TLS Decryption

Powered by the Gigamon Deep Observability Pipeline with GigaSMART

FIPS VALIDATED 140-1 LEVEL 1

Introduction

GigaSMART® TLS/SSL decryption is a comprehensive solution designed to provide deep observability into encrypted network traffic. It enables operations teams to have full visibility into encrypted traffic, including TLS 1.3, on any TCP port or application.

TLS/SSL decryption offers a comprehensive dashboard within GigaVUE-FM that delivers detailed insights into session performance, network capacity, and traffic decryption. This enables SecOps and NetOps teams to monitor decryption status, analyze trends, and identify anomalies in real-time, enhancing security, and compliance.

© 2025 Gigamon. All rights reserved.

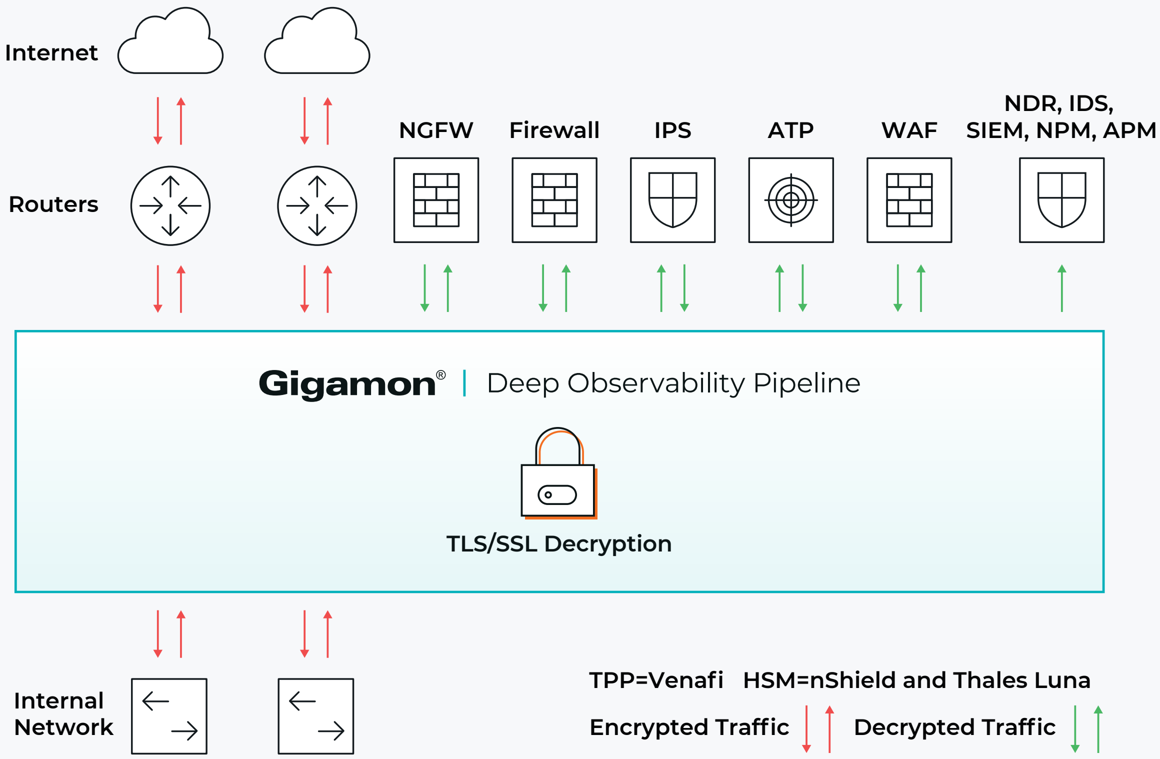

Figure 1. Network topology with the Gigamon Deep Observability Pipeline decrypting and sharing plain-text traffic with in-band and out-of-band tools.

Key Features

- Complete visibility into inbound/outbound traffic
- Visualize encrypted traffic with TLS/SSL Dashboard
- 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 L3/L4 NAT/PAT to explicit tools (for example, firewalls)
- Supports TPP and HSM products

Key Benefits

- Visiblity into inbound and outbound encrypted traffic
- Troubleshoot and monitor issues in encrypted traffic easily
- Improve tool performance by offloading decryption functions from the tools
- Preserve data privacy and compliance
- Maximize session security with latest cryptographic standards
- An essential element to Zero Trust Architecture

© 2025 Gigamon. All rights reserved.

Over 96 percent of Google traffic is encrypted.[2]

Up to 40 percent of large enterprises have already instituted TLS 1.3.[3]

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. TLS/SSL decryption can cause a significant drop in firewall performance.

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.

With TLS/SSL Dashboard, troubleshooting and monitoring TLS/SSL health is easy. The dashboard is accessible through GigaVUE-FM Fabric Health Analytics and helps organizations visualize encrypted traffic to assess performance, compliance, and risks in encrypted traffic. Get granular real-time stats and analyze URLs, CPU, memory, TLS versions, cipher suites, connection rates, concurrency numbers, and more. Easily investigate issues with historical data, track trends and generate reports.

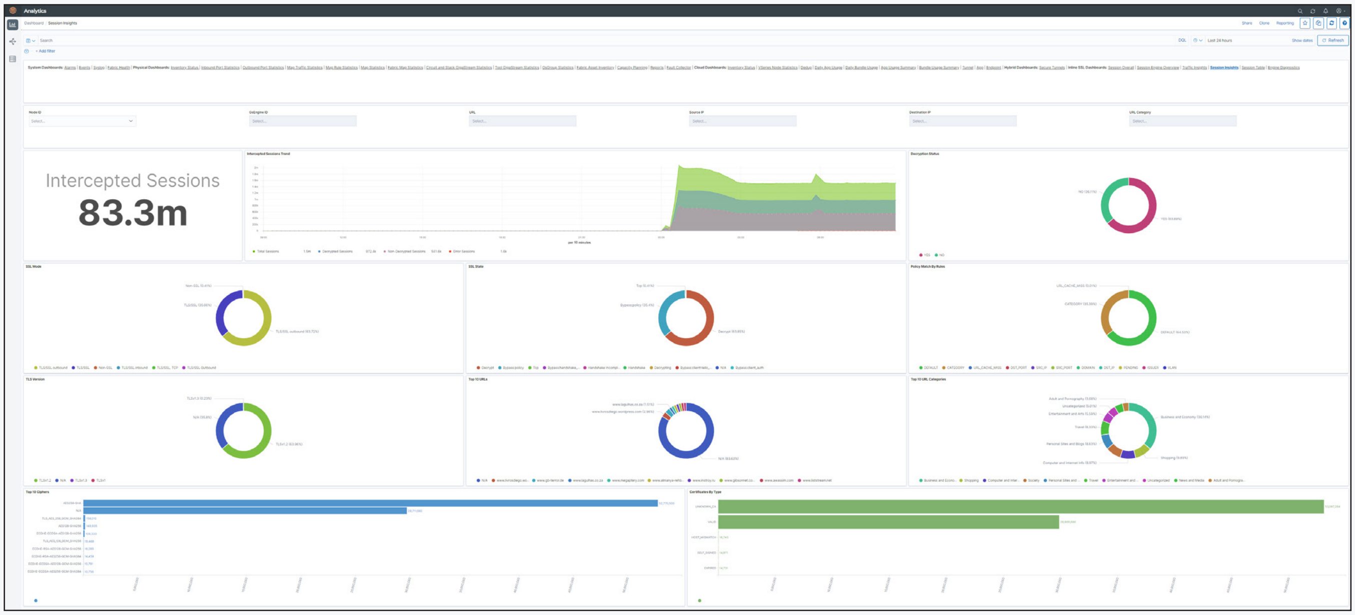

Figure 2. TLS/SSL Dashboard.

© 2025 Gigamon. All rights reserved.

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 TLS/SSL decryption 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.

In 2022, more than 85 percent of attacks took place in encrypted traffic, with 90 percent of those threats involving malware.[4]

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

Flex Inline and Decryption

Using flexible inline maps, you can identify specific flows of traffic using Layer 2 to Layer 4 rules, then designate the tools that will inspect the traffic, and specify the order of traffic to the tools.

It's easy to configure Flex Inline Decryption using GigaVUE-FM fabric manager with the flexible inline canvas.

Figure 3 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.

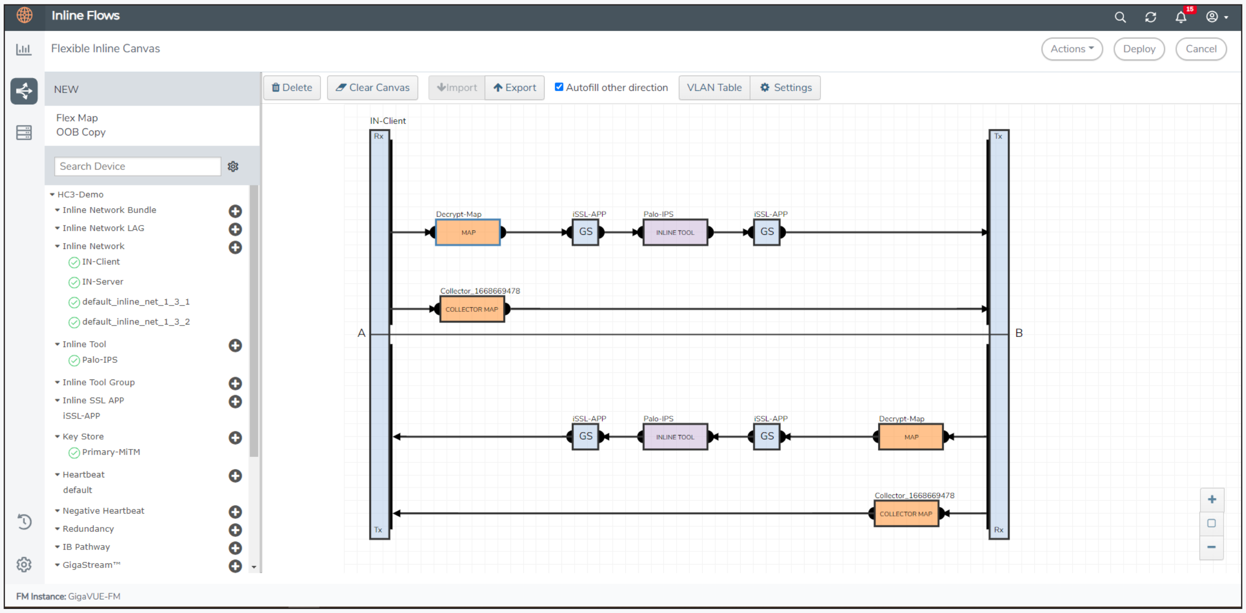

Figure 3. GigaVUE-FM Flex Inline and decryption.

© 2025 Gigamon. All rights reserved.

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	Base chassis plus optional GigaSMART module (SMT-HC1-S)	Base chassis plus optional GigaSMART module (SMT-HC1-S)	Gen3 GigaSMART engine (SMT-HC3-C08)
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, Thales Luna HSM)		
TPP (Trust Protection Platform) support	Yes (Venafi)		
IPv6 support (Passive and Inline TLS/SSL Decryption)	Yes		
Interfaces supported	10/100Mb, 1, 10, and 40Gbps	1, 10, 25, 40, and 100Gbps	10, 40, and 100Gbps
# of categories supported for selective decryption	86		
Physical inline bypass options	1 and 10Gbps	1 and 10Gbps	40 and 100Gbps
FIPS 140-2 certification	Level 2		
Split proxy function	Yes		
TLS/SSL Dashboard support	Yes[1]		

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

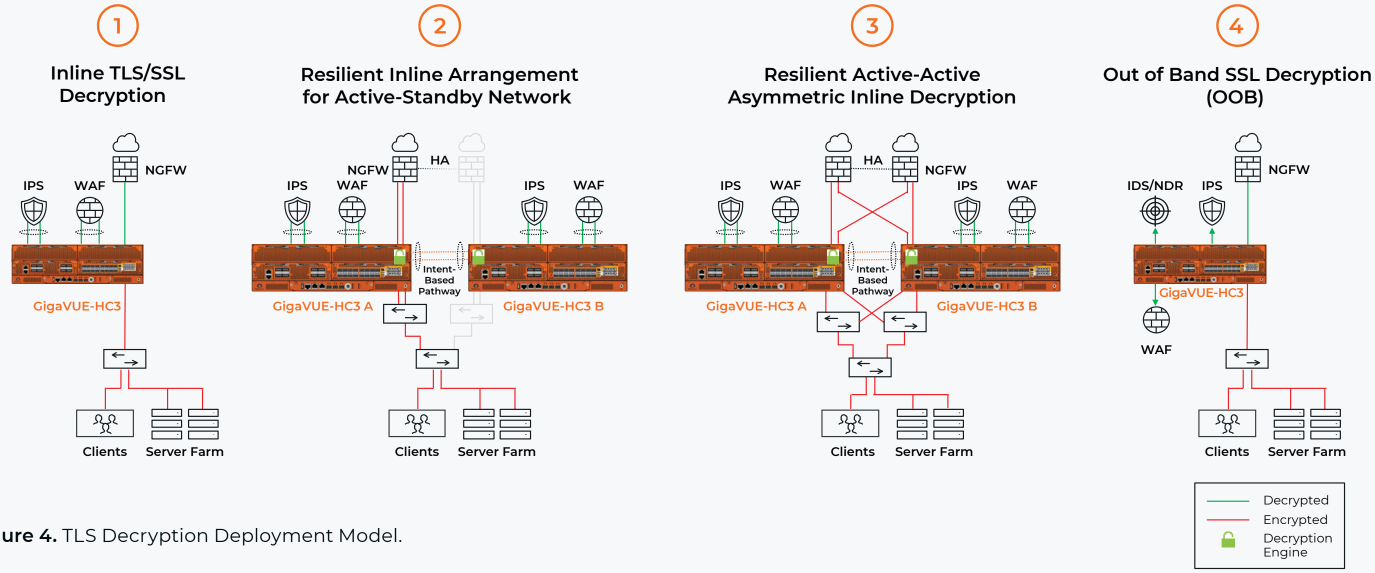

Figure 4. TLS Decryption Deployment Model.

© 2025 Gigamon. All rights reserved.

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	80,800	58	1,600,000
GigaVUE-HC1-Plus	22,090	15	400,000
GigaVUE-HC1	13,751	11	300,000

Out-of-Band

Model	Maximum Connections/Sec.	Maximum Throughput (Gbps)	Maximum Concurrent Connections
GigaVUE-HC3	432,000	315	8,000,000
GigaVUE-HC1-Plus	162,000	98	3,000,000
GigaVUE-HC1	65,000	45	3,000,000

Notes

- Tested with TLS_AES_256_GCM_SHA384 with ECDSA 256, and TLS_ECDSA_RSA_WITH_AES_256_GCM_SHA384 with RSA .
- Throughput based on 2MB file (inline) and 1MB file (out of band).
- Concurrent connections and connections/second based on 128B 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.

© 2025 Gigamon. All rights reserved.

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 efficiently delivers network-derived intelligence to your cloud, security, and observability tools, helping organizations eliminate security blind spots, reduce tool costs, and better secure and manage your hybrid cloud infrastructure. Gigamon goes beyond security and observability log-based approaches by extracting real-time network intelligence derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management. Gigamon has served 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. To learn more, please visit gigamon.com.

[1] For TLS/SSL advanced dashboards, minimum GigaVUE-FM requirements are Medium (ESXi-VM) or higher.

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

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

[4] 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

© 2019-2025 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.