TLS Decryption

Powered by the Gigamon Deep Observability Pipeline with GigaSMART

FIPS
VALIDATED
140-1
LEVEL 1

Introduction

91 percent of threats are using encrypted channels[1] 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 Deep Observability Pipeline with licensed GigaSMART® decryption enables operations teams to have full visibility into encrypted traffic, including TLS 1.3, on any TCP port or application.

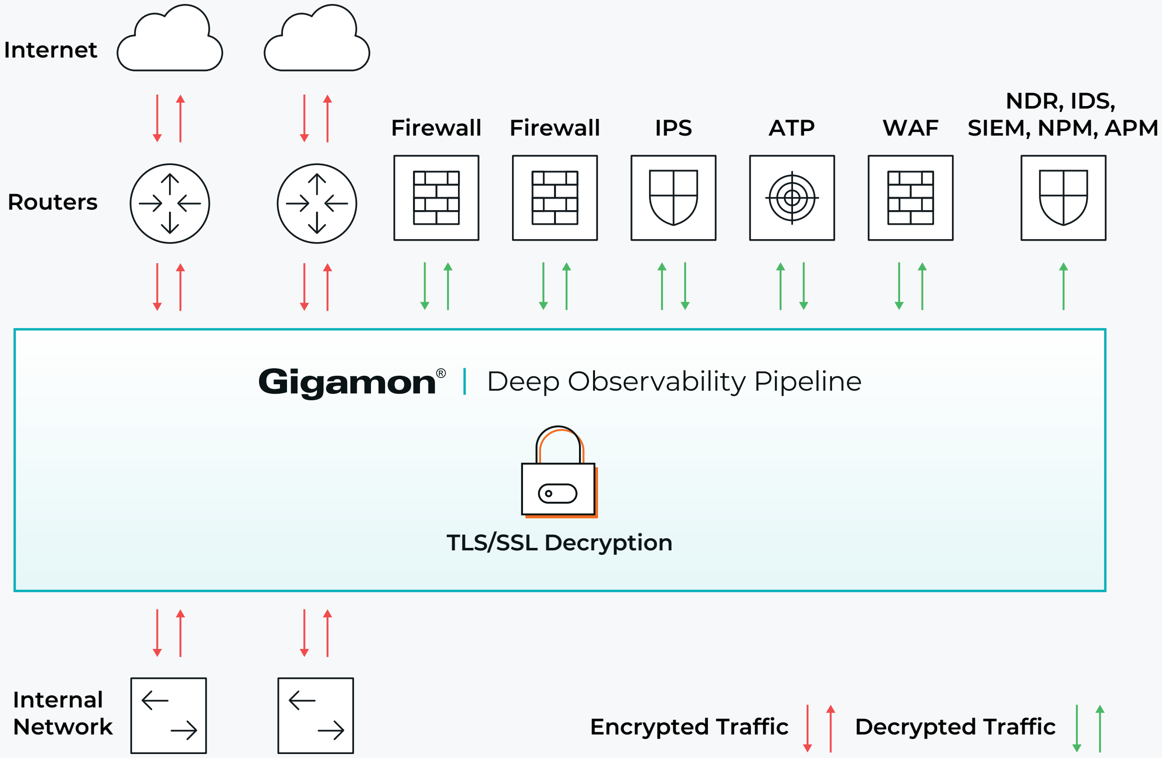

Figure 1. Network topology with the Gigamon Deep Observability Pipeline decrypting and sharing plain-text traffic with in-band and out-of-band tools.

Key Features

- Complete visibility into inbound/outbound traffic
- Automatic TLS/SSL detection on any TCP port
- Decrypt once, feed many tools
- Flexible feeds & speeds and interface support (10M–100Gbs)
- Full control over tool traffic and content.
- Protect tool performance and scale as needed
- Supports all advanced ciphers and TLS 1.3
- Supports NAT/PAT L3 explicit tools (for example, firewalls)
- Supports TPM and HSM products

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 North-South and East-West traffic
- Enable independent security algorithms on client and server sides

Gain Visibility and Control

The increasing volume of encrypted traffic poses a significant security challenge. To effectively address this challenge, organizations need to gain comprehensive visibility and control over encrypted traffic. This can be achieved by decrypting both inbound and outbound encrypted communications.

However, decryption is a resource-intensive operation that can significantly impact the performance of security tools. A study by NSS Labs found that activating TLS/SSL decryption on eight leading next-generation firewalls caused a significant drop in firewall performance, with reductions reaching up to 80 percent[2].

The Gigamon Deep Observability Pipeline with GigaSMART addresses this challenge by offloading the decryption processing to a dedicated appliance. This frees up security tools to focus on their primary function of detecting and mitigating threats. As a result, organizations can gain the visibility they need to protect their networks without sacrificing performance.

The GigaSMART decryption solution also provides automatic visibility into encrypted traffic, regardless of the TCP port or application. This helps organizations to identify and respond to threats that may be hidden in encrypted traffic.

The Solution

The Gigamon Deep Observability Pipeline, with GigaSMART capabilities, can help you efficiently offload the decryption processing burden from your security tools. This frees up your security tools to focus on their primary function of identifying and mitigating malware threats.

With a GigaSMART license, your NetOps, SecOps, and InfoSec teams can automatically gain enhanced visibility into encrypted traffic, regardless of the TCP port or application. This increased visibility helps to protect your networks from potential data breaches and concealed malware threats that may be lurking in encrypted network channels.

Gigamon integrates with the Venafi Trust Protection Platform and Entrust nShield HSM to centralize key management and validation. The Venafi Trust Protection Platform uses the Entrust nShield HSM for private key generation for TLS/SSL keys and certificates.

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 how GigaSMART engines 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.

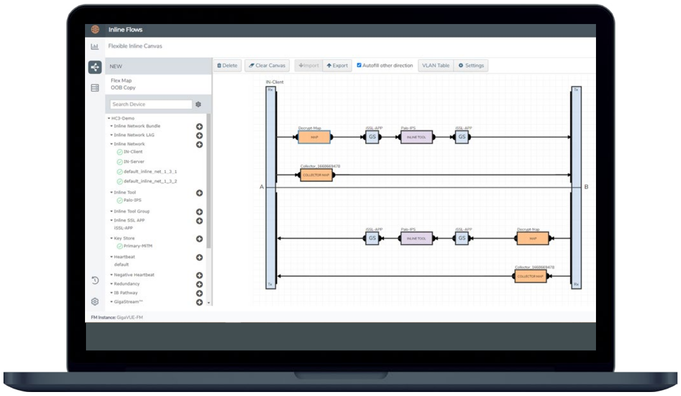

Figure 2. GigaVUE-FM Flex Inline and decryption.

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.[3]

Up to 40 percent of large enterprises have already instituted TLS 1.3.[4]

In 2022, more than 85 percent of attacks took place in encrypted traffic, with 90 percent of those threats involving malware.[5]

Technical Features

Features	**Specifications**		
Products supported	**GigaVUE-HC1** One engine per chassis, One engine per module	**GigaVUE-HC1-Plus** One engine per chassis, One engine per module	**GigaVUE-HC3** Two engines per module
Hardware required	At least the base chassis		
Software required	GigaSMART TLS Decrypction license (see GigaSMART data sheet)		
TLS/SSL versions supported	SSLv3, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3		
Hardware Security Module (HSM) support	Yes (Entrust nShield HSM)		
IPv6 support (Passive and Inline TLS/SSL Decryption)	Yes		
Interfaces supported	1 and 10Gbps	1, 10, 25, 40, and 100Gbps	10, 40, and 100Gbps
# of categories supported for selective decryption	83		
Inline SSL throughput per engine	2.9Gbps (Gen2), 4.6Gbps (Gen3)	4.5Gbps (Module) 7.4Gbps (Built-in)	9.2Gbps (Gen2), 7.3Gbps (Gen3)
Passive SSL throughput per engine	9.3Gbps (Gen2), 19Gbps (Gen3)	18Gbps (Module) 32Gbps (Built-in)	35.9Gbps (Gen2), 48.1Gbps (Gen3)
Inline SSL concurrent connections per engine	100,000 (Gen2), 100,000 (Gen3)	100,000 (Module) 200,000 (Built-in)	200,000 (Gen2), 200,000 (Gen3)
Passive SSL concurrent connections per engine	1,000,000 (Gen2), 1,000,000 (Gen3)	1,000,000 (Module) 1,000,000 (Built-in)	1,000,000 (Gen2), 1,000,000 (Gen3)
Inline SSL connection rate per engine	1,600 (Gen2), 8,500 (Gen3)	8,000 (Module) 13,000 (Built-in)	5,102 (Gen2), 13,000 (Gen3)
Passive connection rate per engine	9,450cps (Gen2), 30,000cps (Gen3)	30,000cps (Module) 55,000cps (Built-in)	35,230cps (Gen2), 57,500cps (Gen3)
Physical inline bypass options	1 and 10Gbps	1, 10, 25, 40, and 100Gbps	40 and 100Gbps
FIPS 140-2 certification	Level 2		
Split proxy function	Yes		

Note: Passive TLS Decryption is also supported by GigaVUE Cloud Suite™. Performance characteristics for GigaVUE Cloud Suite will be provided in future updates.

GigaSMART TLS Performance Specifications

Values reflect the maximum available number of latest generation GigaSMART modules per chassis.

Inline

Model	Maximum Connections/Sec.	Maximum Throughput (Gbps)	Maximum Concurrent Connections
GigaVUE-HC3	104,000	58.4	1,600,000
GigaVUE-HC1-Plus	29,000	16.4	400,000
GigaVUE-HC1	18,600	11.8	300,000

Out-of-Band

Model	Maximum Connections/Sec.	Maximum Throughput (Gbps)	Maximum Concurrent Connections
GigaVUE-HC3	460,000	384.8	8,000,000
GigaVUE-HC1-Plus	115,000	68.92	3,000,000
GigaVUE-HC1	69,450	47.3	3,000,000
GigaVUE Cloud Suite per V Series instance (VM)	15,000	1.1	1,000,000

Notes

- Tested with TLS_AES128_SHA256 cipher suite.
- Throughput based on 2MB file (inline) and 1MB file (out of band).
- Concurrent connections and connections/second based on 1 byte file.
- For inline specifications, outbound and inbound modes are identical.
- Performance specifications per model are measured independently.
- Values are based on Gigamon internal lab tests and actual results in production could vary.

Conclusion

Unlock the potential to uncover concealed threats within both incoming and outgoing encrypted traffic using the dynamic combination of the Gigamon Deep Observability Pipeline and GigaSMART. Through a single decryption process, empower seamless information sharing across all tools, effectively scaling and enhancing the efficiency of each one by eliminating the processor burden. The outcome is a suite of tools operating at the pinnacle of their performance, fully equipped to excel in their specialized role — the mitigation of malware.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding the Gigamon Limited Warranty and its Product Support and Software Maintenance Programs, visit gigamon.com/support-and-services/overview-and-benefits.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

[1] Source: https://www.watchguard.com/wgrd-resource-center/security-report-q2-2021

[2] Source: Jen Stowe. "NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports." NSS Labs, Inc. July 24, 2018.

[3] Source: https://transparencyreport.google.com/https/overview?hl=en

[4] Source: https://www.ssllabs.com/ssl-pulse/

[5] Source: https://www.zscaler.com/blogs/security-research/2022-encrypted-attacks-report

Gigamon®

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