Solution Brief

SSL Insight with Niagara Networks External Bypass

Uncover Hidden Threats in SSL/TLS Traffic While Maximizing Network Uptime

A10 Networks and Niagara Networks have partnered to detect and stop malicious attacks hidden in encrypted traffic, while maintaining high availability. A10 Networks Thunder® SSLi® intercepts and decrypts SSL/TLS traffic and sends the decrypted traffic to third-party security devices for analysis. In the event of a software or hardware failure, the Niagara Networks External Bypass Switch routes network traffic around the Thunder SSLi appliance, ensuring continuous application access.

The joint A10 Networks and Niagara Networks solution offers a cost-effective way to deliver high availability without needing to deploy a second, passive Thunder SSLi appliance. Together, A10 Networks and Niagara Networks ensure a safe and secure experience to users without network downtime.

The Challenge

layers of defense to mitigate these threats. An increasing number of applications use SSL/TLS to encrypt communications. Today, many of the world's most popular websites encrypt every web request and response.

Unfortunately, many legacy security devices cannot inspect encrypted traffic, and the few that can decrypt traffic cannot keep pace with growing SSL/TLS bandwidth and processing demands, exposing dangerous gaps in corporate defenses. As a result, organizations may suffer attacks, intrusions and data loss because attackers can easily bypass security controls.

Challenge

Many legacy security devices cannot inspect encrypted traffic, and the modern versions that can decrypt traffic, are creating dangerous gaps in corporate defenses.

Solution

A10 Networks and Niagara Networks provide organizations full visibility into SSL/TLS traffic without introducing a single point of failure.

Benefits

- Eliminate the blind spot in corporate defenses by decrypting SSL/TLS traffic at high speeds
- Prevent costly data breaches and loss of intellectual property by detecting advanced threats
- Scale security capacity by load balancing multiple third-party security appliances
- Ensure network availability during maintenance windows, power outages or device failures

In addition, all inline appliances present a single point of failure, which could potentially cause network downtime. This downtime can be caused by power failures, software crashes, link loss or a planned maintenance window.

In addition, all inline appliances present a single point of failure, which could potentially cause network downtime. This downtime can be caused by power failures, software crashes, link loss or a planned maintenance window.

The A10 Networks – Niagara Networks Joint Solution

Together, A10 Networks and Niagara Networks provide a scalable solution that eliminates the blind spot in corporate defenses without introducing a single point of failure to the network. Thunder SSLi with A10 Networks SSL Insight® technology intercepts SSL/TLS traffic and sends it unencrypted to third-party security tools.

The Niagara Networks External Bypass Switch connects to the ingress and egress ports of the Thunder SSLi appliance to identify failures and ensure network uptime and availability. The External Bypass Switch preemptively detects Thunder SSLi maintenance windows or downtime and provides fail-to-wire protection—connecting the two sides of the network link together to ensure that traffic continues to flow when downtime occurs. Thunder SSLi then encrypts decrypted traffic and sends it through the Niagara Networks External Bypass Switch to the intended destination.

Using Thunder SSLi with the External Bypass Switch, organizations can transparently decrypt traffic and forward it to security tools such as firewalls, intrusion prevention systems (IPS), data loss prevention (DLP) tools, network forensics, advanced threat protection (ATP) platforms and other security devices—without reducing or compromising the reliability or uptime of the network.

By connecting a Niagara Networks External Bypass Switch to A10 Thunder SSLi, the single point of failure is effectively eliminated, ensuring consistent and complete network uptime. Niagara Networks' bypass solutions make sure that the network always stays intact without deploying redundant Thunder SSLi appliances.

The Niagara Networks External Bypass Switches can be easily configured to work with Thunder SSLi appliances, with zero configuration required on the External Bypass Switch. If a network failure occurs due to a planned or an unexpected outage, the Niagara Networks External Bypass Switch will detect this and reroute all network traffic to bypass Thunder SSLi, keeping the traffic intact and flowing on the network.

Niagara Networks External Bypass Switch

The Niagara Networks External Bypass Switch consists of two bypass technologies:

- **Active Bypass:** The Niagara Networks External Bypass Switch can use an intelligent "active" mechanism that senses the health of the Thunder SSLi appliance by sending a configurable, unidirectional or bidirectional heartbeat. If the heartbeat is lost, the system automatically reroutes the traffic around Thunder SSLi until the device has recovered. The intelligent, active bypass mode preserves the link and the transition is made seamlessly.
- **Passive Bypass:** The second, passive bypass mode monitors the Thunder SSLi power supply. Upon detection of a power outage, the system fails open, making sure that network connectivity stays intact.

In order to ensure proper system operation during inline mode, a Niagara Networks External Bypass Switch will send out Ethernet frames called heartbeats in order to verify appliance health. The high-resolution heartbeat is configurable and will be sent from the External Bypass Switch to one port of the Thunder SSLi appliance and is expected to be received from a second port.

A10 Thunder SSLi

The A10 Thunder SSLi product line is an industry-leading, high-performance SSL/TLS decryption solution. With its SSL Insight technology, Thunder SSLi decrypts SSL/TLS traffic and sends the decrypted traffic to inline or passive, non-inline security solutions for inspection. It then encrypts the traffic again and forwards it to the intended destination. SSL Insight technology enables organizations to protect users and data without degrading the performance of their security infrastructure.

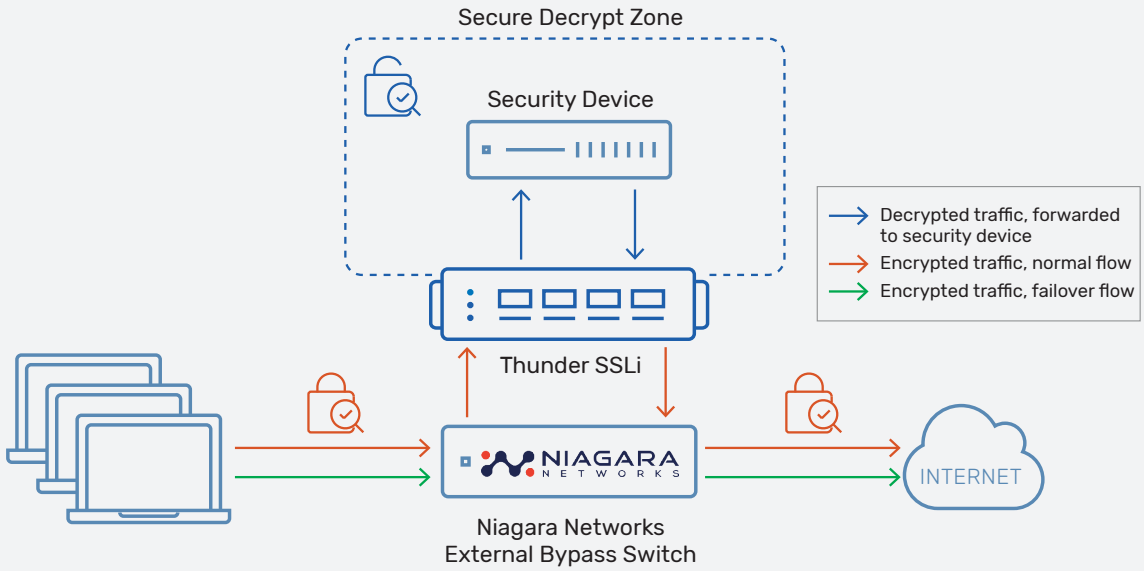

Figure 1: A10 Networks and Niagara Networks joint security solution

Features and Benefits

- The joint solution prevents costly data breaches and loss of intellectual property by detecting and mitigating advanced threats.
- Thunder SSLi eliminates the SSL/TLS blind spot in corporate defenses by intercepting and decrypting traffic at high speeds.
- Thunder SSLi scales security capacity by load balancing multiple third-party security appliances, and ensures network availability during maintenance windows, power outages or device failures.
- The Niagara Networks External Bypass Switch routes network traffic around the Thunder SSLi appliance, ensuring continuous application access.

Solution Components

The A10 Networks and Niagara Networks combined solution consists of:

- A10 Networks Thunder SSLi line of high-performance SSL/TLS decryption appliances
- The Niagara Networks External Bypass Switch, which is available in many different models to accommodate various types of networks.

Summary – Uncover Hidden Threats While Maximizing Network Uptime

Thunder SSLi integrates and works with the network uptime, fail-safe operation and high availability provided by Niagara Networks External Active Bypass Switch to offer organizations a powerful SSL/TLS decryption solution – one that can ensure network continuity and uptime in any situation. Using A10 Thunder SSLi in conjunction with the Niagara Networks External Bypass Switch, organizations can:

- Analyze all network data, including encrypted data, for complete threat protection
- Deploy best-of-breed content inspection solutions to fend off cyber attacks
- Maximize network uptime and continuity by detecting power outages, link loss, software crashes or other typical outages
- Avoid a single point of failure in the network without needing to purchase or deploy multiple A10 Thunder SSLi appliances

Together, A10 Networks and Niagara Networks deliver a high-performance, cost-effective solution for SSL/TLS inspection, enabling organizations to eliminate the SSL/TLS blind spot in their corporate defenses.

Next Steps

To learn more about this joint solution, please contact your A10 Networks representative for more information.

About Niagara Networks

Niagara Networks™ is a Silicon Valley based company that pioneer the Open Visibility Platform™ to bring desperately needed agility to network security. Niagara Networks provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

As 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 advanced packet brokers, bypass switches, network TAPs and a unified management and orchestration software that serves as a single-pane of glass to ease configuration and provisioning of the visibility infrastructure. manufactured in San Jose, CA.
For more information, visit: www.niagaranetworks.com

About A10 Networks

A10 Networks (NYSE: ATEN) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

Learn More

About A10 Networks

Contact Us
a10networks.com/contact

Part Number: A10-SB-19150-EN-03 JUNE 2020