



SSL INSIGHT WITH INTERFACE MASTERS EXTERNAL BYPASS

UNCOVER HIDDEN THREATS IN SSL/TLS TRAFFIC WHILE
MAXIMIZING NETWORK UPTIME

A10 Networks and Interface Masters 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 Interface Masters Niagara External Bypass Switch routes network traffic around the Thunder SSLi appliance, ensuring continuous application access.

The joint A10 and Interface Masters solution offers a cost-effective way to deliver high availability without needing to deploy a second, passive Thunder SSLi appliance. Together, A10 and Interface Masters 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/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 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 Interface Masters 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

Interface Masters

TECHNOLOGIES

Innovative Network Solutions

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 – INTERFACE MASTERS JOINT SOLUTION

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

The Niagara 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 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 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 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 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.

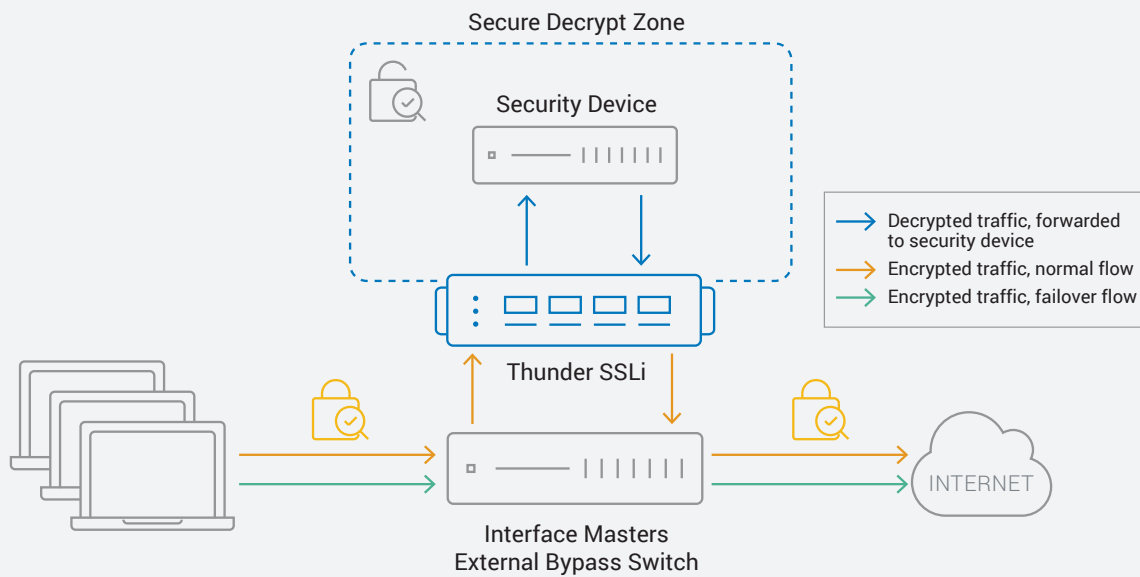


Figure 1: A10 Networks and Interface Masters joint security solution

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.
- Interface Masters Niagara External Bypass Switch routes network traffic around the Thunder SSLi appliance, ensuring continuous application access.

SOLUTION COMPONENTS

The A10 Networks and Interface Masters combined solution consists of:

- A10 Networks Thunder SSLi line of high-performance SSL/TLS decryption appliances
- The Niagara 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 Interface Masters Niagara 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 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 Interface Masters 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 INTERFACE MASTERS

Interface Masters Technologies is a leading provider of Switches, Smart NICS and full custom appliances focused on Gigabit, 10 Gigabit, 40 Gigabit and 100 Gigabit Ethernet. For over 20 years, Interface Masters has been providing innovative networking solutions with customization services. Interface Masters is an OCP member and has contributed multiple white box designs to the project while supporting

customer SDN development. Interface Masters OCP switches can be modified according to customer requirements and are provided with complete SDK and source code required to support software development. All products are designed and manufactured in San Jose, CA. For more information, visit: www.interfacemasters.com

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet [@a10Networks](https://twitter.com/a10Networks)

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

©2019 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, A10 Lightning, A10 Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-SB-19150-EN-02 MAY 2019