NIAGARA NETWORKS

Application Note

Niagara's SSL/TLS Decryption Platform

With the vast majority of internet traffic now encrypted and increasing portions of network traffic also encrypted, networking and security teams need to better assess such traffic while still adhering to policies needed for compliance and regulatory requirements.

The Google Transparency Report from September 2020 shows that now 80-90% of internet traffic is encrypted.
*Studies show that upwards of 70% of network traffic is also encrypted. Decrypting certain traffic is critical to police security threats, meet other compliance requirements and properly assess and manage performance.

The reality is that encryption works both ways. It can certainly help hide your traffic from unauthorized users, but it can also help attackers hide their malware from your cybersecurity infrastructure. Gartner, Inc. predicts that during 2019, more than 50% of new malware campaigns will use various forms of encryption to conceal delivery, and to conceal ongoing communications, including data exfiltration.

To prevent cyber-attacks, data exfiltration and network exploits through Command & Control servers, enterprises need to inspect incoming and outgoing traffic for threats, subject to type of traffic and applicable policies. Today most email and SaaS application traffic is encrypted by default. In fact, most everything is encrypted by default.
Organizations that do not inspect encrypted communications are providing an open door for attackers to infiltrate defenses and for malicious insiders to steal sensitive data.
Internet security teams are in consensus that to defend enterprise networks and corporate information from threat actors they require full network visibility for security tools, such as, next-generation firewalls (NGFW), Data Loss Prevention (DLP), Intrusion Prevention Systems (IPS), and Unified Threat Management (UTM), as the proliferation of encryption has impeded the scrutiny they once had into enterprise network traffic. Solutions that deliver traffic to these security tools need to have the ability to perform decryption of data before delivery. Without SSL decryption built into your network visibility layer, attackers could take advantage of encrypted traffic to exploit blind spot vulnerabilities.

Secure Socket Layer (SSL) is the de facto standard for ensuring the security of traffic across the Internet. SSL and Transport Layer Security (TLS) have long been used to secure Internet-based transactions such as for e-commerce and online banking. (Note: Going forward the use or mention of "SSL" refers to both SSL and TLS).

The whole purpose of SSL/TLS encryption is to convert data packets into code that can only be decrypted by the intended recipient. Key algorithms ensure SSL and TLS maximize privacy without impacting performance.

*Sources: blogs.vmware.com, Network Computing Magazine

The Impact of TLS 1.3 on Network Visibility

Since the introduction of TLS 1.0 in 1999 and TLS 1.1 in 2006, both versions have shown several vulnerabilities to various attacks which led to the introduction of TLS 1.3. In March 2018, the Internet Engineering Task Force (IETF) approved the TLS 1.3 specification. This also led to the deprecation of TLS 1.0 and TLS 1.1 as of March 2020. While the new TLS version has a number of enhancements from a security standpoint, adoption of the new standard has generated concerns as TLS 1.3 requires the use of Perfect Forward Secrecy (PFS).

Without the use of PFS, an attacker may record encrypted traffic of users with a website which is protected by TLS. If after some elapsed time of such recording an attacker manages to steal the private key from the website's server, he would be able to decrypt all TLS connections that were previously recorded, as well as future communications. PFS has been designed to address this vulnerability.

With PFS, even if attackers retrieve the private key of a certificate, they are unable to decrypt communication from the past or future communications. When PFS keys are used, the session key is exclusively generated from both client and server information. The practical effect of PFS is that traffic captured in the past cannot be decrypted if someone is able to obtain the server key.

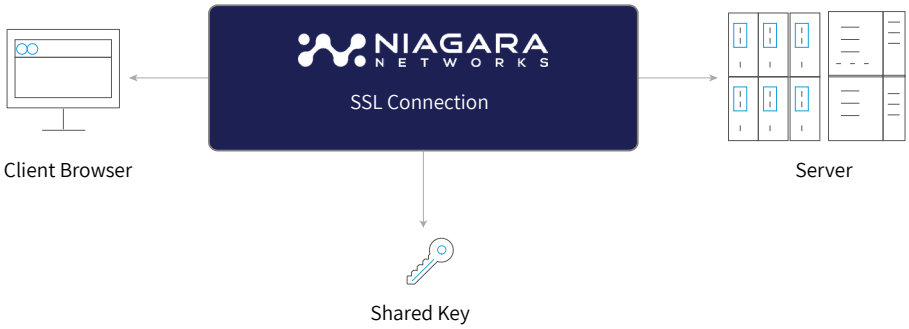
Choosing a SSL/TLS Decryption Deployment Option

The biggest challenge when deploying TLS/SSL decryption is finding the balance between performance and cost efficiency. Often it would appear that the easiest way to implement TLS decryption is to take advantage of next-gen firewalls (NGFWs) with this feature built in. Although this would technically provide TLS decryption, it's far from the optimal option. Activating TLS decryption often degrades NGFW performance significantly. Organizations need NGFWs to run at peak performance to carry out traditional firewall functionality, deep packet inspection, and intrusion prevention. When NGFWs are bogged down with TLS decryption demands, one sacrifices the performance of typical NGFW functions while also reducing TLS/SSL visibility. Rather than trying to force existing security and monitoring tools to carry out TLS decryption, the best approach to balancing performance and cost efficiency is to build this functionality into the network visibility layer.

SSL Decryption in Network Packet Broker (NPB)

By integrating SSL decryption capabilities into the NPB-enabled network visibility layer, it's possible to meet the aforementioned ROI requirements as well as the TLS1.3 challenges. Integrating SSL decryption capabilities through deploying optimized traffic acceleration hardware modules within an NPB is effortless and simpler than the other options and it carries no performance impact for SSL decryption on other NPB functions.

In addition, the NPB is designed to forward traffic requiring inspection to the range of in-place security tools. This means that the NPB can provide a centralized SSL decryption function for network security tools out-of-the-box. The NPB can also maintain the isolation of clear-text traffic, while delivering highly resilient security processing with load-balancing of tools and fail-open behavior.



With PFS, unique session keys are generated using both client and server information. The challenge that PFS presents is that PFS handshakes are incompatible with the decryption capabilities in network monitoring tools which analyze network traffic.

Deploying SSL Decryption with an Intelligent Visibility Layer

Not all NPBs come outfitted with TLS/SSL decryption capabilities. Using the Niagara Networks Packetron module hosted on the N2 series modular packet broker and other fixed modules one can decrypt SSL/TLS streams while fully supporting Perfect Forward Secrecy sessions.

To enable IT teams with optimized SSL decryption deployments and flexible mode of operation, Niagara Networks' solution supports different deployment configurations.

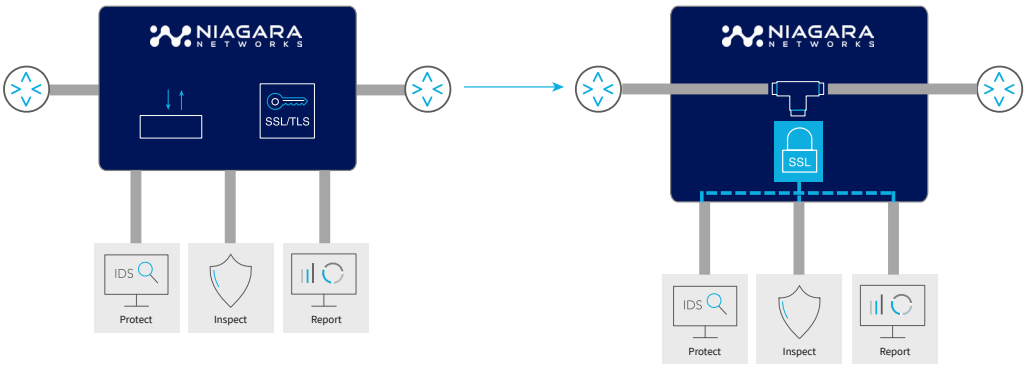
- Passive out-of-band decryption
- Active out-of-band
- Active inline decryption

Passive out-of-band decryption

The passive out-of-band decryption scenario enables decryption outside of the data path. As such there is no performance impact in the traffic path. A copy of the traffic is forwarded to the decryption engine. After decryption, the decrypted traffic can be forwarded to multiple reporting and inspection tools.
This deployment scenario is available for all cypher suites with static (Non PFS) keys.

The Packetron difference is all about building your path to an intelligence visibility layer. This packet acceleration module empowers cutting edge features:

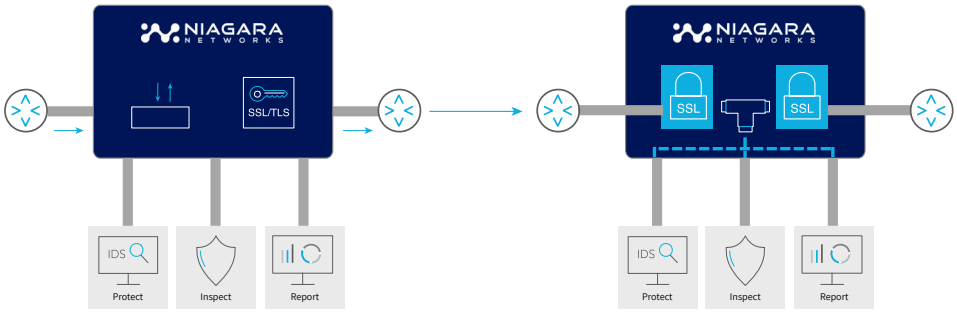
- SSL/TLS decryption support for SSL 3.0, and all TLS versions including TLS 1.3
- Scalable performance with up to 320Gbps processing for different applications, per visibility node
- De-coupled software architecture to make changes without impacting the host NPB
- Intuitive configuration that gives you control over packet flows to support inline and out-of-band tools
- Advanced packet intelligence capabilities to maximize the efficiency of network security and monitoring tools



Passive out-of-band

Active out-of-band decryption

While the Passive out-of-band method with its absence of any performance impact on the data path is suited for many inspection and reporting deployments, its disadvantage is the inability to support a PFS enabled encryption method.
To provide full decryption support for all cypher suites with optimized inline performance, the Active out-of-band decryption scenario can be used.
Opposite to Passive out-of-band, the decryption engine is placed inline with the traffic. However, since the encryption engine is part of a packet broker, pre-filtering can be applied to the traffic assuring that encrypted traffic is sent to the engine only.

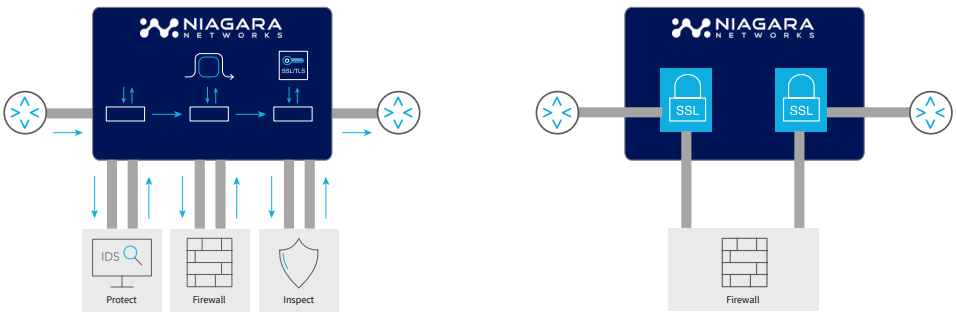


Active out-of-band

The received traffic is decrypted, and a copy of the decrypted traffic is sent to the inspection and reporting tools. After copying, the traffic is immediately re-encrypted and forwarded for further processing.

Active Inline decryption

Both aforementioned decryption methods are specifically suited for reporting and out-of-band inspection purposes.
Often a more elaborate inline inspection of the traffic is required by using next-generation firewalls (NGFW), intrusion prevention systems (IPS) or Unified Threat Management solutions (UTM).
The Active Inline decryption method is especially suited for these deployment scenarios.

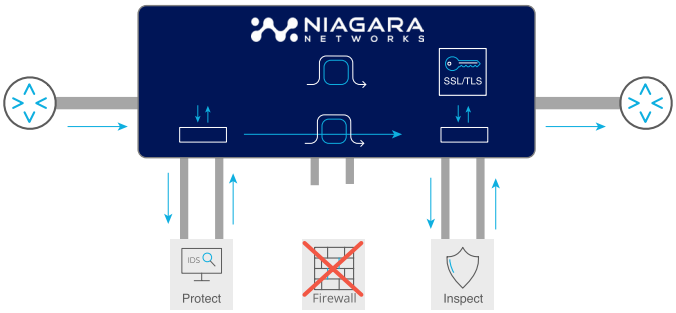


Active Inline

With Active-Inline decryption the received traffic is, after optional pre-filtering, sent to the decryption engine. After decryption, the traffic is forwarded to the inline appliance. The packet brokers service chaining capabilities enables cascading of multiple inline security appliances, all receiving the decrypted traffic. If one of the protections appliances in the chain would unexpectedly fail, the packet broker bypasses the failed appliance thereby restoring the security chain.

After the inspected traffic is returned from the (last) protection appliance, the traffic is re-encrypted and forwarded for further processing. Both, Passive Inline and Active Inline decryption use a technique known as Man-in-the-Middle. The decryption/encryption engine pretends to be the addressed server for the client and acts as a client towards the server.

Decrypted traffic can potentially be seen by anyone with access to network monitoring tools. This is particularly problematic for monitoring data stored in DLPs, logs, and other databases, as it often violates regulatory compliance mandates. Once again, NPBs can help, by masking data that doesn't need to be exposed. In short, SSL-enabled NPBs can decrypt network data, aggregate it and filter it, apply data masking as needed and only then distribute it to the proper security and monitoring tools for analysis.



Summary

SSL/TLS decryption is part of Niagara Networks Open Visibility Platform architecture with foundation around the Packetron process acceleration module and the N2 series Bypass and Packet Broker appliance, providing advanced visibility intelligence functionality such as SSL/TLS decryption, Deduplication, Data masking, Application Filtering, RegEx, Mobile Subscriber-aware GTP tunnel handling and many more.

The Open Visibility Platform's visibility virtualization enables hosting of third-party applications which can be deployed reliably inline or out-of-band.

For more information on our Technology Alliance Program, please follow our web page.

The Value of SSL/TLS Decryption for Intelligent Visibility

- Deep visibility into encrypted data traffic
- Powerful combination of decryption platform and the on-board resident 3rd party security & network applications, delivering a cyber threat detection multiplier
- Seamless support for network tap, or inline bypass deployments on the same platform
- Encrypted traffic can be collected from multiple interfaces - from 1GbE up to 100GbE
- Decrypted traffic packet brokering to multiple tools based on policy rules – decrypt once, use many and various intelligent packet manipulations (masking, filtering, steering and more)
- Off load/minimize performance hit for individual tools

About Niagara Networks

Niagara Networks provides high performance network visibility solutions for seamless administration of security solutions, performance management and network monitoring. Niagara Networks products provide advantages in terms of network operation expenses, downtime, and total cost of ownership. A former division of Interface Masters, Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including network TAPs, bypass elements, packet brokers and a unified management layer.
For more informationplease visit us at www.niagaranetworks.com

NIAGARA NETWORKS
150 E Brokaw Road
San Jose, CA 95112, USA
www.niagaranetworks.com
info@niagaranetworks.com
Tel: +1 408 622 0354
Fax: +1 408 213 7529