

SSL Visibility Appliances SV800/SV1800/SV2800/ SV3800/SV3800B-20

Remove the Security Blind Spots
Created by Encrypted Traffic



At A Glance

Provides Unmatched Visibility into Encrypted Traffic to Protect Against Advanced Threats

- Automatically identifies all SSL/TLS traffic regardless of port number or application
- Uncovers hidden threats that use SSL to bypass detection, such as the Dyre and Zeus trojans, Upatre Command and Control (C&C), VMZeus C&C, etc.
- Leverage state-of-the-art sandboxing to address zero day threats

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

Simplifies Management and Administration

- Delivers detailed logs and alerts to easily spot trends and potential issues with SSL use
- Utilizes Management Center for configuration backup, scheduling and synchronization

Encryption protects the privacy and integrity of data, but also creates a blind spot that attackers can exploit to evade security controls. Considering roughly 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, organizations have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory and acceptable use policies.

Provides 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. Symantec 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.

Supports 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. Utilizing 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 (e.g. “do not encrypt financial or banking traffic going out of the business”). And 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’s market-leading Global Intelligence Network to exchange and update SSL host categorization, threat and malware knowledge across the globe.

Delivers Unmatched Performance and Scale

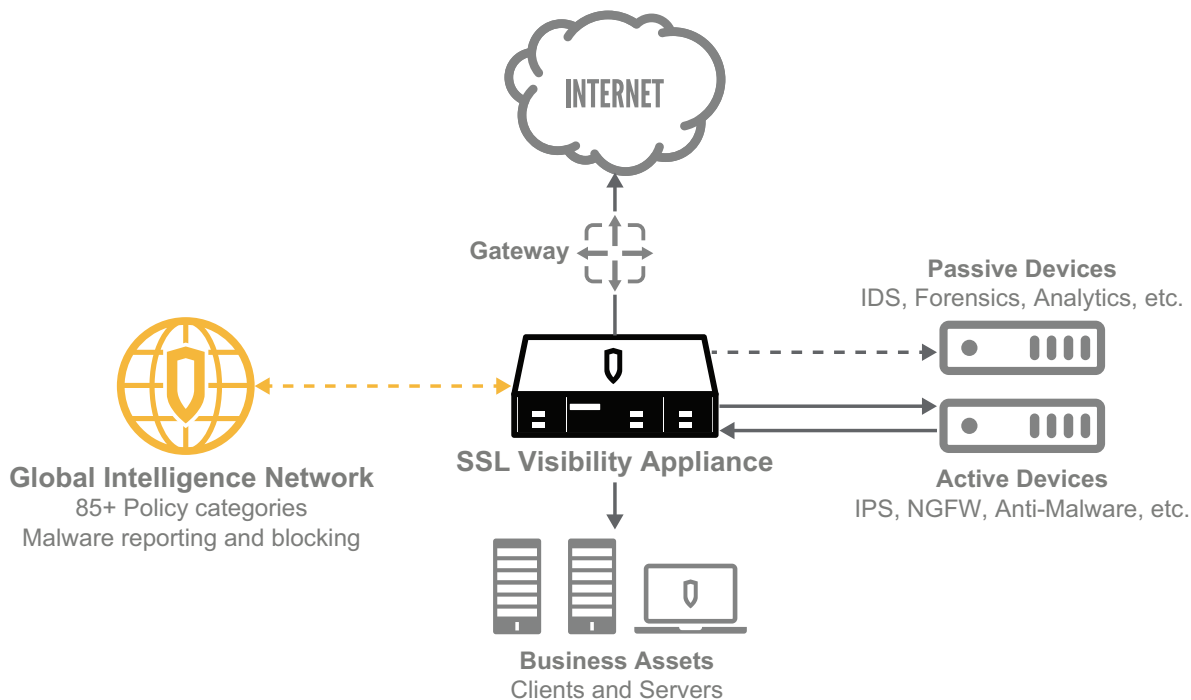
The SSL Visibility Appliances operate at line-rate, providing visibility into encrypted traffic and potential threats, without hindering device or network performance. The Appliances provide:

- **Line-rate Network Performance:** sending non-SSL flows to the attached security appliance(s) or cut-through in less than 40 microseconds to minimize any delay for latency sensitive applications, such as Voice over IP (VoIP). The appliance supports decryption of up to 9 Gbps of SSL traffic for all SSL/TLS versions and over 70 cipher suites.
- **High Connection Rate/Flow Count:** inspecting up to 800,000 concurrent SSL sessions and supporting the teardown and setup of up to 30,000 new 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.

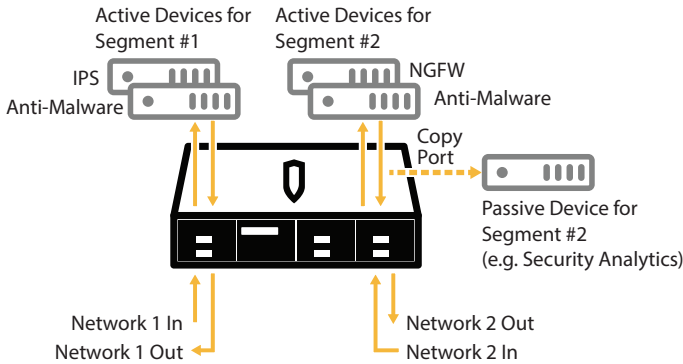
Integrates Seamlessly with Existing Infrastructure

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. The Appliances provide:

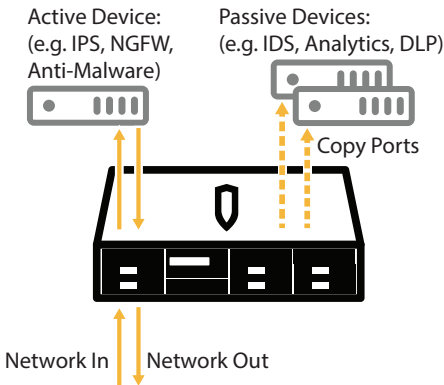
- **Improved ROI of Infrastructure:** enhancing the performance and existing capabilities of network and security appliances, by offloading the decryption and providing visibility into formerly encrypted traffic to help uncover hidden threats.



- **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.



- **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).



- **Copy Ports:** using a unique “Decrypt Once, Feed Many” design, the SSL Visibility Appliance is capable of sending 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 plaintext 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.

- **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 in order 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.

Simplifies 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.
- **Centralized Management:** allowing multiple appliances to be administered via Symantec’s Management Center technology, including inventory and RBAC System performance monitoring, health monitoring, configuration backup and scheduling and configuration synchronization.
- **E-mail 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.

	SV800-250M-C	SV800-500M-C	SV1800-C/-F	SV2800	SV3800	SV3800B-20
PERFORMANCE						
Total Packet Processing Capability	8 Gbps	8 Gbps	8 Gbps	20 Gbps	40 Gbps	40 Gbps
SSL Inspection Throughput	250 Mbps	500 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	9 Gbps
Cut-through Latency	<40µs	<40µs	<40µs	<40µs	<40µs	<40µs
Concurrent SSL Flow States	20,000	20,000	100,000	200,000	400,000	800,000
New Full Handshake SSL Sessions	1,000 per second	2,000 per second	7,500 per second	10,500 per second	12,500 per second	30,000 per second
SSL Session Log Entries	32,000,000	32,000,000	32,000,000	32,000,000	32,000,000	32,000,000
SPECIFICATIONS						
Configurations	Network Interfaces: Fixed 8 x 1 Gbps Copper	Network Interfaces: Fixed 8 x 1 Gbps Copper	Network Interfaces: Fixed 8 x 1 Gbps Copper or 8 x 1 Gbps Fiber (SX)	Network Interfaces: 3 Netmod Slots - Various 1 Gbps and 10 Gbps Interface Options	Network Interfaces: 7 Netmod Slots - Various 1 Gbps and 10 Gbps Interface Options	
Power Supplies	1 x 150W	1 x 150W	1+1 Redundant 450W	1+1 Redundant 650W	1+1 Redundant 750W	
Management Interfaces	1x RJ45	1x RJ45	2 x RJ45	2 x RJ45	2 x RJ45	
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 16 x 2 Char. Display	
Operating Temperature	5°C to 40°C	5°C to 40°C	5°C to 40°C	10°C to 35°C	10°C to 35°C	
Storage Temperature	-10°C to 60°C	-10°C to 60°C	-10°C to 60°C	-10°C to 60°C	-10°C to 60°C	
Dimensions (in.) H x W x D	1.75 x 8 x 12.75	1.75 x 8 x 12.75	1.75 x 17 x 20	1.75 x 17.5 x 29	3.5 x 17.5 x 29	
Regulatory and Environmental Standards/ Compliance	CE (EN55022, EN55024, EN60950), FCC part 15 class A, UL60950-1					
Certifications	None	None	FIPS 140-2 Level 2 for the SV1800, SV2800 SV3800 models; Common Criteria certification in process.			None
Modes of Operation (per network segment)	Passive Tap, Passive In-line, Active In-line (Configurable Fail-to-Wire - FTW), Active In-line (Fail-to-Appliance - FTA)					
Visibility Modes	Controlled-client (Re-sign) Mode [In-line Only], Controlled-server (Known-key) Mode					
Encryption	TLS 1.0, TLS 1.1, TLS 1.2, SSL3, partial SSL2					
Public Key Algorithms	RSA, DHE, ECDHE					
Symmetrical Key Algorithms	AES, AES-GCM, 3DES, DES, RC4, ChaCha20-Poly1305, Camellia					
Hashing Algorithms	MD5, SHA-1, SHA-2, SHA256, SHA384					
RSA Keys	512 to 8192 bits					

SOFTWARE	
Software Licensing	A Symantec License is required for inspection activation for each appliance. Please refer to the Licensing Portal within BlueTouch Online. Host Categorization is an optional, subscription-based service that requires an additional license per appliance, and is available with appliances running v3.7 or later software.

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.

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.
SYMC_ds_SSL_Visibility_SV800-SV1800-SV2800-SV3800_EN_v2a

