Solution Brief

Symantec Technology Integration Partner: FireEye

Business Challenge

The use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for Internet and enterprise traffic is growing steadily. Many modern applications use SSL communications by default. Even hosted and mobile email applications such as Gmail, Yahoo, and Zimbra utilize SSL encryption by default in today's workplace environments. For end users, SSL has long been a means to secure web-based transactions that enable e-commerce and online banking. Over time, the simplicity of SSL has made it the perfect vehicle for migrating new online services to cloud and web-based models. These services include applications for secure viewing of medical records, ordering prescriptions and filing tax returns. It has also emerged as a perfect vehicle for spreading threats. For their protection, it's clear that enterprise organizations now need complete visibility into the encrypted SSL-based traffic transiting their networks.

Historically it has been difficult, if not impossible, to satisfy the competing requirements for comprehensive security, high performance, and effective, policy-based control. While encrypting web sessions protects end-user data from being viewed in transit over the Internet, it creates a blind spot for IT administrators. They typically have no visibility into SSL-encrypted traffic. For that reason, SSL has unfortunately become one of the most popular ways to mask malicious code, such as Trojan horses and viruses. Incoming and outgoing threats can hide in SSL to bypass security solutions and spread freely throughout and between organizations.

This lack of visibility into SSL can make it difficult or impossible for network administrators to enforce acceptable use policies and to ensure that threats like viruses, spam, and malware are stopped before they reach individual users. The inability to examine the content of SSL communications also makes it possible for sensitive or critical information to be accidentally leaked or worse, stolen.

Solution: Symantec SSL Visibility and FireEye Network Threat Prevention Platform (NX Series)

Symantec offers inbound and outbound SSL inspection via the SSL Visibility product line. Symantec SSL Visibility accepts multiple simultaneous streams of data in multiple protocols and feeds decrypted data to multiple security devices, such as the FireEye NX for inspection an analysis. The FireEye NX accepts the decrypted clear text, analyzes it for malicious content, alerts/blocks malicious traffic and can also block call backs from infected systems.

FireEye

Partner: FireEye

Partner Product: FireEye Network Threat Prevention Platform (NX Series)

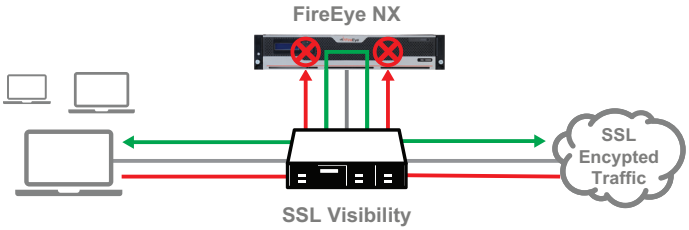
Symantec Product:
Symantec SSL Visibility

Symantec

How it Works

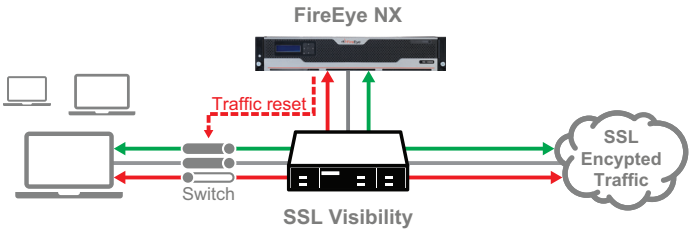
The FireEye NX integrates with SSL Visibility. This integration provides enterprises with a complete solution for protection against advanced cyber threats and threats hidden in SSL traffic. This investment includes the innovative zero-day threat protection capability of FireEye NX to extend the protection across the enterprise.

Active - Inline Deployment (Block or Monitor)



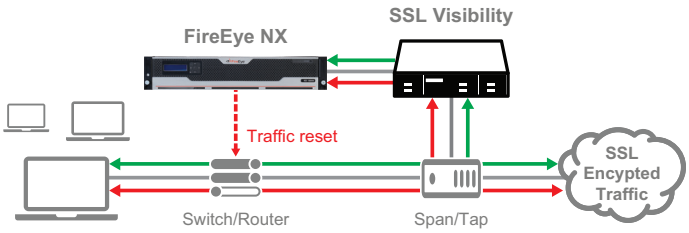
The SSL Visibility is deployed inline and offers line-rate, high-performance throughput with decryption and inspection of up to 9 Gbps of SSL traffic. SSL Visibility decrypts SSL traffic and sends it to FireEye NX. The FireEye NX analyzes the traffic and blocks or just alerts on malicious traffic as the customer desires. If not blocked, SSL Visibility then re-encrypts the traffic and sends it to the destination.

Passive – Inline Deployment (Monitor or Block)



SSL Visibility is deployed inline and offers line-rate, high-performance throughput decrypting SSL traffic as mentioned above. SSL Visibility sends a copy of the decrypted traffic to the FireEye NX for analysis. The FireEye NX analyzes the traffic and sends a reset to a network device or just alerts on malicious traffic as the customer desires.

Passive – Tap Deployment (Monitor or Reset)



The SSL Visibility is deployed on a network tap decrypting SSL traffic as mentioned above. The SSLV sends a copy of the decrypted traffic to the FireEye NX for analysis. The FireEye NX analyzes the traffic and sends a reset to a network device or just alerts on malicious traffic as the customer desires. Note that this particular deployment mode only supports inbound SSL inspection when using RSA key exchange mechanism.

Benefits

The combined Symantec SSL Visibility and FireEye Network Threat Prevention Platform (NX Series) solution:

- Eliminates SSL blind spots
- Stops rogue applications from using SSL to subvert enterprise controls and security measures
- Uses FireEye-provided lists to scan SSL-encrypted traffic for viruses, worms, and Trojans, stopping them at the gateway
- Prevents call backs from infected systems
- Supports multiple deployment modes: active in-line with monitor or block, passive in-line with monitor or reset and passive tap with monitor or reset
- Utilizing the SSL Visibility's unique Host Categorization service your organization can easily balance data privacy and security demands and satisfy your Legal, Compliance and Risk Management teams.

About FireEye

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise – reinforced with an aggressive incident response team – helps eliminate the impact of breaches. FireEye has over 4,300 customers across 67 countries, including 675 of the Forbes Global 2000.

For More Information

Learn more about Symantec Technology Integration Partners on our website.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.
SYMC_sb_TechPartner_SSL-VA_FireEye_EN_v1a