Solution Brief

Symantec Technology Integration Partner: VSS Monitoring

Business Challenge

The ability to respond to evolving online threats is a never-ending race between threat actors and threat defenders. Traditional security methods such as next-generation firewalls and other reactive measures are losing the fight against this new breed of attacks. In this race, it is impossible to know how to prevail against these adversaries – and protect vital assets – without understanding their attack methods.

Threats are becoming more sophisticated and targeted, compromising even the most comprehensive and well-designed network security architectures. A comprehensive and layered defense is a basic need, and visibility into all aspects of the network traffic places greater demands on operations and security personnel. Gartner Research predicts that 50% of all network attacks will be encrypted by 2017. Security tools such as next-generation firewalls (NGFWs), intrusion detection/prevention systems (IDSs/IPSs), data loss prevention (DLP), analytics and malware are blind to the traffic that is being encrypted within SSL, creating security threat challenges.

Solution: Symantec SSL Visibility and VSS Monitoring vBroker Series Network Packet Brokers

Symantec's encrypted traffic management solution eliminates the encrypted traffic blind spot and combats the security threats hidden in encrypted traffic. Comprised of the market-leading Symantec SSL Visibility, it enhances existing security solutions by providing visibility into previously hidden traffic and advanced threats without requiring significant upgrades or re-architecting the network security infrastructure.

SSL Visibility is a high-performance, purpose-built solution that utilizes comprehensive policy enforcement to inspect, decrypt and manage SSL traffic in real time while ensuring data privacy and regulatory compliance. The unique "decrypt once, feed many" design of SSL Visibility empowers multiple security tools.

Partner: VSS Montoring

Partner Product: vBroker Series Network Packet Brokersr

Symantec Product: SSL Visibility

By partnering with VSS Monitoring and using vBroker Series network packet brokers (NPBs), decrypted traffic can be forwarded to multiple security tools through the VSS Unified Visibility Plane. Security tools can perform properly when presented with decrypted traffic. Network visibility into the encrypted traffic effectively detects and eliminates advanced threats without hindering device or network performance. The combination of the SSL Visibility and VSS NPBs delivers a best-in-class solution to decrypt SSL traffic, uncover hidden threats, and eliminate these SSL blind spots.

Symantec SSL Visibility is an integral component of an encrypted management strategy, and provides visibility into SSL encrypted traffic without requiring the re-architecting of the network infrastructure. SSL Visibility gives the VSS Monitoring solution visibility into all SSL traffic and applications to close the security visibility loophole created by encrypted traffic. In addition, it has the ability to selectively decrypt and inspect suspicious or unknown encrypted traffic while not inspecting other SSL traffic due to mandates such as HIPAA, SOX, PCI, Sarbanes-Oxley, and so on. In a layered security deployment, "lean forward" security is needed for organizations to combine existing systems with scalable decryption and sandboxing technologies. VSS NPBs uniquely leverage years of experience building security capabilities for global customers. This joint solution harnesses the capabilities of SSL Visibility to inspect and decrypt SSL traffic with the VSS Unified Visibility Plane, sending relevant decrypted traffic to any or all of your security tools as needed.

Solution Design

The diagram below demonstrates how the Symantec and VSS Monitoring solutions work together to provide best-in-class encrypted traffic management. This example shows a design using Symantec SSL Visibility with the VSS Monitoring vBroker 110 modular 1G/10G NPB, which provides a dynamic, flexible, and cost-effective solution for any network. The joint solution provides visibility and data access across the network for centralized or distributed security tools, and supports flexible designs for both passive and active inline security tools.

SSL Visibility provides decrypted content from SSL flows to the VSS vBroker. The vBroker then shares the decrypted data with all of the existing security appliances that are needed in the design to support functions such as firewall/NGFW, malware analysis, forensics, compliance, and DLP. This provides these complementary security appliances and applications with the necessary visibility into decrypted SSL traffic. The joint solution allows enterprises to easily add SSL visibility and inspection capabilities, along with category-based inspection policies, into their existing network security architectures.

How it Works

1. The VSS Monitoring vBroker 110 receives traffic from the internal network.

2. The vBroker passes only SSL and Port 443 traffic to Symantec SSL Visibility. This allows Symantec SSL Visibility to perform decryption at a very high rate.

3. Symantec SSL Visibility makes a copy of and decrypts the copied traffic, and then sends the decrypted traffic to the vBroker.

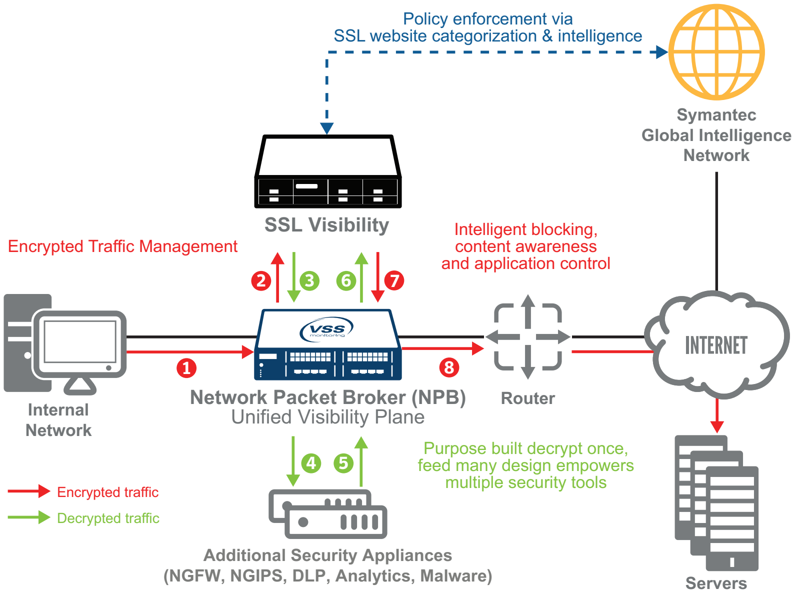
4. The vBroker sends the decrypted traffic to any or all of the additional security tools that are required to have visibility into the data, either sequentially or in parallel, based on either their passive or active nature. These tools then decide whether the decrypted SSL traffic should be allowed to continue to the desired external servers.

5. The security tools return their results to the vBroker.

6. The vBroker returns the traffic to Symantec SSL Visibility.

7. Symantec SSL Visibility determines whether the original encrypted session should continue or be reset. If it determines it can continue, the encrypted SSL traffic is returned to the vBroker.

8. If the traffic is permitted, the vBroker sends the encrypted SSL traffic to the desired external servers, where policy enforcement, categorization, and intelligence are provided by the Symantec Global Intelligence Network.



About VSS Monitoring

VSS Monitoring provides solutions that monitor, analyze and defend today's dynamic network. The VSS Unified Visibility Plane delivers global visibility to network and application monitoring tools, reinforces layered security without performance impact, and provides on-demand network intelligence. Proven in enterprise-scale data centers and service provider environments, VSS Network Packet Brokers (NPBs) simplify IT operations, improve efficiency of tools, and strengthen security systems. For more information, visit www.vssmonitoring.com.

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.