Niagara's SSL/TLS Decryption Platform

Niagara Networks SSL/TLS decryption offering is an important foundation of the security visibility layer. Without SSL/TLS Decryption your organization is blind to attacks, malware and other security and cyber threats impacting your network via the TLS layer. Organizations need a way to identify threats and malware in order to protect their users and intellectual property. While SSL/TLS encrypted traffic protects by ensuring the identity of the server, it does not protect from malicious content being sent to the mission-critical applications being served.

What is SSL Encryption

SSL Encryption - and its successor TLS - make the internet safe and protects the privacy of individuals and corporations. Without it, we would find ourselves exposed to fraud while conducting our online transactions such as online banking, e-commerce, finances, and electronic medical records. SSL/TLS is not limited to web traffic, but it is also widely used for DNS, voice over IP, VPN and e-mail traffic. It is so pervasive in our daily life, with 89% SSL / HTTPS Web Traffic utilization in the USA[1].

Challenge

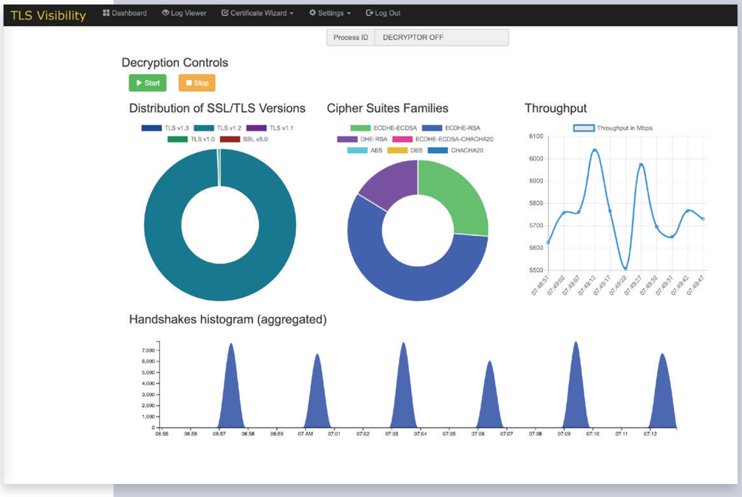
Many network security and monitoring applications do not have visibility to encrypted traffic and cannot inspect the content of encrypted traffic. This creates dangerous gaps in corporate defenses or results in partial management and visibility of the network.

The few security and monitoring application that have embedded TLS decryption technology are not able to keep pace with the high demands of a high throughput environment. Moreover, TLS decryption is demanding in computational resources, that will divert resources from the application's intended primary purpose. This may reduce the security tool throughput to a fraction of its performance without TLS decryption.

Additionally, security deployments typically use multiple appliances and applications to cover different aspects of cyber security. Often they process, inline or out-of-band, the same traffic flows. Having each tool perform its own TLS decryption independently, introduces significant performance and efficiency degradations throughout the deployment.

Product Highlights

- Supports multiple SSL/TLS versions:
  SSLv3, TLS1, TLS1.1, TLS1.2, TLS1.3, DTLS1
- Dynamically detect SSL/TLS session in the traffic stream
- Supports multiple encrypted protocols:
  HTTPS, SMTPS, POP3S, IMAPS, XMAPPS, DNS
- Support multiple deployment scenarios:
  - Passive out-of-band
  - Active out-of-band
  - Active inline
- Dashboard providing realtime insight into the SSL/TLS traffic
- Integrated network packet broker functionality
  - Resides inside the N2 modular multipurpose visibility node
  - 1GbE-100GbE interfaces
- Powered by Packetron modular modules
  - Scale performance
  - Adding multiple Packetron modular modules
  - Open architecture



Process ID DECRYPTOR OFF

Figure 1 - real time dashboard for insights on encrypted traffic processed by Niagara's SSL/TLS Decryption Platform

[1] Google Transparency Report February 2019

Extending the Visibility Layer - Security Visibility Layer

Niagara's SSL/TLS decryption platform supports multiple version of SSL and TLS, including the latest TLS1.3. SSL/TLS flows are dynamically detected from the traffic flow, and detection is not just limited to standard ports such as 443. Moreover, some of the important threat methods of penetration are not limited to HTTP, and in our platform we extend our protocol support to messaging, e-mails, DNS and more.

Users can gain real-time insights from SSL/TLS traffic. As part of the SSL/TLS engine, an application dashboard provides real time statistic on the SSL/TLS traffic.

Niagara’s SSL/TLS decryption platform resides inside the N2 series modular multipurpose visibility node. This offers integrated enhanced flexibility in optimizing the SSL/TLS decryption:

- Encrypted traffic can be collected from multiple interfaces ranging from 1GbE up to 100GbE, whether copper or fiber interfaces.
- Receive aggregated traffic from multiple sources, optimizing use of computational resources.
- Efficiently forwarded decrypted traffic to the right security or monitoring appliance. Decrypted traffic can be replicated to multiple security tools or load balanced between security tools for improved redundancy of the security services and lower cost of deployment.
- Seamless support for network tap, or inline bypass deployments. When deployed inline, the SSL/TLS decryption platform benefits from Niagara's double-protection bypass technology. A failsafe optical/copper relay on network ports, and user-configurable heartbeat-generated packets on appliance ports.

NPB Packetron Power Multiplier

Niagara's SSL/TLS decryption leverages the flexibility and performance of the Packetron module[1]. Multiple Packetron modules can be deployed in the N2 series modular multipurpose visibility node.

The SSL/TLS decryption platform can scale up by introducing additional modules. Furthermore encrypted traffic can be load balanced between the different Packetron modules.

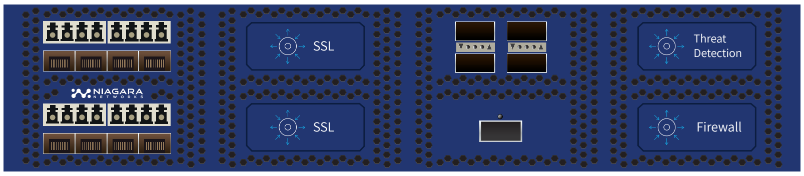


Figure 2 - depicts schematic deployment of Niagara's open architecture. Security application can be deployed on Packetron modules as part of the SSL/TLS decryption platform. This powerful combination enhances the efficiency of both the decryption platform and the on-board resident security application, delivering a cyber threat detection multiplier

With Niagara's open architecture security application can be deployed on Packetron modules as part of the SSL/TLS decryption platform. This enhances the efficiency of both the decryption platform and the ‘resident’ security application ushering a cyber threat detection multiplier to the deployment.

[2] See Niagara Packetron Data Sheet

Niagara's SSL/TLS decryption platform supports three deployment modes:

Passive out of band - the SSL/TLS decryption platform receives a copy of the encrypted traffic. The decrypted traffic can be forwarded to an an out of band tool. The decryption process has not impact of the network traffic. This mode is only available with certain TLS version and cipher suites

Active out of band - the SSL/TLS decryption platform sits inline, receiving the encrypted traffic. The encrypted traffic is decrypted and re-encrypted back to the network. A copy of the decrypted traffic can be forwarded to an out of band appliance. The actions out of band appliance itself have no impact on the network traffic.

Active inline - the SSL/TLS decryption platform sits inline, receiving the encrypted traffic. The encrypted traffic is decrypted, and the decrypted traffic may be forwarded to an inline appliance. Decrypted traffic from the inline appliance is received back at the SSL/TLS decryption platform and is re-encrypted on to the network.

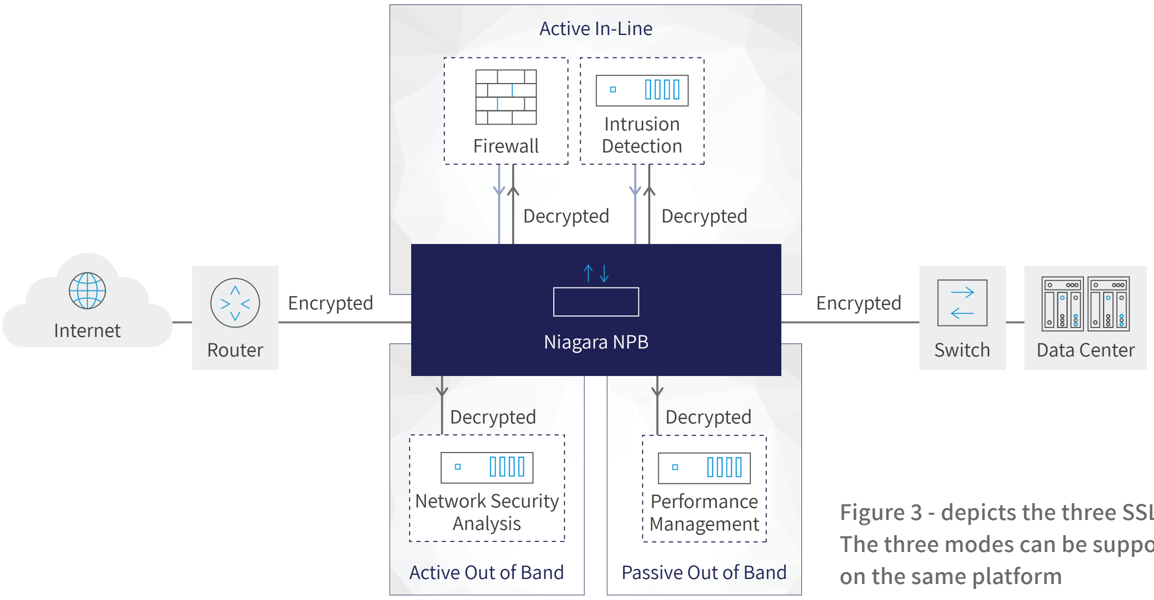


Figure 3 - depicts the three SSL/TLS deployments. The three modes can be supported simultaneously on the same platform

NIAGARA NETWORKS

About Niagara

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 Taps, bypass elements, packet brokers and a unified management layer. Thanks to its integrated in-house capabilities and tailor-made development cycle, Niagara Networks are agile in responding to market trends and in meeting the customized needs of service providers, enterprise, data centers, and government agencies.

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