Symantec Encrypted Tap

Complete Visibility, Compliance, and Logging

Encrypted Tap is an optional feature available for Blue Coat ProxySG and Advanced Secure Gateway appliances that works with SSL Proxy to offer complete visibility into SSL traffic handled by the appliance. A part of Symantec's Advanced Web and Cloud Security solution, Encrypted Tap sends a stream of decrypted traffic to third party logging systems for analysis, archiving, and forensics. By providing SSL visibility and control, Symantec offers a complete SSL web security solution for its ProxySG family of secure web gateway appliances. .

Encrypted Traffic

Use of SSL encryption across the internet is growing. Surveys show that over 50% of enterprise applications such as SharePoint, Exchange, WebEx, SalesForce.com and Google Apps already use SSL, and many social networking and consumer applications likes Facebook and Gmail already allow full time use of SSL. While encrypting the web session protects the data from being viewed in transit over the Internet, it also creates a serious blind spot for threats, malware, DLP, and other regulatory or compliance risks.

As a result, organizations need complete visibility into the SSL network traffic on their Enterprise Networks, and the ability to preserve complete web histories from encrypted web traffic for compliance, regulatory and logging requirements. Symantec offers SSL visibility with Encrypted Tap for ProxySG and Advanced Secure Gateway appliances. Encrypted Tap provides complete visibility of encrypted web traffic for use in logging, forensics, analysis, and is available as an add-on licensing option.

SSL Proxy

Blue Coat ProxySG appliances have the ability to proxy web-based SSL requests. All currently shipping ProxySG and Advanced Secure Gateway appliances include SSL hardware assist and SSL licenses.

SSL Proxy has been an integral part of the ProxySG feature set for years, and includes the ability to selectively inspect attachments for malware, and content for data leakage prevention through the use of policy and third-party integration of anti-malware and DLP offerings over ICAP. SSL Proxy terminates and re-establishes SSL connections and allows the ProxySG to securely send attachments and content for inspection services.

Encrypted Tap builds on the SSL Proxy feature and allows all decrypted content to be transferred to a third-party system for additional analysis, archiving, and forensics.

Capabilities of Blue Coat ProxySG with SSL Proxy and Encrypted Tap

- Eliminates SSL blind spots, so customers gain visibility and control over SSL-encrypted traffic
- Stops rogue applications (e.g., IM and P2P) that use 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
- Halts secured phishing and pharming attacks that use SSL to hide from IT controls or increase the appearance of authenticity
- Accelerates approved and safe SSL-encrypted traffic
- Takes a granular approach to proxying SSL for applications of different trust levels and privacy concerns: pass through, check/verify then pass through, or proxy with full visibility and control

Symantec

- Displays splash screens reminding users of acceptable use, and warns them that monitoring extends to SSL
- Stops information leakage over SSL links through scanning of encrypted traffic for sensitive information

Symantec's SSL proxy functionality provides unprecedented visibility and control of all SSL traffic – both internal and external. Not only is security enhanced, but the user experience is improved. The Symantec solution can also improve overall session performance up to 1,000% by leveraging ProxySG MACH5 acceleration technologies (caching, compression, bandwidth prioritization policies).

All ProxySG appliances are powered by a purpose-built operating system, and can be centrally managed as part of an enterprise-wide solution deployment.

Requirements

- ProxySG or Advanced Secure Gateway (all models)
- Collection system (system configured to receive tapped data)
- For complete security, use a dedicated ProxySG interface on a private network with the collection system
- Minimum SGOS release: 6.5
- SSL License on the ProxySG
- Encrypted Tap License

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.