SOLUTION BRIEF

FireEye and A10 Networks

Encryption reduces visibility and security

SECURITY REIMAGINED

INTEGRATED SOLUTION AT A GLANCE

- **Scalability,** with up to 23.8 Gbps of SSL inspection performance on a 1U appliance.
- **Load Balancing** of up to 16 security devices to maximize uptime and scale security deployments.
- **Advanced SSL Insight** features like automated detection of encrypted traffic, untrusted certificate handling, and more.
- **Hardware Security Module** (HSM) integration for FIPS 140-2 Level 3 compliant SSL key management.
- **Traffic steering** to intelligently route traffic, optimize performance and reduce security appliance costs.
- **Analyze all suspicious Web objects** including PDFs, Flash, multimedia formats, and ZIP/RAR/TNEF archives as well as blocks outbound malware to thwart data exfiltration
- **Consolidate** signature-based and signature-less technologies with integrated IPS functionality

To stop cyber threats like malware and targeted attacks, organizations need to inspect all types of traffic, including encrypted SSL communications. With the transition from 1024- to 2048- bit SSL keys and growing SSL usage, organizations need a powerful, high performance platform that can decrypt and inspect encrypted data.

OVERVIEW

Attackers have set their sights on vulnerable end users, leveraging malware to compromise client computers. Once infected, client computers become unwitting members of botnets, relaying information to command and control servers and exposing not only one machine, but potentially an entire network to reconnaissance and infiltration.

At the same time, more and more applications are encrypting data to prevent third parties from accessing sensitive information. Technologies such as Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are being used to secure web and email traffic.

Increasing SSL usage poses a problem when organizations wish to inspect traffic for malicious content such as malware, viruses or targeted phishing attacks. Many products that secure web, email and file transactions cannot inspect encrypted traffic or cannot keep pace with growing SSL encryption demands, resulting in blind spots in corporate defenses.

HOW THE JOINT SOLUTION WORKS

Inline FireEye Deployment

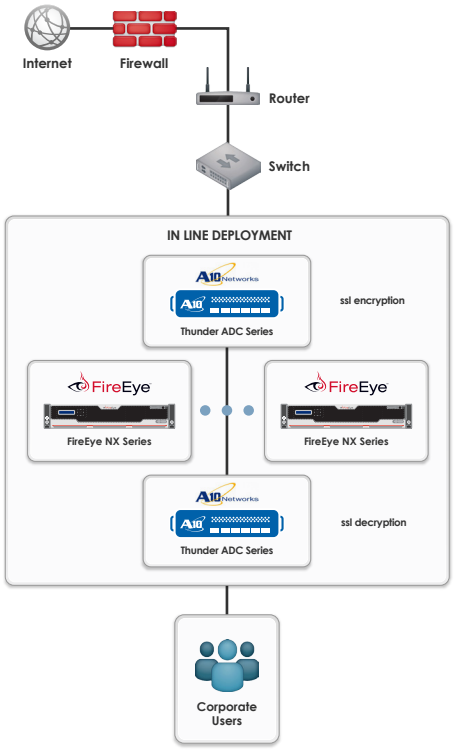
A Thunder ADC appliance deployed between clients and FireEye appliances intercepts outgoing SSL traffic and sends the traffic unencrypted to the FireEye appliances.

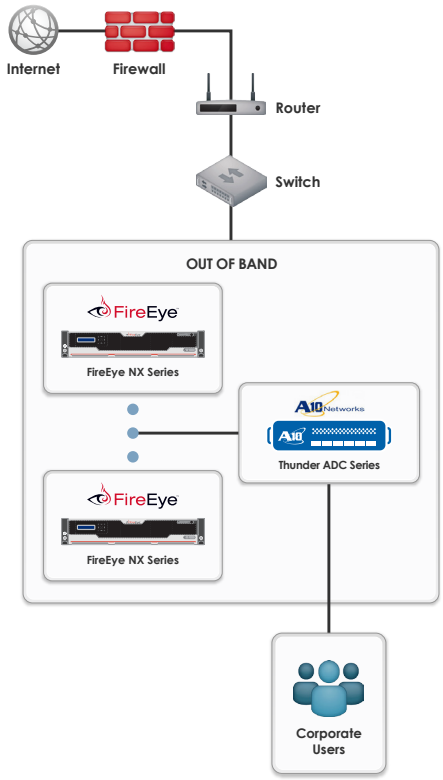
The FireEye appliances inspect traffic for advanced threats and forward legitimate traffic on.

A second Thunder ADC appliance, deployed between the FireEye appliances and the Internet, receives traffic from the FireEye appliances, encrypts the data and sends it to an external server.

Non-inline FireEye Deployment

FireEye platforms can also be deployed in a non-inline passive configuration. In this configuration, a duplicated copy of the decrypted traffic is sent to the FireEye device, so that it can inspect the traffic and even mitigate certain threats if desired. In passive mode, the FireEye unit can easily be integrated in a production network, without disruption. This is a non-intrusive setup; the FireEye Threat Prevention Platform is not involved in the path of the network traffic flow.





ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,700 customers across 67 countries, including over 157 of the Fortune 500.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a technology leader in application networking, 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: http://www.a10networks.com

For more information, contact: CSC@FireEye.com

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye