SOLUTION BRIEF

SSL INSIGHT FOR TREND MICRO DEEP DISCOVERY

UNCOVER CYBER ATTACKS HIDDEN IN SSL TRAFFIC

A10 Networks and Trend Micro are collaborating to detect and stop advanced targeted attacks hidden in encrypted traffic, without compromising on performance. A10 Networks® Thunder® SSLi® intercepts SSL traffic and sends it unencrypted to Trend Micro Deep Discovery so that advanced 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.

THE CHALLENGE

ENCRYPTION CREATES A BLIND SPOT IN DEFENSES

An increasing number of applications are encrypting data to prevent third parties from accessing sensitive information. Application owners are leveraging Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), to encrypt web traffic. Today, up to 85% of internet traffic in North America is encrypted and this number is increasing every year.[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 often cannot keep pace with growing bandwidth demands. This lapse exposes dangerous gaps and blind spots in corporate defenses.

[1] https://transparencyreport.google.com/https/overview?hl=en

CHALLENGE

To stop malware and cyber attacks concealed in SSL traffic, Trend Micro Deep Discovery must have full visibility into encrypted traffic.

SOLUTION

A10 Thunder SSLi empowers Trend Micro customers to eliminate the SSL blind spot in their defenses by intercepting SSL traffic and sending it unencrypted to Trend Micro Deep Discovery to detect and block threats.

BENEFITS

- Decrypt SSL traffic at high speeds to identify threats in encrypted traffic
- Prevent costly data breaches by combining local and global threat intelligence with custom sandboxing
- Rapidly respond to incidents with advanced forensics and shared IOC intelligence
- Maximize uptime and scale using best-in-class load balancing and clustering

THE A10 NETWORKS SSL INSIGHT SOLUTION

UNCOVER THREATS CONCEALED IN ENCRYPTED TRAFFIC

A10 Networks has partnered with Trend Micro to effectively mitigate attacks hidden in encrypted traffic, without compromising performance. Trend Micro Deep Discovery enables you to detect, analyze and respond to today's stealthy, targeted attacks in real time. Deep Discovery is a network appliance that gives you 360-degree network monitoring of all traffic and all protocols to detect all aspects of a targeted attack.

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

The A10 Thunder SSLi product line is an industry-leading, high-performance family of SSL decryption devices. With its SSL Insight® technology, Thunder SSLi decrypts SSL traffic and sends the decrypted traffic to Trend Micro Deep Discovery 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 the Trend Micro appliance's capacity to protect network traffic without needing to perform computationally intensive SSL encryption and decryption processes.

When Thunder SSLi is deployed as a transparent SSL proxy, 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.

SCALE SECURITY CAPACITY WITH INTEGRATED LOAD BALANCING

With its load-balancing capabilities, Thunder SSLi also provides high availability and scale, enabling organizations to deploy multiple Trend Micro Deep Discovery appliances. Furthermore, it allows organizations to easily increase security capacity, enabling more security blades and supporting increased traffic throughput. Thunder SSLi easily scales Trend Micro security deployments and allows organizations to keep up with growing bandwidth requirements.

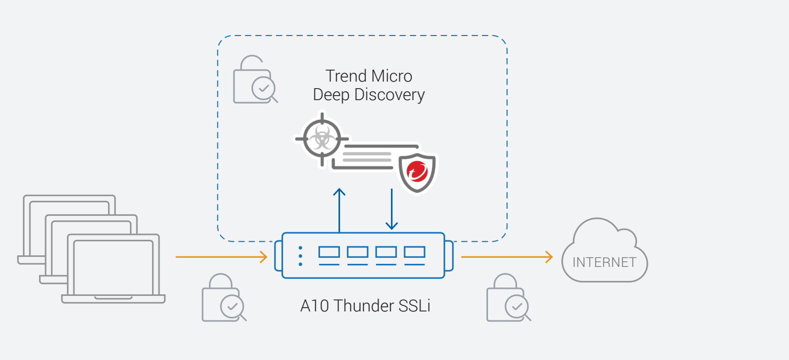

Figure 1: A10 Thunder SSLi working together with Trend Micro security appliances

PROTECT PERIMETER AND DATA CENTER SCENARIOS

Trend Micro and A10 Thunder SSLi can be deployed in a variety of ways to support various use 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 Trend Micro 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 Trend Micro Deep Discovery 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 Trend Micro security appliances.
2. Trend Micro 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.

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.

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.

FEATURES AND BENEFITS

SSL Insight technology for Trend Micro Deep Discovery:

- 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 uptime and scale using best-in-class load balancing and clustering

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 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

SUMMARY – A10 NETWORKS AND TREND MICRO DEFEND AGAINST ATTACKS HIDDEN IN ENCRYPTED TRAFFIC

As an increasing number of applications encrypt data in transit, SSL exposes dangerous blind spots in corporate defenses. A10 Thunder SSLi, combined with Trend Micro Deep Discovery, 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 and Trend Micro security solutions.

Using A10's SSL Insight technology, organizations can:

- Maximize performance, availability and scalability using A10's 64-bit Advanced Core Operating System and specialized security processors
- Integrate Thunder SSLi with advanced network security platforms such Trend Micro Deep Discovery 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: a10networks.com/products/ssl-inspection.

ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Built on 26 years of experience, our solutions for consumers, businesses and governments provide layered data security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by more than 1,200 threat experts around the globe. For more information, visit TrendMicro.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

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-SB-19152-EN-02   NOV 2018