SOLUTION BRIEF

SSL INSIGHT FOR CISCO FIREPOWER AND CISCO ASA

UNCOVER CYBER ATTACKS HIDDEN IN SSL TRAFFIC

A10 Networks® and Cisco are collaborating to detect and stop malicious attacks hidden in encrypted traffic, without compromising on performance. A10 Thunder® SSL Insight® (SSLi®) intercepts SSL traffic and sends it unencrypted to Cisco FirePOWER or Cisco ASA so that threats can be detected and blocked. This gives businesses complete visibility into network activity, including encrypted traffic, so that they can uncover attacks and infiltrations; defend computers, mobile devices and virtual environments from malware; and deliver a safe and secure experience to their users.

CHALLENGE

ENCRYPTION CREATES A BLIND SPOT IN DEFENSES

Security and privacy concerns are driving the adoption of SSL encryption. Just a few years ago, most web applications would only encrypt sensitive communications such as credit card transactions and user logins. Today, many of the most popular websites encrypt every web request and response. In fact, by 2016, two-thirds of North American Internet traffic will be encrypted.[1]

To protect applications and data, organizations must inspect all traffic, even when it is encrypted. Unfortunately, many security devices cannot inspect encrypted traffic, and the few that can decrypt SSL, or its successor Transport Layer Security (TLS), often cannot keep pace with growing bandwidth demands. This lapse exposes dangerous gaps and blind spots in corporate defenses.

[1] Global Internet Phenomena Spotlight, Sandvine, 2015

CHALLENGE

To stop attacks concealed in SSL traffic, Cisco FirePOWER and Cisco ASA platforms must have full visibility into encrypted traffic.

SOLUTION

A10 Thunder SSLi empowers Cisco customers to eliminate the SSL blind spot in their defenses by intercepting SSL traffic and sending it unencrypted to Cisco FirePOWER or Cisco ASA to detect and block threats.

BENEFITS

- Decrypt SSL traffic at high speeds to identify threats in encrypted traffic
- Prevent costly data breaches by integrating real-time contextual awareness and full-stack visibility
- Defend computers, mobile devices and virtual environments from malware
- Maximize availability and scale using best-in-class load balancing

Although Cisco's ASA and FirePOWER products can decrypt SSL traffic, A10's SSL Insight can offload the computational processing overhead to maximize performance, allowing the Cisco security solution to dedicate its resources for traffic inspection. This is especially important due to the use of more complex SSL ciphers and longer key lengths.

A10 NETWORKS SSL INSIGHT SOLUTION

UNCOVER THREATS CONCEALED IN ENCRYPTED TRAFFIC

A10 Networks has partnered with Cisco to effectively mitigate attacks hidden in encrypted traffic. Cisco network security solutions provide integrated real-time contextual awareness, full-stack visibility and intelligent security automation. The Cisco FirePOWER Next Generation IPS and the Cisco Adaptive Security Appliance (ASA) firewall work together to protect corporate networks and data centers of all sizes.

Deployed in conjunction with A10 Thunder SSLi, Cisco network security solutions deliver the visibility and control to mitigate sophisticated threats and advanced malware. A10 Thunder SSLi decrypts SSL and TLS traffic, enabling Cisco network security solutions to inspect all communications and inspect users, applications and devices to identify threats.

A10 Networks SSL Insight technology enables Thunder SSLi to decrypt SSL traffic and send the decrypted traffic to Cisco FirePOWER or Cisco ASA for inspection. It then encrypts the traffic again and forwards it to the intended destination. A10's SSL Insight technology enables organizations to use 100% of Cisco appliance capacity to protect network traffic without needing to perform computationally intensive SSL encryption and decryption processes.

Thunder SSLi 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 is still an end-to-end encrypted session that is only decrypted within the client's network, in a contained environment. With SSL acceleration hardware, Thunder SSLi 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.

SCALE SECURITY CAPACITY WITH INTEGRATED LOAD BALANCING

With its integrated load-balancing functionality, Thunder SSLi also provides high availability and scale, enabling organizations to deploy multiple Cisco FirePOWER or Cisco ASA appliances. Furthermore, it allows organizations to easily increase security capacity, enabling more security blades and supporting increased traffic throughput.

Supporting a wide range of load-balancing algorithms, including round robin, weighted round robin, least connections and fastest response, Thunder SSLi scales Cisco security deployments and allows organizations to keep up with growing bandwidth requirements.

Advanced health monitoring ensures that Cisco security gateways are responding as expected and routes traffic to available security appliances. With scriptable health checks, Thunder SSLi can evaluate the responsiveness of multiple security appliances based on a wide set of criteria and direct traffic to the best security appliance to meet performance and reduced latency goals.

PROTECT PERIMETER AND DATA CENTER SCENARIOS

Cisco and A10 Thunder SSLi can be deployed in a variety of options to support various user cases and security needs. For maximum efficiency, both inbound traffic to corporate-owned servers and outbound traffic from internal users can be secured using one set of Cisco and A10 Networks appliances.

In a typical scenario, a pair of Thunder SSLi appliances in a high availability configuration decrypts the SSL traffic and forwards it to Cisco FirePOWER or Cisco ASA appliances for multi-layer protection, and then Thunder SSLi re-encrypts the traffic. As shown in Figure 1, for each SSL session:

1. A10 Thunder SSLi decrypts the SSL traffic and sends it to one or more Cisco security appliances.
2. Cisco security appliances inspect the traffic for malicious activity and, if the traffic does not violate a security policy, forwards it back to A10 Thunder SSLi.
3. A10 Thunder SSLi encrypts the data and sends it to the intended server or user.

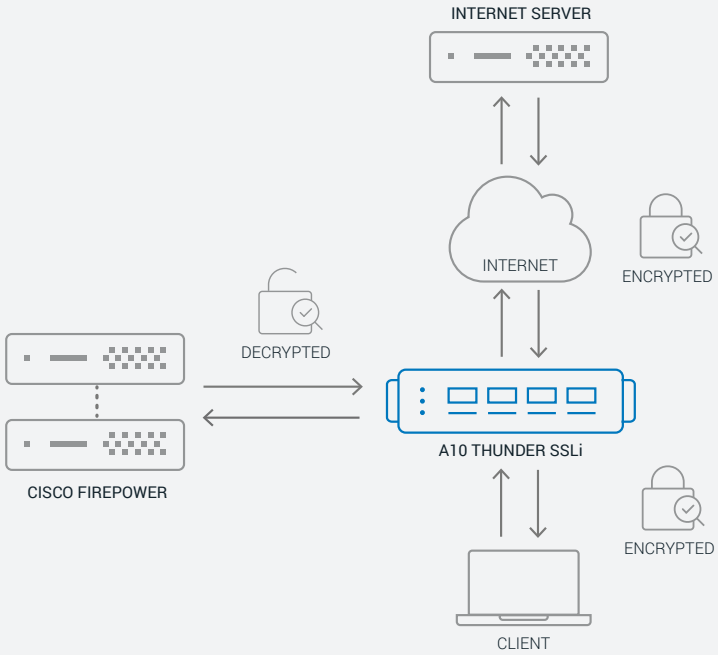

Figure 1: A10 Thunder SSLi working together with Cisco security appliances

HIGH-PERFORMANCE WITH POWERFUL SSL SECURITY PROCESSORS

The initial SSL handshake is the most computationally demanding part of SSL encryption. Encrypting and decrypting the bulk data of a session is still CPU-intensive, but to a lesser degree. A10 Thunder SSLi has been architected to manage many secure connections simultaneously and provides exceptional SSL connection and throughput rates.

Powered by the 64-bit A10 Networks Advanced Core Operating System (ACOS®), Thunder SSLi provides linear scalability and offers the maximum performance available from general purpose CPUs and dedicated security processors. All appliances, hardware, hybrid or local can support SSL offloading, but select models include dedicated high-performance security processors that are exceptionally well suited for managing many SSL sessions simultaneously.

The A10 Thunder SSLi product line enables customers' applications to be highly available, accelerated and secure, for an enhanced application experience.

FEATURES AND BENEFITS

SSL Insight technology for Cisco FirePOWER and Cisco ASA:

- Decrypts SSL traffic at high speeds to identify threats in encrypted traffic
- Prevents costly data breaches by integrating real-time contextual awareness and full-stack visibility
- Defends computers, mobile devices and virtual environments from malware
- Maximizes availability and scale using best-in-class load balancing

A10's powerful SSL Insight capability enables businesses to:

- Gain complete visibility into network activity, including encrypted traffic, to uncover attacks and infiltrations, and to deliver a safe and secure user experience
- Use Thunder SSLi as a centralized point for load balancing and decryption, intercepting SSL traffic and sending it to multiple security devices, such as security analytics, data loss prevention (DLP), threat protection and intrusion detection appliances, for inspection
- Optionally bypass traffic to sensitive websites, such as communications to banking and healthcare sites, to prevent confidential data from being decrypted
- Future-proof their investment as SSL usage expands and encryption key lengths increase

CONCLUSION

As an increasing number of applications encrypt data in transit, SSL exposes dangerous blind spots in corporate defenses. A10 Thunder SSLi, combined with Cisco FirePOWER and Cisco ASA, offers organizations an ideal, easy-to-deploy and scalable solution for intercepting and securing encrypted traffic. A10 Networks has successfully tested and validated interoperability between A10 Thunder SSLi and Cisco network security solutions.

Using A10's SSL Insight technology, organizations can:

- Maximize performance, availability and scalability using A10's 64-bit Advanced Core Operating System (ACOS) and specialized security processors
- Integrate Thunder SSLi with advanced network security platforms such Cisco FirePOWER and Cisco ASA to identify and stop cyber attacks and malware
- Leverage integrated real-time awareness and intelligent security automation to protect their network from advanced threats

NEXT STEPS

For more information, please contact your A10 representative and visit: https://www.a10networks.com/products/ssl-insight-securing-encrypted-traffic.

ABOUT CISCO

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolio of solutions across the broadest set of attack vectors. Cisco's threat–centric and operationalized approach to security reduces complexity while providing unmatched visibility, consistent control, and advanced threat protection before, during, and after an attack. For more information visit: www.cisco.com/go/security.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, 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, Calif., and serves customers globally with offices worldwide.

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

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19149-EN-03 AUG 2017