Bring Visibility to the Blind Spot with A10 Networks & Fidelis Cybersecurity

Stopping Encrypted Attacks with A10 Thunder SSLi and Fidelis Network

Challenge:

The rising volume of SSL/TLS encryption makes it impossible for traditional security solutions to inspect all enterprise traffic, without compromising the network performance. As a result, organizations bypass encrypted traffic – and introduce an attack vector – and an avenue for data exfiltration.

Solution:

A10 Networks and Fidelis Cybersecurity, together, offer a complete security solution that has the ability to monitor all enterprise traffic and eliminate the SSL/TLS blind spot.

Benefits:

- Versatile deployments
  - In–line or out-of-band
- Visibility into encrypted network traffic
  - Exclude sites from SSL decryption
- Actionable insight into network sessions
  - Stop the initial exploit
  - Reduce response time
  - Increase detection and remediation coverage

A10 and Fidelis Bring More Visibility

While SSL/TLS keeps communications secure, it creates a blind spot that is used as an attack vector by adversaries – or a means for disgruntled employees to exfiltrate proprietary information. Without visibility into encrypted network traffic at the network session and content level, security teams cannot answer CIO and CISO questions pertaining to the threats and their impact on enterprises. Businesses require solutions that expose encrypted threats, without compromising the user experience.

Modern network security solutions must deliver deep visibility into sessions and session content that goes beyond simple packet inspection.

The Challenge

The existing blind-spot of SSL/TLS traffic is increasing and this renders many security devices ineffective, reducing the value of customers' capital investment in security solutions. This is due to the computation intensity required to perform SSL decryption – often resulting in degraded performance.

Organizations need greater context aware network information to identify threats that may be cloaked with encryption. CIOs and CISOs can no longer think that because their network traffic is encrypted, everything is safe.

According to the Ponemon Institute, "Hidden Threats in Encrypted Traffic: A Study of North America & EMEA," more than 60 percent of organizations have not implemented proper SSL decryption due to concerns over performance.

The A10 Thunder SSLi and Fidelis Network Solution

The Fidelis Network™ solution, coupled with A10 Thunder® SSLi®, provides the ideal solution to this performance and blind spot dilemma. Combining Fidelis Cybersecurity's next-generation intrusion prevention capabilities with A10's SSL Insight (SSLi) technology, eliminates the encryption blind spot without compromising performance. Fidelis Cybersecurity's Deep Session Inspection®, inspects network traffic and provides visibility that can prevent malware of proprietary information from infecting or leaving the network. Together A10 and Fidelis can cast a light on threats that were previously lurking in the shadows.

Here's how it works:

The A10 Thunder SSLi provides visibility into encrypted traffic to stop potential threats by decrypting the traffic and allowing it to be inspected before it is re-encrypted and sent to its destination. It helps reveal malicious traffic that may be hidden by SSL encryption.

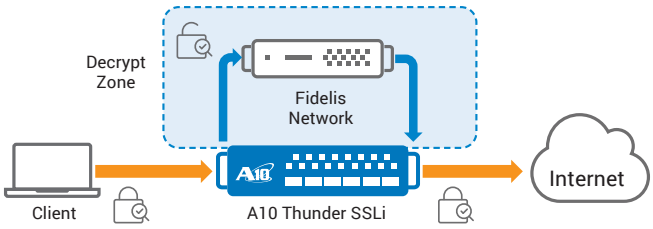
The Fidelis Network solution has sensors that can be deployed both in-line and out-of-band. The sensors are connected to the network, looking for threats traversing the network. If any detections are made, the connection is reset and users are notified via alerts and detailed analytics into the origin of the attack.

The A10 and FIdelis solution focuses on network sessions rather than just packets, looking at the entire complete network sessions in real-time. The Fidelis Deep Session Inspection runs on the Fidelis network sensors allowing customers to see deeper into the content flowing over the networking, providing an X-Ray-like view of the content that is flowing over the network.

Solution Components

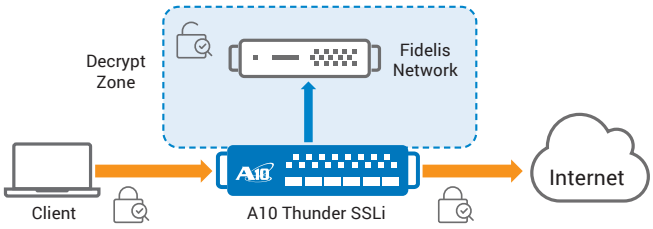
Active Inline Deployment with Fidelis Network

Encrypted traffic is intercepted and decrypted – and the clear-text traffic is transmitted for inspection. Fidelis Network can immediately block detected threats. Legitimate traffic is re-encrypted and dispatched towards the destination. If traffic levels increase and additional security tools are needed, A10 natively supports server load balancing without any additional license.



Passive Out-of-Band Monitoring Deployment with Fidelis Network

For Enterprises that only wish to passively monitor threats and still offer prevention options, Fidelis can be deployed in a passive mode. In this mode, traffic is intercepted, decrypted, re-encrypted, and sent to the destination – and a copy of decrypted traffic is transmitted to Fidelis for inspection. The Fidelis device can issue alerts, send RESETS, and perform further analytics on the traffic. If traffic levels increase and additional passive security tools are needed, A10 natively supports server load balancing without any additional licenses.



Features and Benefits

- Decrypts SSL/TLS-encrypted traffic across all ports and protocols
- Scales up to 40+ Gbps of SSL/TLS traffic in a 1U form factor
- Dynamically detect SSL/TLS across all ports
- Control cipher-suites used for SSL/TLS sessions
- Decrypt SSH and STARTTLS (SMTP, XMPP, etc.) protocols
- Supports many SSL/TLS PFS ciphers
- Integrated FIPS 140-2 level 3 Hardware Security Module supported
- Simultaneously decrypt and load balance to multiple sensors
- Provides flexible deployment options
- Supports URL classification for URL filtering and bypassing
- Deep Session Inspection provides contextual visibility and security
- Faster resolution time with automated alerts and endpoint validation
- Shrinks security stack with IPS, malware protection, analytics and data loss prevention, available in one solution
- Cloud-based updates available

Stop Encrypted Attacks: Discover and Prevent Advanced Threat Tactics

Together, A10 Networks and Fidelis Cybersecurity offer increased visibility and security for any organization facing cyber threats, including government, healthcare, and financial sectors. This solution eliminates the encryption blind spot and enables organizations to analyze all network data and close the inspection gap.

Next Steps

To learn more about the A10 SSLi and Fidelis Network intrusion prevention solution, please contact your A10 representative or visit www.a10networks.com.

About Fidelis Cybersecurity

We prevent intrusions. And we do it relentlessly. Whether attackers are trying to gain a foothold in your network or accessing sensitive data on your laptops and servers, Fidelis detects it. Then, we tell you everything you need to find them and stop them in minutes (not days or weeks). We call it next generation intrusion prevention. And we're the first and only company to deliver it from the cloud. To learn more about our products and incident response services, visit www.fidelissecurity.com.

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: www.a10networks.com or tweet @A10Networks.

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-19173-EN-01
May 2017

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 discover how A10 Networks products will enhance, accelerate and secure your business, contact us at **a10networks.com/contact** or call to speak with an A10 sales representative.