cloud deployments.

SSL/TLS decryption is available directly on some monitoring tools. However, using these solutions for that purpose tends to cause a severe performance degradation. NSS Lab reports that the performance of security appliances can drop by 80 percent when SSL/TLS decryption is done on an appliance such as a firewall.[4] As certificate authorities shift to larger keys, SSL/TLS decryption engines will have to bear an even greater workload. Many monitoring tools are based on general-purpose processors from Intel and AMD, which lack crypto acceleration required for efficient decryption of SSL/TLS traffic, thereby causing severe performance degradation

The drastic slowdown in the performance of a firewall, web gateway or an IPS when they are called to decrypt or re-encrypt traffic leads to unnecessary upgrades of these appliances. SSL/TLS processing significantly increases the network traffic inspection investment due to the hardware, software and support costs to handle the additional workload increase. Offloading SSL/TLS decryption not only allows the tools to return to full performance but also eliminates the need to have multiple decryption licenses for multiple tools.

Existing inline technologies, such as firewalls, web security gateways, SSL proxies and application load balancers provide SSL/TLS decryption, but they are not optimized for a visibility architecture. Solutions such as firewalls and web security gateways decrypt SSL/TLS traffic but often cannot share that decrypted traffic to other monitoring and security tools. Likewise, load balancers are good at terminating SSL/TLS traffic and load balancing to servers but lack the ability to distribute this traffic to multiple inline security tools prior to re-encryption. With limited modularity or extensibility, increasing SSL/TLS throughput often requires new hardware. Lastly, these solutions lack the traffic selection controls to forward non-encrypted traffic at line rate and often send all traffic to the decryption engine, creating performance issues.

There is however a better way, one that is less complex, does not degrade performance and results in cost efficiencies.

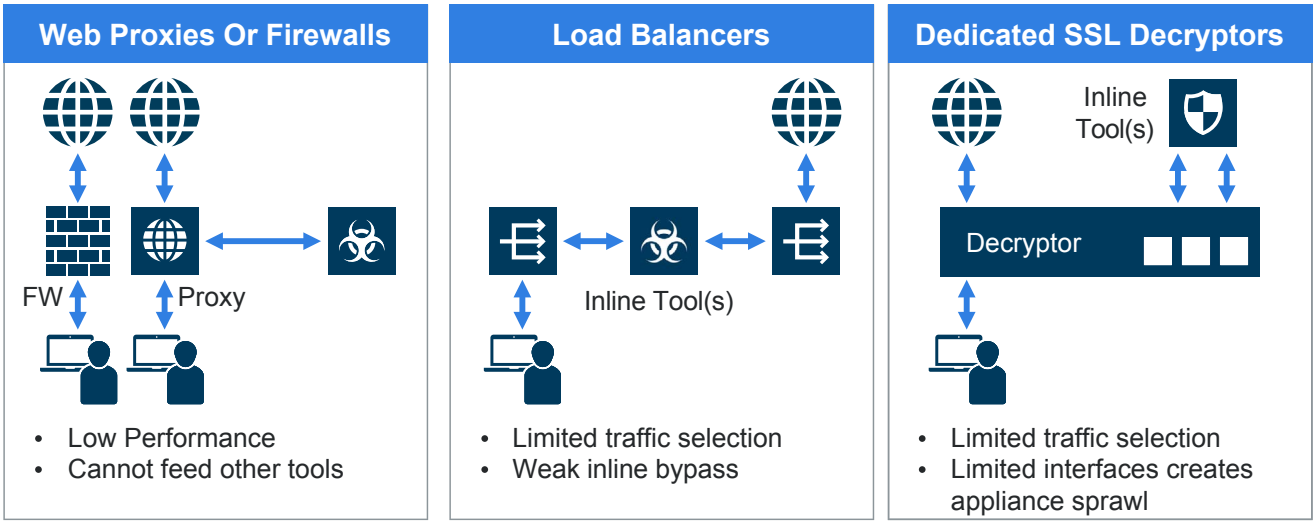

Figure 1: Traditional Approaches to Decrypting SSL/TLS Traffic

[4]John Pirc, "SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvements," NSS Labs 2013. https://www.nsslabs.com/linkservid/13C7BD87-5056-9046-93FB736663C0B07A/

A Better Approach: "Decrypt Once, Feed Many Tools"

Legacy architectures described in the previous section were acceptable when the amount of SSL/TLS traffic was a small percentage of overall network traffic. Gartner now estimates that in 2019 over 80 percent of traffic will be encrypted[5]. As the volume of encrypted traffic continues to rise, organizations are more vulnerable to encrypted attacks, hidden command and control threats and data exfiltration exploits that go undetected. Gartner further recommends that security and risk leaders "ensure that network traffic will be decrypted only once."[6]

The Gigamon GigaSECURE® SSL/TLS Decryption solution, with inline capabilities, brings visibility into encrypted data. This marks the first time such a capability is available on a Visibility Platform, enabling security operations to take a unique architectural approach of a "decryption zone" to solve the problem of SSL/TLS decryption. In a "decryption zone," SSL/TLS traffic is decrypted once and fed to multiple security and operational tools for analysis, thereby eliminating unnecessary and repetitive cycles of decryption and re-encryption within the infrastructure.

With its expanded SSL/TLS decryption solution, Gigamon delivers network visibility to expose malicious threats and feeds decrypted traffic-of-interest to the appropriate security tools for immediate analysis and mitigation.

Inline SSL/TLS decryption addresses a vastly expanded universe of use cases such as monitoring access to Internet-based services for risk or compliance violations, detecting malicious activities such as command and control communications, decrypting TLS sessions that use modern cipher suites and above all, creating an efficient framework to manage encrypted traffic at scale.

The Gigamon Visibility Platform offers the SSL/TLS Decryption solution as an application on the purpose-built GigaSMART® hardware module. This application complements other GigaSMART applications on the platform, such as de-duplication, application session filtering, data masking, and metadata generation. that optimize, automate and deliver traffic-of-interest to the appropriate monitoring and security tools across the network.

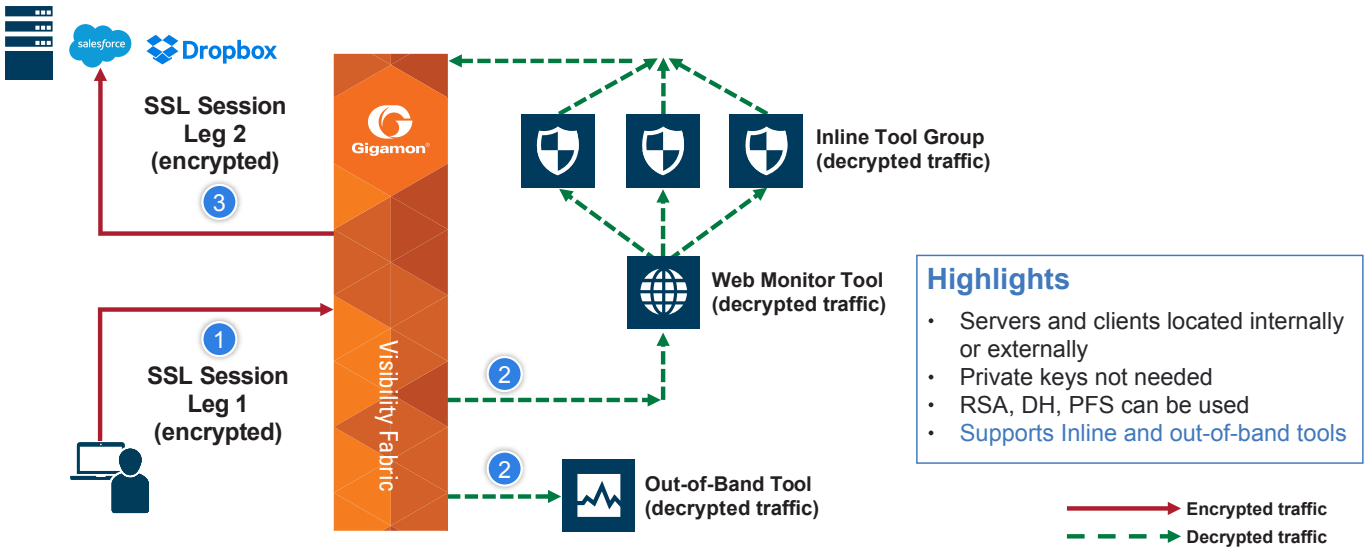

Figure 2: Gigamon Inline SSL Viibility Solution

[5]Source: Gartner "Predicts 2017: Network and Gateway Security", December 13 2016
[6]Source: Gartner "Hype Cycle for Threat Facing Technologies 2017", July 17 2017

Benefits of Using Gigamon SSL/TLS Decryption Solution

Security Operations teams who are challenged to manage increasing volumes of encrypted traffic can now avoid repetitive decryption and re-encryption of SSL/TLS sessions by tools not purpose-built for decryption. They can circumvent unnecessary appliance sprawl and its related costs, complexity and potential to introduce latency. SSL/TLS decryption is an inherently compute-intensive function, so by centralizing this function in the Gigamon Visibility Platform, the processing capacity of security tools can be freed to focus on their primary functions.

There are six key benefits of this approach:

1. **Decrypt Once; Feed Many Tools**
   The Gigamon SSL/TLS decryption solution enables a "decrypt once and feed to multiple tools" design for improved scale and resiliency. A key enabler of this solution is an advanced set of traffic selection and distribution capabilities in the Gigamon Visibility Platform that simplifies deployment of SSL/TLS decryption at scale, enhancing existing security tools by centralizing and offloading SSL/TLS decryption and re-encrypting in the same device. Moreover, Gigamon features inline bypass such that in the event of a tool failure, traffic can be redistributed to the remaining healthy tools.

2. **Automatic SSL/TLS Detection on Any Port or Application**
   The Gigamon SSL/TLS decryption solution provides automatic visibility into SSL/TLS traffic regardless of TCP port or application, so that you can monitor application performance, analyze usage patterns and secure your network against malware hiding in SSL/TLS and STARTTLS sessions.

3. **Scalable Interface Support**
   The Gigamon SSL/TLS decryption solution operates in networks that range from 1Gb to 100Gb. The flexibility in interface support allows you to connect fast networks to security tools with slower interfaces.

4. **Strong Crypto Support**
   The Gigamon SSL/TLS decryption solution supports a broad range of ciphers including RSA, Diffie-Hellman (DH), Diffie-Hellman Ephemeral (DHE), Perfect Forward Secrecy (PFS) and Elliptic Curve.

5. **Certificate Validation and Revocation Lists**
   The Gigamon SSL/TLS decryption solution works with any certificate authority and checks the certificate validity against Certificate Revocation Lists (CRLs) as well as Online Certificate Status Protocol (OCSP) to strengthen your organization's security posture.

6. **Strong Privacy Compliance**
   Advanced policies enable traffic filtering and selective decryption based on URL categorization using the market-leading Webroot BrightCloud® Web Classification Service, domain names as well as whitelist and blacklist policies to ensure that sensitive data remains secure and to meet data privacy and compliance requirements. These privacy controls ensure that security administrators can set policies that are in compliance with governance controls, industry and government regulations, such as policies to decrypt traffic that does not contain any personally identifiable information or other sensitive information, or to only decrypt traffic exiting the organization but not internal traffic.

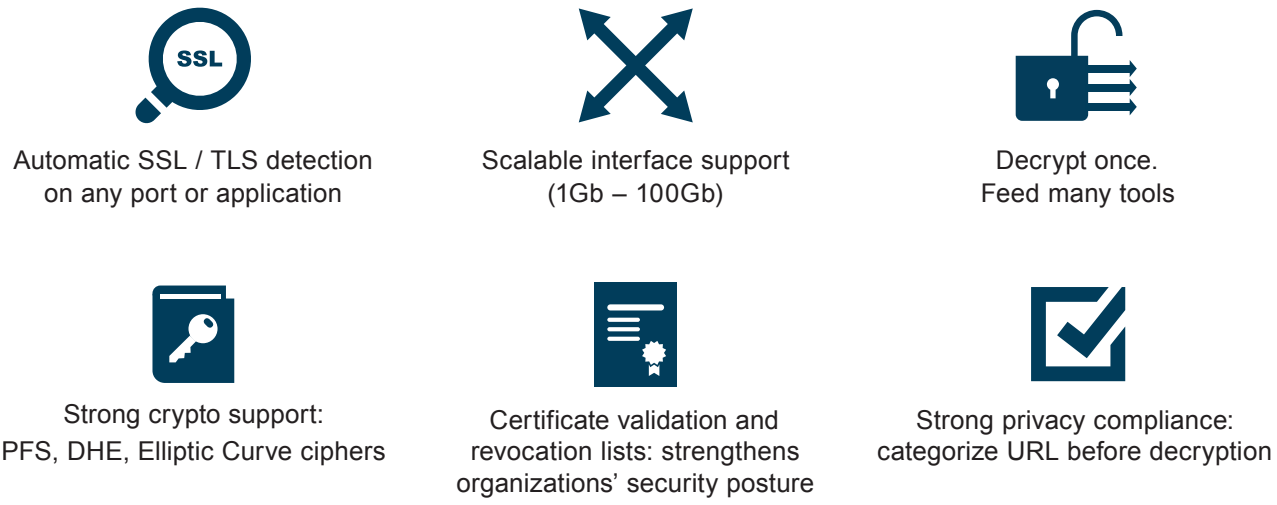

Figure 3: Key Benefits of Gigamon SSL/TLS Decryption

Best of all, the Gigamon decryption solution scales as your needs increase. One instance of SSL/TLS Decryption in a Gigamon visibility cluster is sufficient for any port in a cluster to take advantage of SSL/TLS decryption. Enterprises can increase SSL/TLS decryption throughput by simply adding more GigaSMART modules.

Summary

With the recent increase in SSL/TLS-encrypted traffic comes the need for multiple security tools to decrypt and inspect SSL/TLS traffic. Without decryption, the growing threat of malware is invisible to security tools that cannot see inside encrypted sessions. While legacy solutions can do the job, their approach leads to massive inefficiencies such as performance degradation, unnecessary replication of the same functionality in multiple tools, repetitive decryption and re-encryption actions and unnecessary increased expenditure. Integrating inline SSL/TLS decryption with a visibility platform represents a strategic technology evolution that significantly increases overall infrastructure efficiency. Organizations can now manage growing SSL/TLS traffic volumes by creating a centralized "decryption zone" to decrypt traffic once and giving security tools newfound visibility into formerly encrypted traffic and threats.

Next Steps

- View the Gigamon SSL Decryption Application Note: **https://www.gigamon.com/content/dam/resource-library/english/application-note/an-ssl-decryption.pdf**
- Visit the Gigamon SSL/TLS Decryption web page: **https://www.gigamon.com/products/traffic-intelligence/gigasmart/ssl-tls-decryption.html**
- Watch Networking Field Day videos to learn about Gigamon SSL/TLS Decryption: **https://insight.gigamon.com/TechFieldDay-On-Demand-Videos-Registration.html**
- Find out for yourself why Gigamon is the best choice for your business:
  - Speak to a Gigamon expert: **https://www.gigamon.com/contact-sales.html**,
  - Ask for a demonstration: **https://insight.gigamon.com/aws-test-drive.html**
  - Sign up for a free trial today! **https://insight.gigamon.com/TryandBuyPromo.html**

3244-01 08/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com