SSL/TLS Decryption

Powered by the Gigamon Visibility and Analytics Fabric with GigaSMART

Bad actors are now instigating 50 percent of new malware campaigns using encryption to conceal delivery and ongoing communications, including data exfiltration. This is why network and security operations teams must not give a free pass to encrypted traffic.

The Gigamon Visibility and Analytics Fabric™ with licensed GigaSMART® Decryption enables operations teams to have full visibility into encrypted traffic, including TLS 1.3, on any TCP port or application.

“Over 94 percent of Google traffic is encrypted, and 96 of the top 100 non-Google sites, accounting for 25 percent of the total throughput, implement encryption by default.”
Source: https://transparencyreport.google.com/https/overview?hl=en

“Up to 40 percent of large enterprises have already instituted TLS 1.3.”
Source: https://www.ssllabs.com/ssl-pulse/

“During 2020, more than 50 percent of new malware campaigns will use various forms of encryption and obfuscation to conceal delivery, and to conceal ongoing communication, including data infiltration.”

KEY FEATURES

- Automatic SSL and TLS detection on any TCP port
- Scalable interface support (10M–100Gbs)
- Decrypt once, feed many tools
- Policy-based selective decryption
- Supports all advanced ciphers including TLS 1.3 with Perfect Forward Secrecy
- Supports non-NAT/PAT L3 explicit tools (e.g., firewalls)
- Supports SSL/TLS split proxy

KEY BENEFITS

- No blind spots on the network
- Legacy tools can connect to the fabric
- Enhanced tool performance
- Preserve data privacy and compliance
- Maximum session security with latest cryptographic standards
- Optimize protection of East-West traffic
- Enable independent security algorithms on client and server sides
Gain Visibility and Control

To gain visibility and control of the sharply rising amount of encrypted traffic and its attendant security threats, you need to first decrypt inbound and outbound encrypted communications.

Decryption is a processor-intensive function that steals a large amount of resources from security tools. In a study of eight leading next-generation firewalls, NSS Labs found that turning on SSL/TLS decryption degraded the firewall performance by as much as 80 percent and reduced transactions per second by as much as 92 percent.

In contrast, by using the Gigamon Visibility and Analytics Fabric with GigaSMART you can offload decryption processing so security tools focus on detection and mitigation of malware. The GigaSMART license gives your operations teams automatic visibility into encrypted traffic, regardless of TCP port or application, to secure networks against data breaches and hidden malware in encrypted networks.


THE SOLUTION

Using the Gigamon Visibility and Analytics Fabric with GigaSMART lets you offload decryption processing so security tools focus on detection and mitigation of malware.

A GigaSMART license gives your operations teams automatic visibility into encrypted traffic, regardless of TCP port or application — to secure their networks against data breaches and hidden malware in encrypted networks.

Gigamon also integrates with the Venafi Trust Protection Platform™ to centralize key management and validation.

Figure 1: Network topology with the Gigamon Visibility and Analytics Fabric decrypting and sharing plain-text traffic with in-band and out-of-band tools.
Flex Inline and Decryption

It’s easy to configure Flex Inline Decryption using GigaVUE-FM Fabric Manager with the built-in fabric maps feature.

Figure 2 shows a standard fabric map. The GigaSMART “GS” cards create a decryption zone within the inline map.

Need to make changes? Simply drag and drop to move tools in and out of the zone as needed.

Technical Features

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>SPECIFICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products supported</td>
<td>GigaVUE-HC1 One engine per chassis, one engine per module</td>
</tr>
<tr>
<td>Hardware required</td>
<td>At least the base chassis</td>
</tr>
<tr>
<td>Software required</td>
<td>GigaSMART SSL/TLS Decryption license (see GigaSMART datasheet)</td>
</tr>
<tr>
<td>SSL/TLS versions supported</td>
<td>SSLv3, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3</td>
</tr>
<tr>
<td>Interfaces supported</td>
<td>1 and 10Gbps</td>
</tr>
<tr>
<td># of categories supported for selective decryption</td>
<td>83</td>
</tr>
<tr>
<td>Inline SSL throughput per engine</td>
<td>2Gbps (Gen2)</td>
</tr>
<tr>
<td>Passive SSL throughput per engine</td>
<td>6.8Gbps (Gen2)</td>
</tr>
<tr>
<td>Inline SSL concurrent connections per engine</td>
<td>100,000 (Gen2)</td>
</tr>
<tr>
<td>Passive SSL concurrent connections per engine</td>
<td>880,000 (Gen2)</td>
</tr>
<tr>
<td>Inline SSL connection rate per engine</td>
<td>1,500 (Gen2)</td>
</tr>
<tr>
<td>Passive SSL connection rate per engine</td>
<td>9,600cps (Gen2)</td>
</tr>
<tr>
<td>Physical inline bypass options</td>
<td>1 and 10Gbps</td>
</tr>
<tr>
<td>FIPS 140-2 certification</td>
<td>–</td>
</tr>
<tr>
<td>Split proxy function</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note:
- Gen3 GigaSMART engine performance will be provided in future updates.
- Passive SSL/TLS Decryption is also supported by Cloud Suite. Performance characteristics for Cloud Suite will be provided in future updates.
Conclusion

Identify hidden threats in both inbound and outbound encrypted traffic with the Gigamon Visibility and Analytics Fabric and GigaSMART. Decrypt once and share across all tools, scaling and increasing the efficacy of each by eliminating the processor overhead. The result: Tools operating at peak performance to do what they are best at — malware mitigation.

For more information on GigaSMART Decryption, please visit gigamon.com/ssl-decryption.