Symantec
A Division of Broadcom

Data Sheet

Symantec® SSL Visibility Appliance

Remove Security Blind Spots Created by SSL/TLS Encryption

Overview

- 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 ProxySG
- Simplifies management and administration:
  - Delivers detailed logs and alerts to easily spot trends and potential issues with SSL use
  - Integrates with Management Center for configuration backup, scheduling and synchronization

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, a key component of the Encrypted Traffic Management solution set, enables organizations to cost-effectively eliminate blind spots within their environment and maximize the effectiveness of their security infrastructure investments. With Symantec technology, organizations 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. Broadcom identifies and decrypts all SSL connections and applications across all network ports (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.

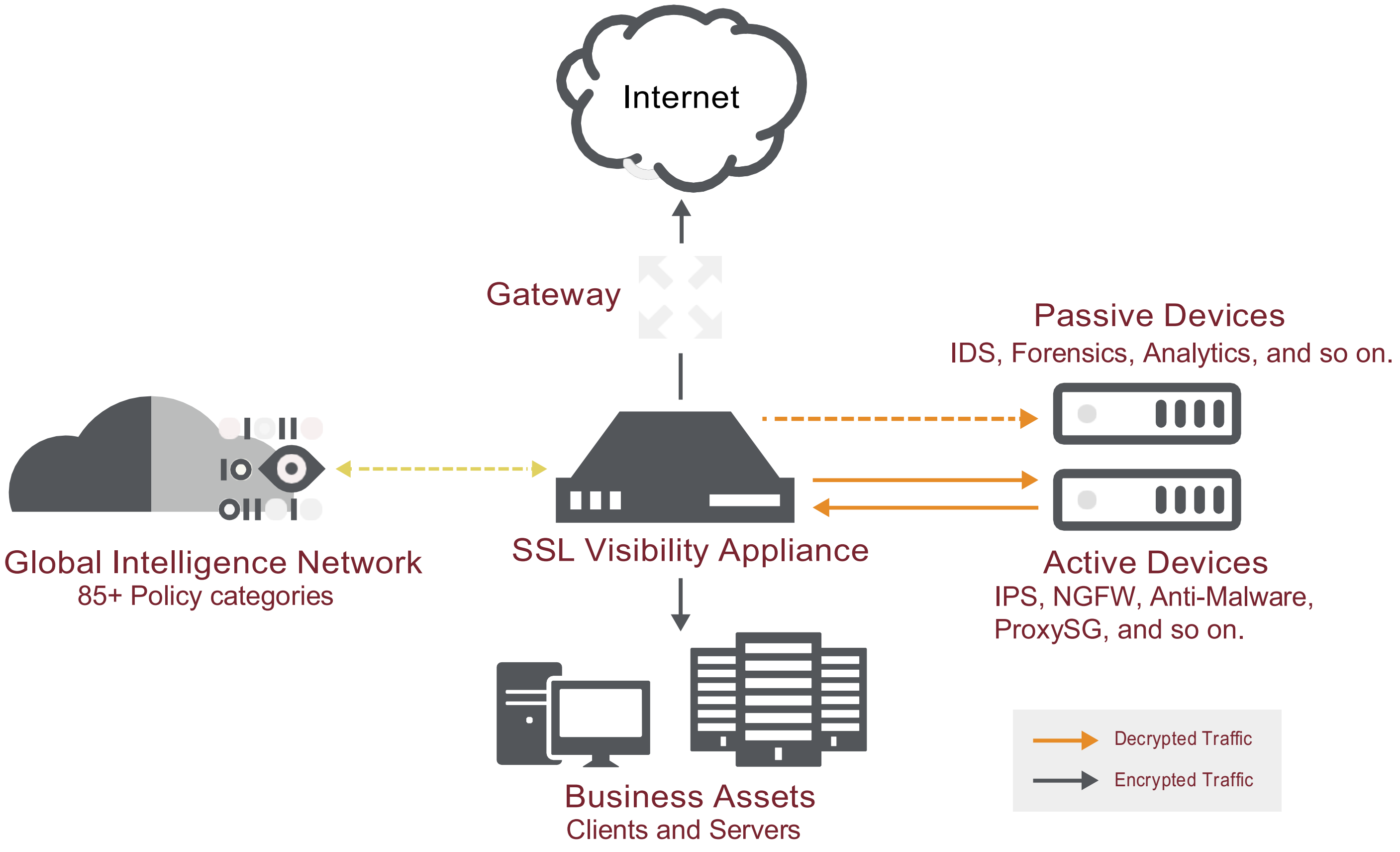
This enables organizations to focus on the communications that represent the highest risks effectively balancing security with data privacy and compliance requirements. These policies also utilize Symantec market-leading Global Intelligence Network to exchange and update SSL host categorization, threat 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. The appliances provide:

- 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: inspecting up to 2,500,000 concurrent SSL sessions and supporting the setup and teardown of up to new 24,000 RSA 4K sessions per second.
- High Availability: offering integrated fail-to-wire/fail-to-open hardware and configurable link state monitoring and mirroring for guaranteed network availability and network security.

Figure 2: Symantec SSL Visibility Appliance Helps Centralize the Management of Encrypted Traffic

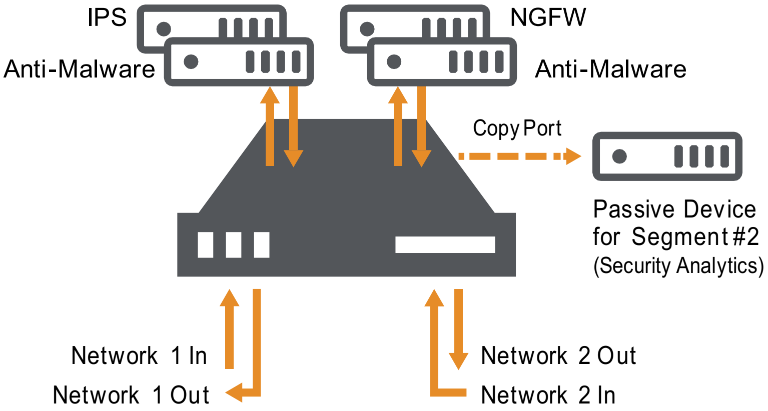


Integrate Seamlessly with Existing Infrastructure

The SSL Visibility Appliances are simple to deploy within your existing infrastructure; there is no need to duplicate security appliances or re-architect the network infrastructure. Hardware and Virtual Appliances provide:

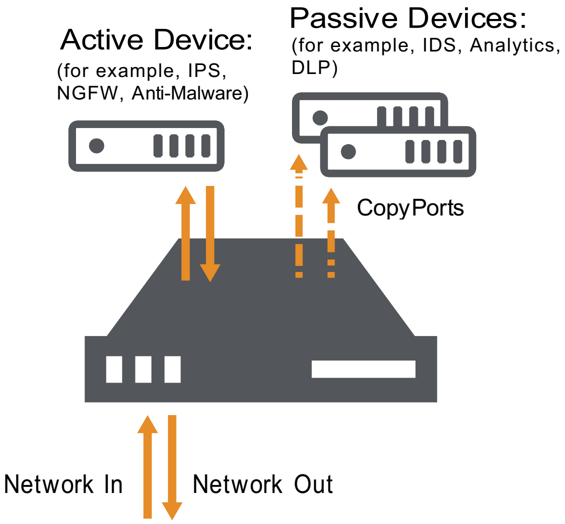
- Improved ROI of Infrastructure: enhancing the performance and existing capabilities of network and security appliances, by offloading the decryption and providing visibility into formerly encrypted traffic to help uncover hidden threats.
- Network Transparency: deploying the SSL Visibility Appliance 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.

Figure 3: Active Devices for Segment 1



- Flexible Deployment Options: supporting multiple in-line or tap segments that feed one or more active or passive attached appliances (the number of segments supported varies depending on model number).

Figure 4: Active Devices for Segment 2


Active Device:
(for example, IPS, NGFW, Anti-Malware)
Passive Devices:
(for example, IDS, Analytics, DLP)
Copy Ports
Network In
Network Out

- Copy Ports: the SSL Visibility Appliance can send copies out to many devices over the additional ports on the device. This allows organizations to feed all traffic (decrypted and non- SSL) to additional passive devices on the network.
- Application Preservation: delivering decrypted plain-text to security appliances as a generated TCP stream, with the 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 their scope and provide protection from threats hiding in the previously encrypted traffic. This is done without requiring any special software or capabilities in the attached security tools. When feeding ProxySG the SSL Visibility Appliance must be running a 4.x or later software release and ProxySG must be running 6.7.2.x or later software.
- Comprehensive Support: delivering complete visibility into inbound and outbound SSL sessions; supporting networks with asymmetric traffic routing; providing support for multiple re- signing Certificate Authorities (CA) when inspecting outbound SSL flows; allowing the import of many server key/ cert pairs to inspect inbound SSL flows to enterprise SSL servers.
- Input Aggregation: allowing 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, providing:

- Single Device Management: offering a powerful, SSL-secured, simple-to-use, web-based user interface (UI) for configuration and management with Role-based Access Control (RBAC).
- Centralized Management: allowing administration of 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: configuring logs to trigger alerts that can be immediately forwarded via email or sent at intervals to designated network administrators.
- SSL Session Identification: providing session logs that detail all SSL flows, inspected or not, allowing suspicious trends or patterns of SSL use to be detected.
- Syslog Reporting: supporting up to 8 remote syslog servers to enable enhanced reporting and logging applications within distributed environments.
- SNMP Support: Enables monitoring and management by 3rd party devices via the SNMP v3 standard.

Table 1: SSLV Performance in Classic (Non-ProxySG) Mode Only

Software Version	**4.5.x**				**5.2.x**
Product Model	**SV1800B-C/F**	**SV2800B**	**SV3800B**	**SV3800B-20**	**SV-S550-20**
Total Packet Processing Capacity (Gb/s)	8	20	40	40	100
Classic segment Inspection capacity (Gb/s)	2.0	4.5	7.5	9.0	20
Concurrent SSL Flow States	100,000	200,000	500,000	900,000	2,500,000
New Full Handshake RSA 2048 bit	4,500	6,000	9,000	12,000	28,000
New Full Handshake RSA 4096 bit	Not Tested	Not Tested	Not Tested	600	24,000
New Full Handshake ECDHE 256	4,000	6,000	8,000	14,000	25,000
SSL Session Log Entries	32,000,000	32,000,000	32,000,000	32,000,000	250,000,000

Table 2: SSLV Performance for ProxySG Segment

Software Version	**4.5.x SGOS 6.7.4.4**				**5.2.x SGOS 7.2.3.2**
Product Model	**SV1800B-C/F**	**SV2800B**	**SV3800B**	**SV3800B-20**	**SV-S550-20**
Total Packet Processing Capacity (Gb/s)	8	20	40	40	100
Proxy segment Inspection capacity (Gb/s)	1.8	3.5	4.4	7.0	9.0
Chained Segment Capacity A + B (Gb/s)	NA	2.2	2.6	4.0	7.88
Concurrent SSL Flow States	50,000	100,000	250,000	450,000	2,500,000
New Full Handshake RSA 2048 bit	4,500	6,000	9,000	12,000	28,000
New Full Handshake ECDHE 256	4,000	6,000	8,000	14,000	25,000
SSL Session Log Entries	32,000,000	32,000,000	32,000,000	32,000,000	250,000,000

Hardware Specifications

Specifications	**SV1800B**	**SV2800B**	**SV3800B**	**SV3800-B20**	**SV-S550-20**
Configurations	Fixed 8x 1 Gb/s Copper or 8x 1 Gb/s Fiber (SX)	3x Netmod Slots Various 1 Gb/s and 10 Gb/s Interface Options	7x Netmod Slots Various 1 Gb/s and 10 Gb/s Interface Options	7x Netmod Slots Various 1 Gb/s and 10 Gb/s Interface Options	5x PCI Slots Various 10 Gb/s, 40 Gb/s, and 100 Gb/s Interface Options
Power Supplies	1+1 Redundant 450W	1+1 Redundant 450W	1+1 Redundant 750W	1+1 Redundant 750W	1+1 Redundant 1200W
Management Interfaces	1 x RJ-45	1 x RJ-45	1 x RJ-45	1 x RJ-45	1 x 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 16 x 2 Char. Display	LCD 16 x 2 Char. Display	LCD 16 x 2 Char. Display	LCD 16 x 2 Char. Display	LCD 32 x 4 Char. Display
Operating Temperature	5°C to 40°C	10°C to 35°C	10°C to 35°C	10°C to 35°C	0°C to 40°C
Storage Temperature	–10°C to 60°C	–10°C to 60°C	–10°C to 60°C	–10°C to 60°C	–40°C to 70°C
Dimensions H x W x D	1.75 x 17 x 20 in.	1.75 x 17.5 x 29 in.	1.75 x 17.5 x 29 in.	1.75 x 17.5 x 29 in.	1.7 x 17 x 30 in. 43.5 x 438 x 759.2 mm
Regulatory and Environmental Standards / Compliance	CE (EN55022, EN55024, EN60950), FCC part 15 class A, UL60950-1 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 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.				

Symantec™
A Division of Broadcom