SOLUTION BRIEF

ANALYZE HIDDEN WEB TRAFFIC WITH A10 NETWORKS & CISCO WEB SECURITY

PREVENT MALWARE AND SENSITIVE DATA LOSS HIDDEN IN SSL TRAFFIC WITH A10 THUNDER SSLi AND CISCO WEB SECURITY APPLIANCE (WSA)

A10 Networks® and Cisco® offer a collaborative solution to mitigate malicious attacks and insider abuse hidden in encrypted traffic. A10 Thunder® SSLi® intercepts SSL traffic and sends it in clear text to the Cisco Web Security Appliance (WSA), allocating 100 percent of the WSA resources to protect network traffic without the need to perform computationally intensive SSL encryption and decryption tasks.

CHALLENGE

As the volume of SSL-encrypted traffic grows, it renders many security devices ineffective. Organizations need a way to see what is happening on their networks and identify any threats that may be cloaked with encryption.

According to NSS Labs, 75 percent of web traffic will be encrypted with SSL/TLS by 2019. SSL decryption and inspection is processor-intensive and may result in performance degradation when decryption is not performed by the hardware.

Modern network security solutions must deliver deep visibility into sessions. Unfortunately, many security devices today cannot inspect encrypted traffic without significant performance degradation. The inability to perform deep session visibility creates dangerous gaps and blind spots in corporate defenses.

CHALLENGE

The rising volume of SSL/TLS traffic makes it impossible to inspect all enterprise traffic with existing security solutions.

SOLUTION

A10 Networks and Cisco Web Security offer a complete Advanced Malware Protection (AMP) and Data Loss Prevention (DLP) solution that decrypts, inspects and re-encrypts SSL/TLS traffic.

BENEFITS

- Decrypt SSL traffic at high speeds
- Identify threats in encrypted traffic
- Prevent costly data breaches
- Maximize scalability through integrated load balancing and clustering
- Exclude sites from SSL decryption by category or custom lists

THE A10 NETWORKS SSLi AND CISCO WSA SOLUTION

The Cisco WSA deployed in conjunction with A10 Thunder SSLi provides the perfect solution to this problem. A10's SSL Insight (SSLi) technology eliminates the encryption blind spot by decrypting SSL/TLS traffic, enabling Cisco Web Security solution to use 100 percent of its resources to protect web traffic without performing resource-intensive SSL encryption and decryption processes.

Cisco Web Security Appliance (WSA) is powered by Talos Security Intelligence and Research Group, the largest threat detection network in the world. This team inspects decrypted traffic in real time, pre-emptively blocking access to suspicious URLs, and actively prevents malware from infecting the network.

These experts help block sensitive data from leaving the network. Enabled with the power of SSL Insight, Cisco WSA can detect threats that were previously invisible.

HOW IT WORKS

A10 Thunder SSLi is an industry-leading, high-performance solution that decrypts SSL traffic before sending it to the Cisco WSA for advanced malware protection and data-loss prevention.

A10 then re-encrypts the traffic before routing it to its final destination. A10 Thunder SSLi implements SSL decryption in high-performance hardware to handle PFS ciphers to avoid a negative user experience.

The Cisco WSA is an on-premise solution that protects businesses with broad threat intelligence, multiple layers of defense and vital data-loss prevention capabilities. Cisco WSA detects and correlates threats in real time by tapping into Cisco's Talos Threat Intelligence system and applying web reputation filters to block suspicious URLs before any traffic is transmitted.

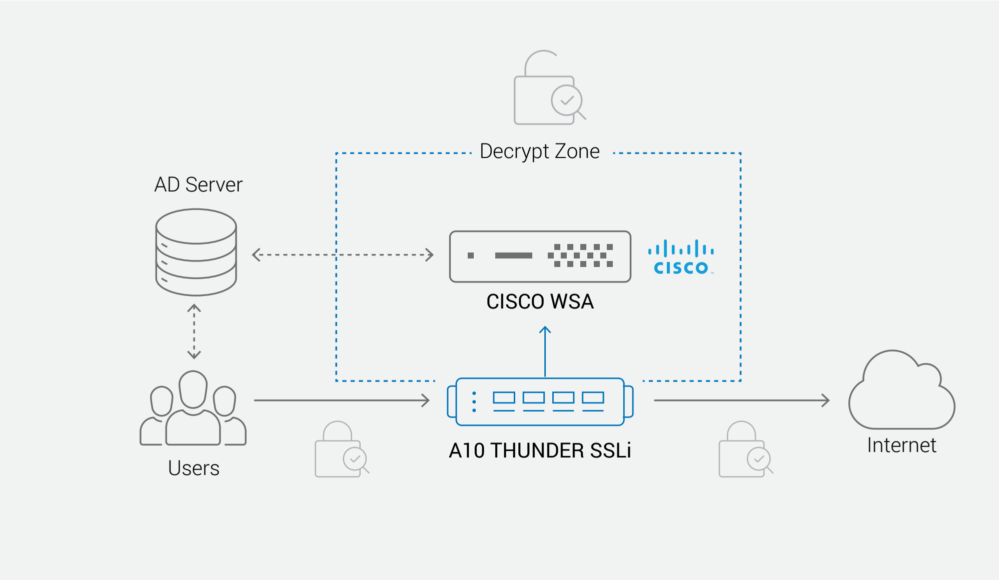
When a web session is in progress, the Cisco WSA delivers robust anti-malware protection by employing enhanced malware defense signature and analytical scanning engines running in parallel in real time.

Cisco WSA integrates DLP functionality to analyze for content markers, such as confidential files, credit card numbers and customer data, and prevents this data from being uploaded to the web. This is combined with actionable reporting capabilities, alerting the end-user as well as the web administrator about the security policy action being applied.

SOLUTION COMPONENTS

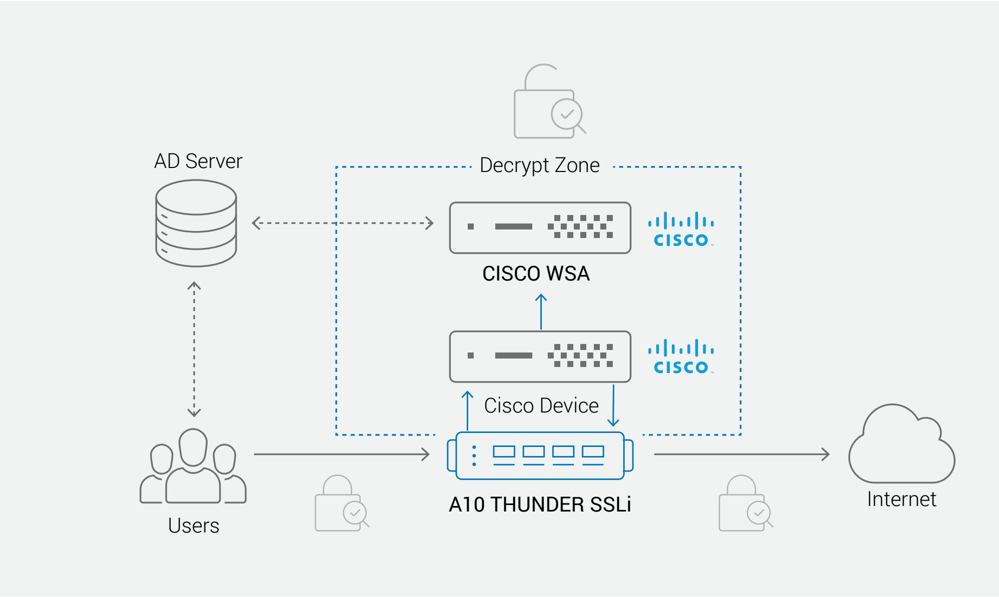
A10 Networks and Cisco Web Security provide a complete solution that provides a look into encrypted traffic to detect and prevent bad actors from defeating network defenses. The following solution components are needed for this integration:

- 1 A10 Thunder SSLi appliance for SSL decryption/re-encryption
- 1 Cisco WSA for web traffic analysis
- 1 authentication server (e.g., Microsoft Active Directory server)



ACTIVE INLINE DEPLOYMENT WITH CISCO WSA

The Cisco WSA is connected in transparent mode directly to the Thunder SSLi appliance. The Thunder SSLi appliance transparently redirects HTTP and decrypted HTTPs traffic to the Cisco WSA, while bypassing all other network traffic. The WSA is also able to reach the authentication server for the domain and apply user-based polices. The Cisco WSA can immediately block incoming and outgoing threats detected in web traffic.



ACTIVE INLINE DEPLOYMENT WITH CISCO WCCP AND WSA

This option allows an existing Cisco WSA deployment to continue working with A10 Thunder SSLi. The Cisco WSA is connected in transparent mode to a WCCP server, such as a Cisco ASA or router.

This WCCP server appliance is connected inline with the Thunder SSLi appliance. The Thunder SSLi appliance sends all traffic through the WCCP server appliance, including decrypted SSL traffic. The WCCP server appliance redirects web traffic to the Cisco WSA. The WSA is able reach the authentication server for the domain and apply user-based polices. The Cisco WSA can immediately block incoming and outgoing threats detected in web traffic.

FEATURES AND 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 uptime and scale using best-in-class load balancing and clustering
- Support many SSL protocols and ciphers, including DHE and ECDHE
- Simultaneously decrypt and load balance
- Support transparent and explicit proxy deployment*

* Explicit proxy mode requires enabling explicit proxy server on the Thunder SSLi appliance, while Cisco WSA operates in transparent mode.

DISCOVER AND PREVENT ADVANCED THREAT TACTICS

Together, A10 Networks and Cisco Web Security offer increased visibility and security for organizations facing critical security threats. The joint solution eliminates the encryption blind spot and enables organizations to analyze all web traffic traversing the network.

Inspect encrypted data by intercepting SSL/TLS communication, decrypting the traffic and sending the traffic in clear text to third-party security devices, such as Cisco WSA.

NEXT STEPS

To learn more about the A10 Thunder SSLi and the Cisco WSA, please contact your A10 representative or visit a10networks.com/SSLi.

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.

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

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19174-EN-01 JUL 2017