DATA SHEET

KEY FEATURES

- Provides unmatched visibility into encrypted traffic to protect against advanced threats:
  - Automatically identifies all SSL/TLS traffic, regardless of port number or application
- Supports privacy and compliance initiatives:
  - Selectively decrypts traffic to meet data privacy and compliance requirements
  - Enforces acceptable use policies for encrypted traffic
- Integrates seamlessly with the existing security infrastructure:
  - Preserves and extends the ROI of the infrastructure
  - Supports multiple network segments and can feed active and passive security appliances simultaneously and provide TLS offload for Symantec® ProxySG
- Simplifies management and administration:
  - Delivers detailed logs and alerts to easily spot trends and potential issues with SSL use
  - Integrates with Symantec Management Center for configuration backup, scheduling, and synchronization

SSL Visibility Appliance

Remove Security Blind Spots Created by SSL/TLS Encryption

Introduction

Encryption protects the privacy and integrity of data, but also creates a blind spot that attackers can exploit to evade security controls. Considering over half of all Internet traffic today is encrypted, it creates a rather large gap in an organization's security posture, leading to increased vulnerability and risk, as well as a damaged reputation. The Symantec® SSL Visibility Appliance enables organizations to cost-effectively eliminate blind spots within their environment and maximize the effectiveness of their security infrastructure investments. This technology enables organizations to have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory and acceptable use policies.

Provide Visibility into Encrypted Traffic to Improve Security

The SSL Visibility Appliance is an integral component to any organization's traffic management strategy, providing visibility into encrypted traffic that ensures attacks cannot slip by undetected. The appliance identifies and decrypts all SSL connections and applications across all network ports, and even irregular ports. The decrypted feeds can be used by the existing security infrastructure to strengthen their ability to detect and protect against advanced threats; by offloading process intensive decryption, the SSL Visibility Appliance also helps improve the overall performance of the organization's network and security infrastructure.

Figure 1: SSL Visibility Appliance Hardware

Support Privacy and Compliance Initiatives

The SSL Visibility Appliance serves as an effective policy enforcement point to control SSL traffic throughout the enterprise, reducing risks posed by encrypted traffic, while maintaining compliance with relevant privacy policies and regulatory requirements. Using Host Categorization and SSL traffic types for policies, organizations can easily create and customize granular policies to selectively decrypt traffic to meet their business needs, for example, *do not decrypt financial or banking traffic going out of the business*. Policies can easily be set to control obsolete or weak ciphers and standards, such as traffic using SSL v3.0.

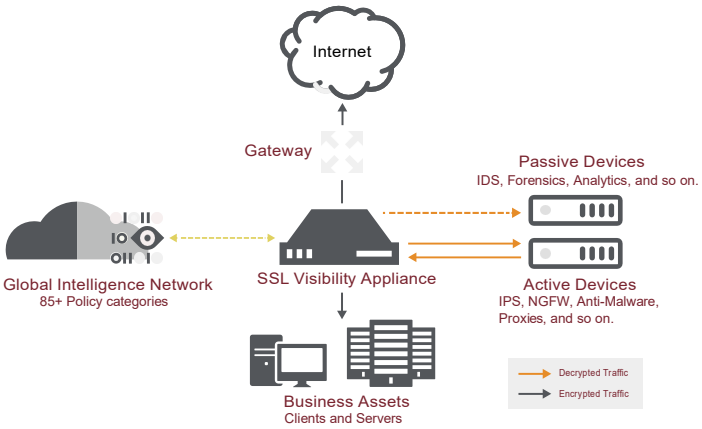
This enables organizations to focus on the communications that represent the highest risks, effectively balancing security with data privacy and compliance requirements. These policies also utilize Symantec Global Intelligence Network to exchange and update SSL host categorization, threat, and malware knowledge across the globe.

Deliver Unmatched Performance and Scale

The SSL Visibility Appliances operate at line-rate, providing visibility into encrypted traffic and potential threats, without hindering device or network performance:

- **Line-rate Network Performance:** Port-to-port latency for non-SSL flows is less than 40 microseconds. Hardware appliances support decryption of up to 25 Gb/s of SSL traffic for all SSL/TLS versions and more than 100 cipher suites.
- **High Connection Rate/Flow Count:** Inspects up to 2,500,000 concurrent SSL sessions and supports the setup and teardown of up to new 24,000 RSA 4K sessions per second.
- **High Availability:** Integrated fail-to-wire/fail-to-open hardware and configurable link state monitoring and mirroring for guaranteed network availability and network security.

Figure 2: Centralized Management of Encrypted Traffic



Integrate Seamlessly with Existing Infrastructure

SSL Visibility Appliances simplify deployment within existing infrastructures; there is no need to duplicate security appliances or re-architect network infrastructure. The appliance provides a suite of features:

- **Improved ROI of Infrastructure:** Enhance the performance and existing capabilities of network and security appliances by offloading decryption and providing visibility into formerly encrypted traffic to help uncover hidden threats.
- **Network Transparency:** Deployment is transparent to end systems and to intermediate network elements. It does not require network reconfiguration, IP address or topology changes, or modifications to client IP and web browser configurations.
- **Flexible Deployment Options:** Support multiple in-line or tap segments that feed one or more active or passive attached appliances; the number of segments supported varies depending on the product model number.
- **Copy Ports:** Send copies to many devices via the additional ports on the device. This allows organizations to feed all decrypted and non-SSL traffic to additional passive devices on the network.
- **Application Preservation:** Deliver decrypted plain-text to security appliances as a generated TCP stream, with packet headers as they were received. This allows applications and appliances, such as next-generation firewalls (NGFW), intrusion detection/prevention systems (IDS/IPS), data loss prevention (DLP) systems, and security analytics to expand scope and provide protection from threats hiding in the previously encrypted traffic. This is done in the attached security tools, without any special software or capabilities. When feeding Symantec ProxySG, the SSL Visibility Appliance must be running software version 4.x or later, and ProxySG must be running software version 6.7.2.x or later.

Figure 3: Active Devices for Segment 1

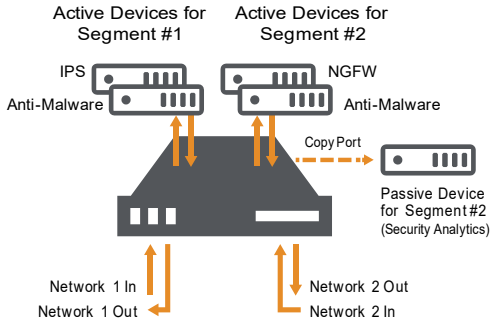
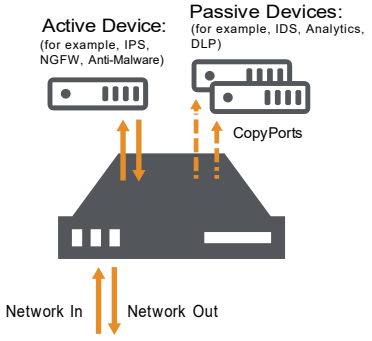


Figure 4: Active Devices for Segment 2



- **Comprehensive Support:** Deliver complete visibility into inbound and outbound SSL sessions; support networks with asymmetric traffic routing; provide support for multiple re-signing Certificate Authorities (CA) when inspecting outbound SSL flows; allow the import of many server key/cert pairs to inspect inbound SSL flows to enterprise SSL servers.
- **Input Aggregation:** Allow the aggregation of traffic from multiple network taps onto a single passive-tap segment for inspection.

Simplify Management and Administration

The SSL Visibility Appliances are simple to configure and manage:

- **Single Device Management:** A powerful, intuitive, SSL-secured, web-based user interface provides configuration and management with Role-based Access Control (RBAC).
- **Centralized Management:** Allows multiple appliances to be administered by Symantec Management Center for inventory and system performance monitoring, health monitoring, configuration backup, and scheduling and configuration synchronization. Management Center also supports RBAC.
- **Email Alerting:** Configure logs to trigger alerts that can be immediately forwarded via email or sent at intervals to designated network administrators.
- **SSL Session Identification:** Provide session logs that detail all SSL flows, inspected or not, allowing suspicious trends or patterns of SSL use to be detected.
- **Syslog Reporting:** Support up to eight remote syslog servers to enable enhanced reporting and logging applications within distributed environments.
- **SNMP Support:** Enables monitoring and management by third-party devices via the SNMP v3 standard.

SSLV Performance in Classic (Non-ProxySG) Mode Only

Software Version	5.5.x			5.4.x		
Product Model	**SSP-S210-10**	**SSP-S410-20B**	**SSP-S410-40B**	**SV-S550-5**	**SV-S550-10**	**SV-S550-20**
Total Packet Processing Capacity (Gb/s)	10	40	70	25	50	100
Classic Segment Inspection Capacity (Gb/s)[a]	2.0	9.6	19.4	5	10	20
Concurrent SSL Flow States	394,920	896,471	1,704,871	1,000,000	1,500,000	2,750,000
Full Handshake EC 256[b]	4161	17,892	19,327	8000	14,000	28,000
Full Handshake RSA 4096	2486	8670	14,003	8000	16,000	23,000
Full Handshake EC 256[c]	3376	15,406	18,680	8500	14,500	27,000
SSL Session Log Entries	80,000,000	80,000,000	160,000,000	250,000,000	250,000,000	250,000,000

a. Testing based on TLS inspected throughput
b. Utilized RSA 2048 cert
c. Utilized ECDSA 256 cert

SSLV Performance for ProxySG Segment

Software Version	SGOS 7.3.4.1					
	5.5.x			5.4.x		
Product Model	**SSP-S210-10 12 Core**	**SSP-S410-20B 32 Core**	**SSP-S410-40B 64 Core**	**SV-S550-5**	**SV-S550-10**	**SV-S550-20**
Total Packet Processing Capacity (Gb/s)	10	40	70	25	50	100
Proxy Segment Inspection Capacity (Gb/s)[a]	1.3	5.1	9.0	5	9	15
Chained Segment Capacity A + B (Gb/s)[a]	0.8	3.9	6.0	4.5	8	12
Concurrent SSL Flow States	197,460	448,236	852,436	550,000	800,000	1,250,000
SSL Session Log Entries	80,000,000	80,000,000	160,000,000	250,000,000	250,000,000	250,000,000

a. Tested with 3 x 34K Proxy transaction size and SSP-S410-40B appliances

Hardware Specifications

Specification	SSP-S210-10[a]	SSP-S410-20B[a]	SSP-S410-40B[a]	SV-S550-5	SV-S550-10	SV-S550-20
Configuration	2 x PCI slots with various 1 Gb/s, 10 Gb/s, and 10/25 Gb/s interface options	4 x PCI slots with various 1 Gb/s, 10 Gb/s, and 10/25 Gb/s interface options	4 x PCI slots with various 1 Gb/s, 10 Gb/s, and 10/25 Gb/s interface options	5 × PCI slots with various 10 Gb/s , 40 Gb/s, and 100 Gb/s interface options	5 × PCI slots with various 10 Gb/s , 40 Gb/s, and 100 Gb/s interface options	5 × PCI slots with various 10 Gb/s , 40 Gb/s, and 100 Gb/s interface options
Power Supply	2 × 300W	2 × 1200W	2 × 1200W	1+1 redundant 1200W	1+1 redundant 1200W	1+1 redundant 1200W
Management Interface	1 × RJ-45 1 GbE copper	1 × RJ-45 1 GbE copper	1 × RJ-45 1 GbE copper	1 × RJ-45	1 × RJ-45	1 × RJ-45
Manageability	SNMP v1, v2c and v3 supported; GETs and TRAPs supported across multiple Symantec MIBs; SETs supported only for the System Group					
Display	—	—	—	LCD 32 × 4 character display	LCD 32 × 4 character display	LCD 32 × 4 character display
Operating Temperature	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)
Storage Temperature	–20°C to 70°C (–4°F to 158°F)	–20°C to 70°C (–4°F to 158°F)	–20°C to 70°C (–4°F to 158°F)	–40°C to 70°C (–40°F to 158°F)	–40°C to 70°C (–40°F to 158°F)	–40°C to 70°C (–40°F to 158°F)
Dimensions H × W × D	9.65 in. × 22.8 in. × 36.42 in.	11.41 in. × 24.01 in. × 39.17 in.	11.41 in. × 24.01 in. × 39.17 in.	1.7 in. × 17 in. × 30 in. (43.5 mm × 438 mm × 759.2 mm)	1.7 in. × 17 in. × 30 in. (43.5 mm × 438 mm × 759.2 mm)	1.7 in. × 17 in. × 30 in. (43.5 mm × 438 mm × 759.2 mm)
Regulatory and Environmental Standards/Compliance	CE (EN55022, EN55024, EN60950), FCC part 15 class A, UL60950-1SSL-Visibility-DS104 EN 62368-1:2014 / IEC 62368-1:2014 (Second Edition), UL62368					
Modes of Operation (per network segment)	Passive-Inline, Active-Inline Fail to Network (FTN) and Fail to Appliance (FTA), ProxySG segment					
Visibility Modes	Controlled-client (Re-sign) Mode (In-line Only), Controlled-server (Known-key) Mode A full list of modes is available in the Administrator Guide.					
Encryption	TLS 1.3 (RFC 8446), TLS 1.2, TLS 1.1, TLS 1.0, SSLv3, partial SSLv2					
Public Key Algorithms	RSA, DHE, ECDHE					
Symmetrical Key Algorithms	AES, AES-GCM, AES-CCM, 3DES, DES, RC4, ChaCha20-Poly1305, Camellia					
Hashing Algorithms	MD5, SHA-1, SHA-2, SHA256, SHA384					
RSA Keys	512 bits to 4096 bits					
Software Licensing	A license is required for inspection activation for each appliance. Refer to the licensing section within the Support portal. Host Categorization is an optional, subscription-based service that requires an additional license per appliance.					

a. For more detailed information see the SSP product brief: docs.broadcom.com/docs/secure-web-gateway-appliances.

BROADCOM
connecting everything®

For more information, visit our website at: www.broadcom.com

SSL-Visibility-DS108 July 16, 2025