HAUMOUN
IT PIONEERS

Managing Encrypted Traffic with Symantec Solutions

The use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for Internet and enterprise traffic is growing steadily. Modern applications that use SSL communications by default – such as SharePoint, Exchange, WebEx, Salesforce.com and Google Apps – are commonplace and rapidly growing. Even hosted and mobile email applications such as Gmail, Yahoo and Zimbra utilize SSL encryption by default in today's workplace environments.

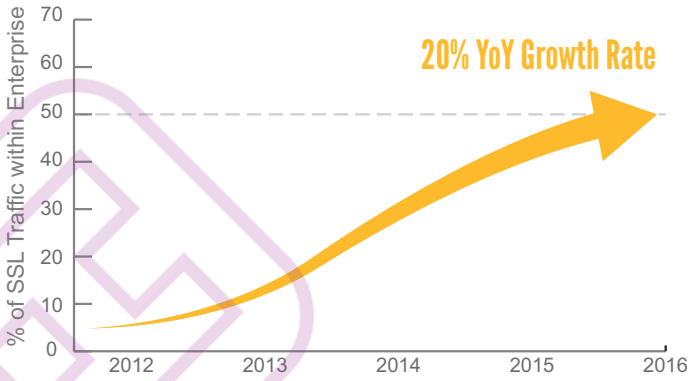
It's clear that Enterprise organizations now need complete visibility into the encrypted SSL-based traffic. A holistic encrypted traffic management strategy that considers the various division needs, policies to be established, regulatory compliance requirements, and data privacy mandates is essential for all federal agencies. Symantec has solutions today to manage this growing encrypted traffic dilemma.

The Impact and Risks Associated with SSL-based Encrypted Communications

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, including applications for secure viewing of medical records, ordering prescriptions and filing tax returns.

It's clear that there are legitimate needs for encrypted data within, to, and from federal agencies. But as many IT managers are aware, its privacy benefits can be overshadowed by its risks.

SSL Encrypted Traffic in Enterprises



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 issue is becoming a "hot button" for security applications that tackle data loss prevention (DLP), compliance reporting and lawful decryption – solutions that could, at one time, see what was outgoing, but are suddenly in the dark because of the growth of SSL traffic and the increase in data privacy practices.

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. This was apparent in the highly-publicized and costly data exfiltration and security breachesat multiple enterprise organizations in the past year.

Symantec

Regulatory compliance requirements, including the identification of accidental or intentional leakage of confidential information, are also virtually impossible to meet because of SSL encryption. In many instances, organizations face conflicting requirements to encrypt and examine data. This SSL conundrum has wreaked havoc on organizations subject to industry and government compliance mandates, such as HIPAA and Sarbanes-Oxley (SOX), which require that only authorized individuals have access to hardware and software resources within the network infrastructure. Other compliance mandates require organizations with publicly accessible networks to have the capability to provide law enforcement agencies with documentation of network activity – which requires that all traffic be unencrypted.

SSL Encrypted Traffic Management Options

Network Security Operators (SecOps) already deploy an array of network security appliances to protect their organizations, enforce internal acceptable-use policies, and satisfy government regulations. These devices can detect rogue applications, control unrestricted web surfing, traffic, provide VPNs, provide intrusion detection and prevention (IDS/IPS), anti-virus (AV) protection, DLP and more. Unfortunately, these network and security appliances, in many instances, can only inspect plaintext traffic and are unable to inspect SSL-encrypted communications for malware, hidden threats or extracted data. They are therefore less effective as the volume of encrypted SSL traffic continues to grow.

Network operators have had to choose between two extremes in confronting these issues. They can take a draconian approach by blocking all SSL communications entirely, or allow SSL communications transparently, without inspection, by leaving TCP port 443 open within their security infrastructure. The former approach is impractical and risky due to the growing number of enterprise cloud and mobile applications that rely on encrypted communications like SSL. The latter approach is also insufficient as it significantly increases risk and greatly reduces the effectiveness of network security appliances to examine encrypted flows. Neither of these choices is a viable option for enterprise networks.

Other approaches provide limited inspection of SSL-encrypted flows, enabling the dropping of content that doesn't meet acceptable-use policies or the logging of suspected attacks to a management station. While these approaches may successfully allow or block some encrypted traffic, such as just HTTPS or web traffic, they are limited in scope and effectiveness. A more holistic approach is needed.

Symantec Encrypted Traffic Management Solutions

Symantec can assist the Enterprise with an appropriate encrypted traffic management strategy and supporting security architecture. Symantec provides comprehensive, policy-based visibility into encrypted traffic through Symantec SSL Visibility and Blue Coat ProxySG solutions. Whether exposing previously hidden advanced persistent threats (APTs), or offloading the performance burden on existing security appliances and enabling them with visibility into formerly encrypted traffic, or simply protecting data from loss and exfiltration, Symantec solutions can help government organizations of all sizes with managing encrypted communications.

The Symantec SSL Visibility Appliance

Symantec SSL Visibility provides decrypted content of SSL flows to existing security appliances used for NGFW, IDS, IPS, forensics, compliance, DLP and more. This enables these existing security appliances with the necessary visibility into both SSL and non-SSL network traffic. Organizations can easily add SSL inspection and management capabilities to their network security architectures immediately to uncover the security visibility blind spot that SSL creates.

Features and Benefits

The unique capabilities of Symantec SSL Visibility help organizations remove risks arising from incomplete visibility and ineffective management of SSL traffic – while increasing the performance of security and network appliances. With market reports highlighting that merely enabling SSL decryption and encryption within these common security appliances results in a dramatic decrease in performance of up to 80% – simply enabling encrypted traffic management as an add-on feature is not sufficient. A complementary approach that maintains the performance of the installed network security infrastructure is needed – especially to extend the life and return on investment (ROI) of these appliances throughout the organization.

SSL Visibility offers the following benefits:

- Line-rate, high-performance throughput with decryption and inspection of up to 9 Gbps of SSL/TLS traffic
- Offers up to 40 Gbps of overall packet processing across multiple ports
- Manages and inspects up to 800,000 concurrent active SSL sessions
- Provides an SSL session setup and teardown rate of up to 30,000 sessions per second
- Provides advanced policy creation and enforcement, enabling the necessary balance of security and data privacy based on organizational needs
- Supports multiple deployment modes: active inline, passive inline and passive tap, input aggregation and output mirroring
- Provides resiliency and high-availability through fail-to-wire (FTW), fail-to-appliance (FTA) and configurable link state monitoring and mirroring
- Unmatched and complete support of all SSL/TLS versions and over 70 cipher suites

Deploying SSL Visibility is transparent to end systems and to intermediate network elements. It doesn't require network reconfiguration, IP addressing or topology changes, or modification to client and web browser configurations. Decrypted plaintext is simply delivered to security appliances as a generated TCP stream that contains the packet headers as they were received.

Lastly, SSL Visibility allows agencies to establish, enforce and manage policies for encrypted traffic throughout their networked infrastructure. Using the Host Categorization function, SSL Visibility can block, permit and forward SSL encrypted traffic based on numerous, familiar policies, such as whether the traffic contains personal banking or healthcare data. This is accomplished in a similar manner as that used in the Blue Coat ProxySG, PacketShaper and other proven solutions, utilizing the comprehensive Global Intelligence Network for comprehensive, host category and threat updates across the globe.

Symantec SSL Visibility are FIPS 140-2 Level 2 certified and Common Criteria (CC) certified.

The ProxySG Appliance

SSL inspection and management are not new to the ProxySG, Symantec's industry-leading secure web gateway solution. Through advanced policies the ProxySG can selectively inspect and decrypt network traffic and attachments for malware, and content for data leakage prevention. It also enables third-party integration of AV and DLP offerings over ICAP (Internet Content Adaptation Protocol). The SSL Proxy function terminates and re-establishes SSL connections, and allows the ProxySG to securely send attached files and content to other security devices for inspection services.

Features and Benefits

Encrypted Tap is an optional feature for ProxySG appliances that works with the SSL proxy to provide visibility into SSL traffic, while sharing the decrypted content with attached logging, monitoring or analysis devices. Encrypted Tap sends a stream of decrypted traffic to third-party logging systems for analysis, archiving and forensics. By providing this SSL visibility and control, Symantec now offers a complete SSL web security solution with its ProxySG family of secure web gateway appliances.

Encrypted Tap is available for the latest ProxySG appliances. These appliances already include SSL hardware assist and SSL licenses, and would need only the additional Encrypted TAP license to deliver comprehensive SSL visibility to leading monitoring and analysis appliances.

- The ProxySG Appliance offers the following benefits:
- A purpose-built operating system that can be centrally managed as part of an enterprise-wide solution deployment
- Stops rogue applications from using SSL to subvert enterprise controls and security measures
- Scans SSL-encrypted traffic for viruses, worms, and Trojans, and stops them at the gateway
- Prevents spyware from installing or communicating over SSL and stops phishing and pharming attacks that use SSL to hide from
  IT controls
- Accelerates approved and safe SSL-encrypted traffic
- Provides advanced policy creation and enforcement, enabling the necessary balance of security and data privacy based on organizational needs

In contrast to SSL Visibility, the policy capabilities of the ProxySG allow for the display of splash screens reminding users of acceptable use, and warning them that monitoring extends to SSL.

Conclusion

Encrypted traffic is pervasive in today's organizations and market research indicates continued rapid growth over the next several years. IT security operators are looking for new solutions that satisfy the need for information security for both the Enterprise and individual users, as well as requirements for compliance, acceptable-use policies and government regulations for security and privacy. The resulting solution must not require re-architecting the security infrastructure, nor impact network performance, because compliance at the expense of throughput is no more acceptable than meeting user and application bandwidth requirements while ignoring security. Historically it has been difficult, if not impossible, to satisfy these competing requirements for comprehensive security, high performance and effective, policy-based control. Symantec offers a choice of encrypted traffic management solutions that meet these requirements, and give complete visibility and control of SSL communications and the potential threats therein.

Choosing the right solution

SSL VISIBILITY	PROXYSG
• Supports multiple, simultaneous streams (i.e. feeds up to three attached security devices simultaneously with decrypted traffic)	• Supports a single output stream of decrypted traffic - via the Encrypted Tap option
• Copy of decrypted traffic can be sent to: › Inline deployment with policy enforcement options for active appliances › In-line with passive appliances • SPAN/Tap/Mirror deployment with passive appliances	• Decrypted traffic can be sent to attached AV, URL filtering or DLP solutions via ICAP (optional) • All ProxySG deployment methodologies supported (see Secure Web Gateway Deployment Methodologies white paper)
• High Performance (multi-gigabit/sec SSL visibility throughput	• Performance based on ProxySG performance
• Policy capability based on web host categories, IP addresses, CA status, destination TCP port and other network parameters • Host Categorization-based policies utilize and sync with the Symantec Global Intelligent Network for real-time updates and protection against advanced malware and threats	• Full policy creation and enforcement capabilities with Symantec Intelligent Services • Utilizes Symantec Global Intelligent Network for real time updates, web & traffic categorization and threat risk level assessment
• Detection of all SSL traffic, irrespective of destination port value (application), using deep packet inspection techniques • Provides the clear text of any SSL flow, including HTTPS, SPDY, POP3, IMAP, SMTP, FTP and other protocols that use SSL/TLS.	• Visibility of web traffic only (i.e. HTTPS)
• Standalone, dedicated appliance: SV800, SV1800, SV2800 or SV3800 and SV3800B-20 • Requires OS v3.7 or later for support of Host Categorization-based policies	• Requires existing or new ProxySG appliance • Requires SGOS release v6.5 or later
• Requires an Enterprise Activation license • Requires the 'Host Categorization' subscription-based license for creating policies based on web host categories	• Requires the SSL license (included) • Requires the Encrypted Tap license • A collection system - configured to receive copied or tapped data - is needed for effective operation

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