NIAGARA NETWORKS

Application Note

Unleashing Network Intelligence through Packetron™ TLS Decryption

TLS Decryption Solutions

Many network security and monitoring applications lack visibility into encrypted traffic, preventing them from inspecting content and detecting threats hidden within it. Even tools that support TLS decryption often struggle to keep pace with the high demands of modern high-throughput environments. This results in dangerous gaps in corporate defenses, partial network visibility, and potential compliance issues.

Niagara Networks' TLS Decryption Solution enhances cybersecurity threat detection by offloading intensive decryption tasks from NetSecOps tools, improving overall performance and compliance processes. The solution can selectively filter traffic from specific points of interest, dynamically detect, and decrypt encrypted web content, emails, messaging, DNS, and files collected from multiple interfaces. This intelligent approach ensures that only the required traffic is decrypted and efficiently delivered to the appropriate security tools.

Our TLS Decryption Solution is an integral part of the Niagara Network Intelligence framework, seamlessly integrated into the Packetron acceleration module. It provides a modular, scalable system that allows enterprises to cost-effectively expand capacity and performance to meet evolving decryption and security requirements.

Niagara Networks' TLS Decryption Solution support three modules:

- Passive TAP
- Passive Inline[1]
- Active Inline

Inline Implementation[1]

With Inline or MiTM implementations, the TLS decryption application running in the Packetron acts as a proxy. This means two TLS sessions are established, versus a single TLS session when MiTM is not inserted. The Inline TLS Decryption Solution always needs to reside Inline with the network traffic stream. Establishing two TLS sessions means that traffic is decrypted in TLS session 1 (depicted in Figure 1 as "Client-to-MiTM" traffic) and reencrypting the same traffic in TLS session 2 (depicted in Figure 1, as "MiTM-to-Server" traffic). Through the decryption-reencryption process, visibility into the encrypted traffic is created for analysis by security tools.

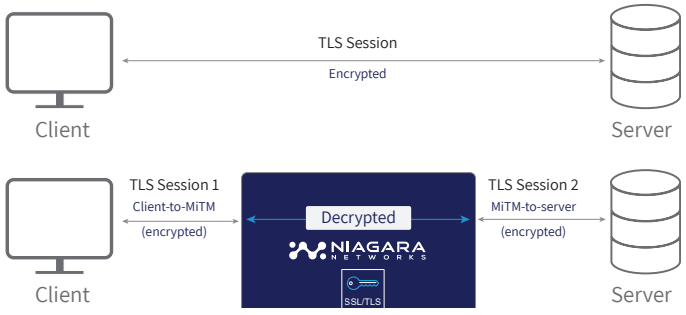

Figure 1: Niagara Inline TLS Decryption Solution (MiTM)

[1] *An active implementation uses a Man-in-The-Middle* approach (MiTM).

Throughout this brief, "MiTM" is used interchangeably with Niagara's active TLS Decryption Solution.

What's the difference between Passive Inline and Active Inline?

Passive Inline

The appliance (security tool) to which to send the decrypted traffic is deployed out-of-band (OOB) relative to the network stream.

Any actions or failures of the appliance will not affect the network traffic flow. The decryption-re-encryption cycle taking place in the inline TLS Decryption Solution is immediate.

Note: Examples of OOB appliances include Network Security Analyzers (NSA), Intrusion Detection Systems (IDS), SIEM collectors, forensic analysis platforms, data loss prevention (DLP) systems, application performance monitoring tools, and malware analysis solutions.

Active Inline

The appliance (security tool) to which we send the decrypted traffic is itself deployed Inline with the network traffic stream. Decrypted traffic is sent from the Inline TLS Decryption Solution[2] to the appliance (security tool) application, which is also deployed inline.

After traffic processing by the appliance (deployed inline security tool), the traffic is sent back to the Inline TLS Decryption Solution for re-encryption and is then sent to the network.

Note: Examples of Inline appliances are: Firewalls, Intrusion Prevention Systems (IPS), Denial of Service (DDoS), Web Application Firewall (WAF), and others.

Passive Inline (MiTM) is depicted in Figure 2. In the figure, decrypted client-to-server and decrypted server-to-client streams are depicted as two traffic streams to the out-of-band (OOB) tool for clarity. In an actual deployment, this is configurable by the user, and both traffic directions can be combined to a single traffic stream to the OOB tool.

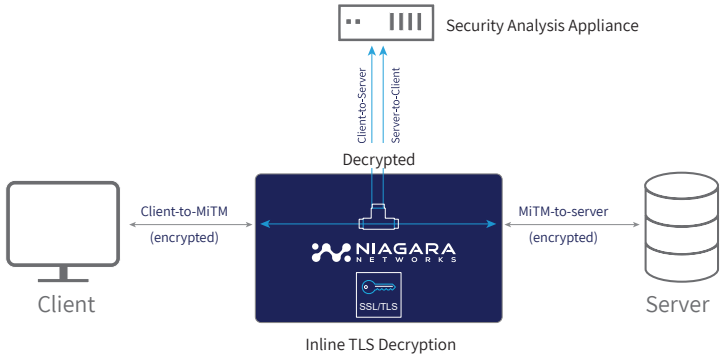

Figure 2: Passive Inline TLS Decryption (for OOB appliances)

Active Inline is depicted in Figure 3. In the forward path (traffic moving from client-to-server), the encrypted session client-to-MiTM is decrypted, and this decrypted session is sent to the security appliance which is deployed Inline. The forward path continues as the security appliance sends the traffic back to the Inline TLS Decryption application inside the Packetron after it completed its traffic processing (forward-appliance-MiTM). At this stage, the MiTM re-encrypts the traffic and sends it back to the network (MiTM-to-server). A reverse path is also depicted for the traffic from the server to the client.

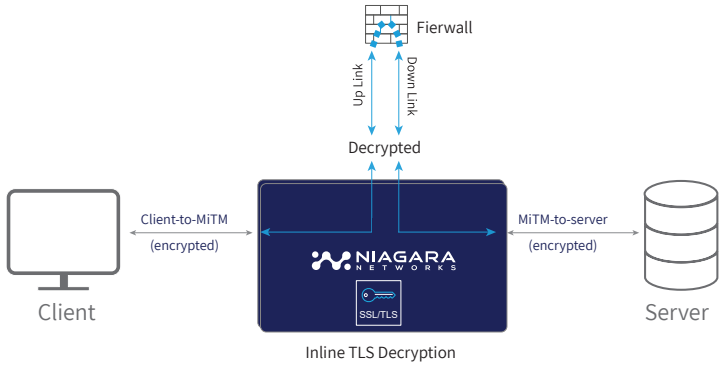

Figure 3: Active Inline TLS Decryption (for Inline security appliances)

[2] *An Inline implementation uses a Man-in-The-Middle approach (MiTM).*

Throughout this brief, "MiTM" is used interchangeably with Niagara's Inline TLS Decryption Solution.

TLS Decryption - Solution Composition

A comprehensive TLS Decryption Solution is composed of five core elements:

- The TLS Decryption core
  Responsible for terminating and re-establishing SSL/TLS sessions to decrypt and re-encrypt traffic while maintaining session integrity and compliance.
- Supporting TLS protocols and extensions
  Full compatibility with modern cipher suites, key exchange mechanisms, and TLS versions to ensure visibility across diverse encrypted traffic.
- Filtering of TLS sessions
  Intelligent filtering and policy-based traffic selection ensure that only relevant encrypted sessions are decrypted, reducing overhead and preserving privacy.
- Supported deployment scenarios
  Flexible operation in inline or out-of-band (OOB) modes to serve a wide range of security and monitoring tools without disrupting live traffic flow.
- Scalability - decryption powered by hardware acceleration to meet the demands of modern carrier-grade environments.

TLS Decryption Core

The Decryption Engine refers to the solution's ability to decrypt the different TLS protocol versions and to support the leading asymmetric key exchanges, the leading symmetric keys, and hash algorithms.

Table 1: TLS Decryption core functionality matrix

Feature	Active Inline	Passive Inline	Passive TAP
SSL/TLS Version	TLS1, TLS1.1, TLS1.2, TLS1.3	TLS1, TLS1.1, TLS1.2, TLS1.3	SSL3, TLS1.1, TLS1, TLS1.2
Asymmetric Key Exchange	RSA, ECDH, ECDHE	RSA, ECDH, ECDHE	RSA
Symmetric Keys	AES, 3DES	AES, 3DES	AES, 3DES, RC4
Hash algorithms	SHA1, SHA256, SHA384	SHA1, SHA256, SHA384	SHA1, SHA256, SHA384
Private Key Storage	Write only	Write only	Write only

Supporting TLS Protocols and Extensions

While TLS decryption is most well-known for browser traffic and HTTPS, many other protocols often make use of the TLS framework as well, such as e-mail protocols.

Table 2: TLS Decryption protocols and extensions feature matrix

Feature	Status	Feature	Status
TLS on any port (not limiting solution to port 443)	Supported	Online Certificate Status Protocol (OCSP) cache	Supported
SMTP, POP3, IMAP	Supported	Certificate Revocation Lists (CRL)	Supported
XMPP	Supported	STARTTLS	Supported
DoH, DoT	Supported	OCSP Staple	Supported
Online Certificate Status Protocol (OCSP)	Supported	Cipher Suite Integrity	Supported

Filtering of TLS Sessions

When decrypting TLS traffic, administrators often want to focus on certain types of traffic, or possibly send different decrypted traffic to different appliances. Filtering is supported on different TLS fields.

Table 3: TLS Decryption core functionality matrix

Feature	Status	Feature	Status
IP Address Source	Supported	Issuer State	Supported
IP Address Destination	Supported	Issuer Organization Unit	Supported
Destination Port	Supported	Subject Common Name	Supported
Server Name Indication (SNI)	Supported	Subject Organization Unit	Supported
Issuer Common Name	Supported	Subject Organization	Supported
Issuer Country	Supported	Subject Locality	Supported
Issuer Organization	Supported	Subject State	Supported
Issuer Locality	Supported	Subject Country	Supported

Supported Deployment Scenarios

TLS decryption must support two key deployment scenarios: Inbound and Outbound.

Inbound Deployment: When TLS traffic originates from the Internet and targets the customer's servers (providing web or application services). Decryption enables inspection for threats such as malware, exploits, and data exfiltration attempts targeting the organization's infrastructure.

Outbound Deployment: When TLS traffic originates from the organization's internal users and flows to the Internet. Decryption provides visibility into user activity, protects against phishing, malicious downloads, and data leaks, and ensures compliance with security policies.

Beyond these two primary scenarios, additional use cases include:

Lawful Interception: Supporting regulatory requirements for real-time monitoring and recording of encrypted communications in compliance with legal mandates.

Advanced Threat Detection: Enabling integration with malware sandboxes, DLP systems, and behavioral analytics tools that require decrypted traffic for deep inspection.

Forensics / Incident Response: Supplying decrypted traffic for investigation and root-cause analysis.cause analysis.

Figure 4: Inbound and Outbound deployment scenarios

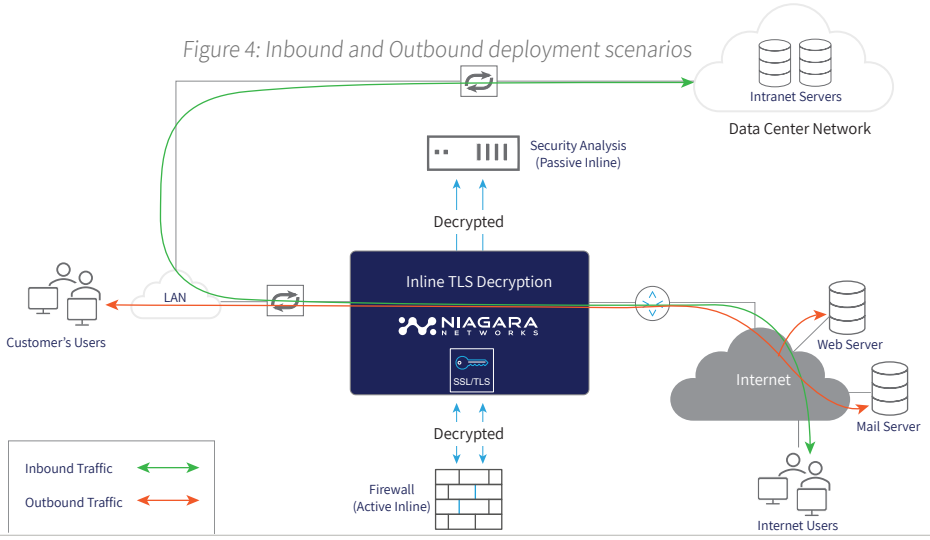

Table 4: Summarized Deployment Solutions	
Feature	Status
Multiple Topologies where each Topology represents a TLS network/segment	Supported
Active and Passive Inline on the same Topology	Supported
Multiple OOB appliances, each with different policies on the same Topology	Supported
Separating decrypted client-to-server and server-to-client traffic stream	Supported
Load Balancing decrypted traffic to multiple appliances	Supported
Replicating decrypted traffic to multiple appliances	Supported

Customers can scale their TLS by combining multiple Packetron modules in a single device

Summary

Niagara Networks' TLS Decryption Solution delivers a modular, scalable, and high-performance approach for visibility into encrypted traffic. It supports inbound and outbound deployment scenarios, enabling organizations to protect infrastructure, enforce security policies, comply with regulations, and address critical use cases such as lawful interception, advanced threat detection, and forensics.

To meet diverse deployment requirements, Niagara supports multiple integration options:

1. Active Inline mode for real-time decryption and re-encryption of traffic to inline security appliances.
2. Passive Inline mode, leveraging Active TAP functionality, for safely delivering decrypted traffic to out-of-band monitoring and analysis tools without impacting live traffic.

For environments requiring always-on availability, Niagara inline bypass protection can be deployed to guarantee uninterrupted traffic flow during failures or maintenance of the TLS decryption module or inline security tools, eliminating single points of failure and ensuring operational continuity.
Combined with Niagara's advanced packet broker capabilities, which deliver full network intelligence, this architecture goes beyond simple decryption—enabling traffic aggregation, filtering, deduplication, load balancing, and distribution of decrypted traffic to multiple inline and out-of-band tools. This creates a resilient, future-ready visibility fabric that scales to meet evolving security demands.

About Niagara Networks

Niagara Networks is a Silicon Valley-based company delivering high-performance, reliable network visibility and traffic delivery solutions for mission-critical environments. Our solutions empower Security and Network Operations Centers (SOC/NOC) with complete visibility and actionable intelligence across physical, virtual, and cloud networks. As a former division of Interface Masters, we provide all the building blocks for an advanced Visibility Layer, including packet brokers, bypass switches, network TAPs, and unified management software, offering a single pane of glass for simplified visibility infrastructure. For more information please visit us at www.niagaranetworks.com.

NIAGARA NETWORKS
48430 Lakeview Blvd,
Fremont, CA 94538, USA
www.niagaranetworks.com
info@niagaranetworks.com
Tel: +1 408 622 0354
Fax: +1 408 213 7529