BLUE COAT®

Security Empowers Business

DATASHEET

BLUE COAT SSL VISIBILITY APPLIANCES SV800/SV1800/SV2800/SV3800

Remove the Security Visibility Blind Spot Created by Encrypted Traffic

The majority of cyber threats today are hiding in encrypted network traffic. Organizations risk financial loss and damaged reputations if they do not address them. Blue Coat's SSL Visibility Appliance, a key product within its Encrypted Traffic Management solution set, provides the most cost-effective means to eliminate the encrypted traffic blind spot while preserving privacy, policy, compliance and the investment in the security infrastructure.

Enforce Policy to Ensure Data Privacy and Expose Malware

The Blue Coat SSL Visibility Appliance is an integral component to any enterprise SSL encrypted management strategy, by offering complete visibility into encrypted traffic without requiring the duplication of security appliances or re-architecting of network infrastructure. This holistic strategy should address and enforce acceptable use policies for inbound and outbound encrypted traffic, protect against advanced threats, and strengthen existing network security infrastructure; all while adhering to data privacy and compliance demands.

The unique capabilities of the Blue Coat SSL Visibility Appliance help to remove risks arising from lack of visibility into SSL traffic while also increasing the performance of security and network appliances. It is an effective policy-enforcement point for encrypted traffic for organizations of all sizes.

Unmatched Performance and Scale

- **Line-rate Network Performance**: Non-SSL flows will be sent to the attached security appliance(s) or cut-through in less than 40 microseconds, minimizing delay for applications, such as Voice over IP (VoIP). The appliance also supports decryption of up to 4 Gbps of SSL traffic for a variety of SSL versions and cipher suites.
- **Scalable Flow-based Processing**: At up to 40 Gbps, the SSL Visibility appliance supports the analysis of up to 6,000,000 simultaneous TCP flows to check if they contain SSL.
- **High Connection Rate/Flow Count**: The SSL Visibility Appliance supports up to 400,000 concurrently active SSL sessions that are being inspected. The setup and teardown rate of up to 12,500 SSL sessions per second is more than 10x higher than other solutions.
- **High Availability**: Integrated fail-to-wire/fail-to-open hardware and configurable link state monitoring and mirroring for guaranteed network availability and network security.

Extensive Interoperability and Compatibility

- **Extend ROI:** The SSL Visibility Appliance enhances the existing security infrastructure with necessary visibility into formerly encrypted traffic and hidden potential threats without hindering device or network performance.
- **Network Transparency**: Deploying the SSL Visibility Appliance is transparent to end systems and to intermediate network elements and does not require network reconfiguration, IP addressing or topology changes, or modification to client IP and web browser configurations.
- **Flexibility**: Supports both passive and active appliances as well as in-line and tap modes of operation:
  - Inbound and outbound SSL visibility,
  - Support for asymmetrically routed traffic.
- **Application Preservation**: Decrypted plaintext is delivered to security appliances as a generated TCP stream with the packet headers as they were received. This allows applications and appliances, such as NGFW, IDS/IPS, DLP and forensics, to expand their scope and provide protection from previously hidden traffic and potential threats.

BLUE COAT

Security Empowers Business

DATASHEET

- **Input Aggregation**: Allows aggregation of traffic from multiple network taps onto a single passive-tap segment for inspection.
- **Output Mirroring**: Allows the SSL Visibility Appliance to feed traffic to up to two attached passive security appliances in addition to the primary security appliance.

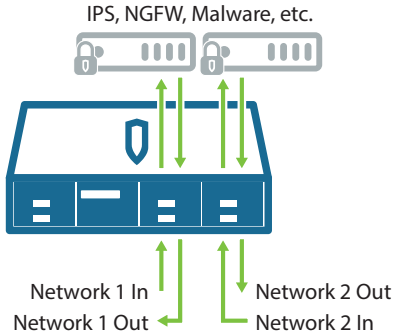
Effective Management and Administration

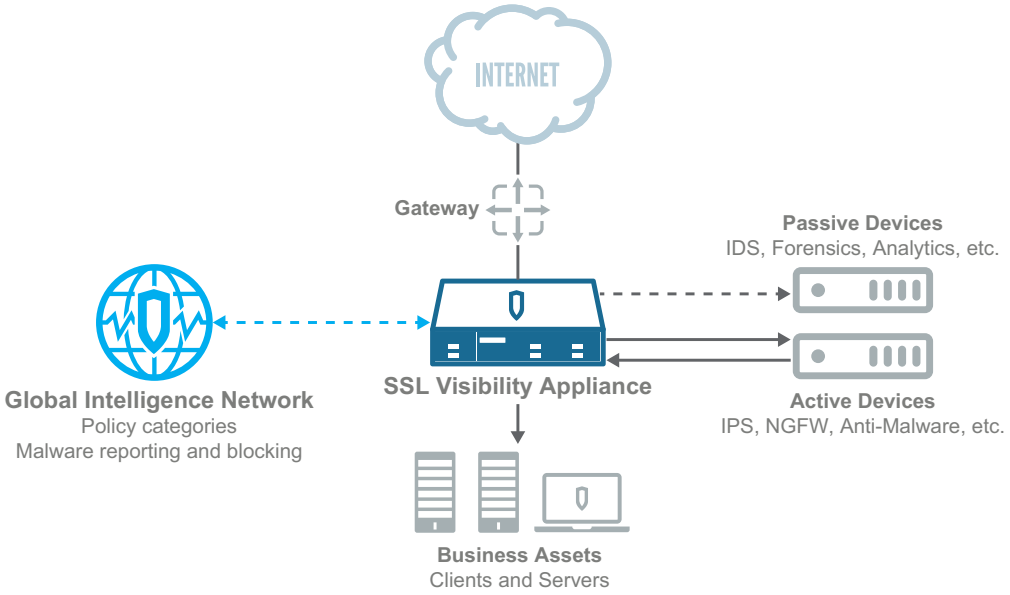
- **Management**: A powerful, SSL-secured, yet simple-to-use, web-based user interface (UI) is provided for configuration and management. Custom web UI and third-party management options are also available for OEM partners.
- **E-mail Alerting**: Logs can be configured to trigger alerts that can be forwarded via email immediately or at intervals to designated network administrators.
- **SSL Session Identification**: The session log provides details of all SSL flows, inspected or not, allowing suspicious trends or patterns of SSL use to be detected.
- **Syslog Reporting**: Up to 8 remote syslog servers are supported to enable enhanced reporting and logging applications within distributed environments.
- **Policy Enforcement**: The appliance acts as an enforcement point to control SSL traffic throughout the enterprise. Utilizing Host Categorization and SSL traffic types for policies, organizations can easily create and customize granular policies to meet their business needs (e.g. "do not encrypt all financial or banking traffic going out of the business"). These policies also utilize Blue Coat's market-leading Global Intelligence Network to exchange and update SSL host categorization, threat and malware knowledge across the globe.

Multiple Segment Support

The SSL Visibility Appliance supports multiple in-line or tap segments that feed one or more active or passive attached appliances. The number of segments varies depending on model number.

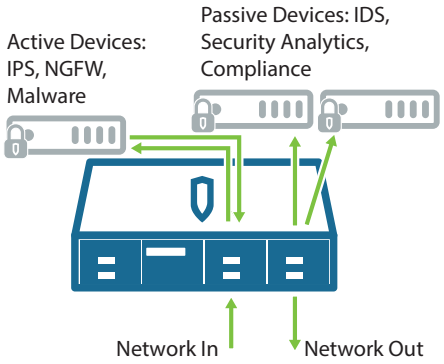
It also provides support for multiple re-signing Certificate Authorities (CAs), as well as server keys, allowing rules based per-flow signatures and keys.





Port Mirroring

With its 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.



	SV800-250M-C	SV800-500M-C	SV1800-C/-F	SV2800	SV3800
PERFORMANCE					
Total Packet Processing Capability	8 Gbps	8 Gbps	8 Gbps	20 Gbps	40 Gbps
SSL Inspection Throughput	250 Mbps	500 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps
Cut-through Latency	<40µs	<40µs	<40µs	<40µs	<40µs
Concurrent SSL Flow States	20,000	20,000	100,000	200,000	400,000
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
SSL Session Log Entries	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 Blue Coat 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	-10C to 60°C	-10C to 60°C	-10C 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.		
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)				
Proxying Modes (per network segment)	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				
RSA Keys	512 to 8192 bits				
SOFTWARE					
Software Licensing	A Blue Coat 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.				

BLUE COAT®

Security Empowers Business

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000