SSL INSIGHT WITH EXTERNAL BYPASS

Uncover Hidden Threats in SSL Traffic While Maximizing Network Uptime

Challenge:

Many network security devices cannot inspect encrypted traffic, and the few that can decrypt traffic, creating dangerous gaps in corporate defenses.

Solution:

A10 Networks and Niagara Networks provide organizations full visibility into SSL traffic without introducing a single point of failure. Using A10 Thunder ADC with the Niagara External Bypass Switch, organizations can transparently decrypt traffic and forward it to security tools.

Benefits:

- Eliminate the blind spot in corporate defenses by decrypting SSL 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

A10 Networks® and Niagara Networks have partnered to detect and stop malicious attacks hidden in encrypted traffic, while maintaining high availability. A10 Networks Thunder® ADC line of Application Delivery Controllers intercepts and decrypts SSL traffic and sends the unencrypted 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 ADC appliance, ensuring continuous application access.

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

The Challenge

As threats continually evolve, organizations often deploy multiple layers of defense to mitigate these threats. An increasing number of applications use SSL – or its successor TLS – to encrypt communications. Today, many of the world's most popular websites encrypt every web request and response. And by 2016, two-thirds of North American Internet traffic is expected to be encrypted.

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

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 ADC with A10 Networks SSL Insight™ technology intercepts SSL traffic and sends it unencrypted to third-party security tools.

The Niagara External Bypass Switch connects to the ingress and egress ports of the Thunder ADC appliance to identify failures and ensure network uptime and availability. The External Bypass Switch preemptively detects Thunder ADC 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 ADC then encrypts decrypted traffic and sends it through the Niagara External Bypass Switch to the intended destination.

Using Thunder ADC 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 External Bypass Switch to A10 Thunder ADC, the single point of failure is effectively eliminated, ensuring consistent and complete network uptime. Niagara Networks' bypass solutions make sure that the network stays intact at all times without deploying redundant Thunder ADC appliances.

The Niagara External Bypass Switches can be easily configured to work with Thunder ADC 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 External Bypass Switch will detect this and reroute all network traffic to bypass Thunder ADC, keeping the traffic intact and flowing on the network.

Niagara External Bypass Switch

The Niagara External Bypass Switch consists of two bypass technologies:

- **Active Bypass:** The Niagara External Bypass Switch can use an intelligent "active" mechanism that senses the health of the Thunder ADC appliance by sending a configurable, unidirectional or bidirectional heartbeat. If the heartbeat is lost, the system automatically reroutes the traffic around Thunder ADC 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 ADC 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 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 ADC appliance and is expected to be received from a second port.

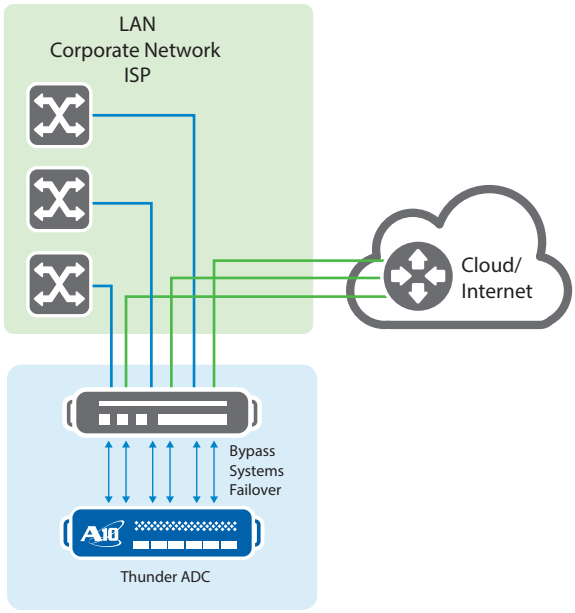

Figure 1: A10 Networks and Interface Masters joint security solution

A10 Thunder ADC with SSL Insight Technology

The A10 Thunder ADC product line is an industry-leading, high-performance family of application delivery controllers. With its integrated SSL Insight technology, Thunder ADC decrypts SSL 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.

Thunder ADC functions as a transparent SSL proxy in order to intercept SSL traffic. From both the client's and the server's point of view, there still is an end-to-end encrypted session that is only decrypted within the client's network, in a contained environment. With SSL acceleration hardware, Thunder ADC delivers near parity performance between 1024-bit and 2048-bit key sizes and has the extreme power needed to handle 4096-bit keys at high-performance production levels.

Features and Benefits

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

Solution Components

The A10 Networks solution consists of:

- A10 Networks Thunder ADC line of Application Delivery Controllers
- A10 Networks SSL Insight

The Niagara External Bypass Switch is available in many different models to accommodate various types of networks. The following is a list of available configurations:

- 1 to 4 segments (each segment contains two network ports and two appliance ports)
- 1 Gigabit SX/LX/Copper
- 10 Gigabit SR/LR/ER
- 40 Gigabit SR/LR/ER
- 100 Gigabit

Summary

As a standard feature of A10 Thunder ADC, SSL Insight 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 decryption, load balancing and high availability solution – one that can ensure network continuity and uptime in any situation. Using A10 Thunder ADC in conjunction with the Niagara 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 ADC appliances

Together, A10 Networks and Niagara Networks deliver a high-performance, cost-effective solution for SSL inspection, enabling organizations to eliminate the SSL 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 leader in the network monitoring and visibility market providing Network Bypass, TAP and Network Packet Broker solutions. Niagara Networks' expertise lies in Gigabit, 10GbE, 40GbE and 100GbE network visibility solutions that integrate with inline and out-of-band security and monitoring tools, including IPS, UTM, load balancing, and WAN acceleration. Flagship product lines include Deep Packet Inspection Systems, Packet Brokers, external intelligent Network TAP, Bypass and failover systems. Company Headquarters are located in San Jose, CA with satellite offices in Hong Kong and Europe. For more information, visit: www.niagaranetworks.com

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-SB-19150-EN-01
Sep 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
HongKong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at **www.a10networks.com/contact** or call to talk to an A10 sales representative.