BLUE COAT

Security Empowers Business

BLUE COAT SSL VISIBILITY APPLIANCES
SV1800 / SV2800 / SV3800

GREATER VISIBILITY INTO NETWORK TRAFFIC, HIGHER PERFORMANCE FOR SECURITY APPLICATIONS

A new offering within the Security and Policy Enforcement Center, the Blue Coat SSL Visibility Appliance decrypts multiple streams of SSL content across all network ports to provide intrusion detection and prevention (IDS/IPS), logging, forensics, and data loss prevention. The SSL Visibility Appliance preserves complete network and web traffic histories necessary for compliance, threat analysis, and more. This enables organizations to add SSL inspection capabilities to their network security architecture and close the security loophole created by SSL; it also allows network appliance manufacturers to provide their security applications with visibility into both SSL and non-SSL network traffic and increase their applications' performance.

Features and Benefits

The unique capabilities of the Blue Coat SSL Visiblity Appliance helps to remove risks arising from lack of visibility into SSL traffic while also increasing the performance of security and network appliances.

- **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 VoIP.
  › 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 11,500 SSL sessions per second is more than 10x higher than other solutions.

- **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.
- **Application Preservation**: Intercepted 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 IDS, IPS, forensics and data loss prevention, to expand their scope to provide benefits for SSL-encrypted traffic.
- **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.
- **Management**: Powerful web UI management interface. Custom web UI and third-party management options for OEMs.
- **High Availability**: Integrated fail-to-wire/ fail-to-open hardware and configurable link

state monitoring and mirroring for guaranteed network availability and network security.
- **FIPS 140-2 Level 2 Certification**: Versions of the product that are certified to FIPS 140-2 Level 2 will be available. (In process)
- **Flexibility**: Supports both passive and active appliances.
  › In-line and Tap modes of operation
  › Inbound and outbound SSL visibility
  › Support for asymmetrically routed traffic
- **SSL Policy Enforcement**: Provides a single point to control usage of SSL throughout the enterprise.
- **Web-based Management**: The SSL Visibility Appliance is configured and managed via an SSL-secured, web-based graphical user interface, keeping administration simple.
- **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.

BLUE COAT

Multiple Segment Support

Supports multiple in-line or tap segments that feed one or more active or passive attached appliances. Number of segments varies depending on model number.
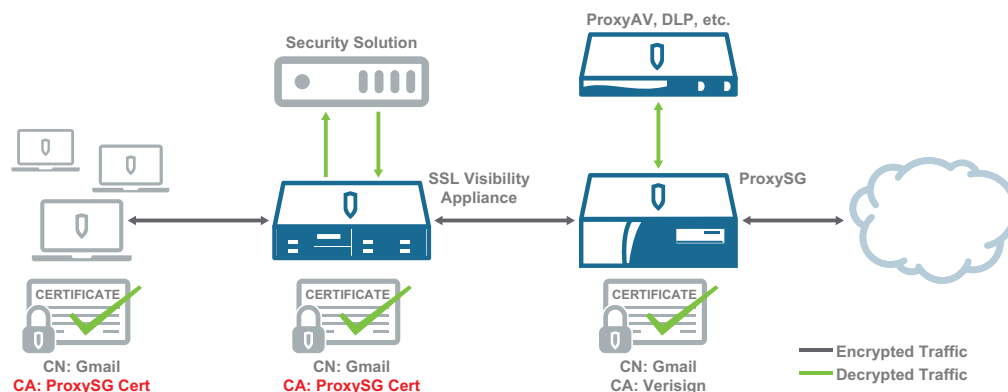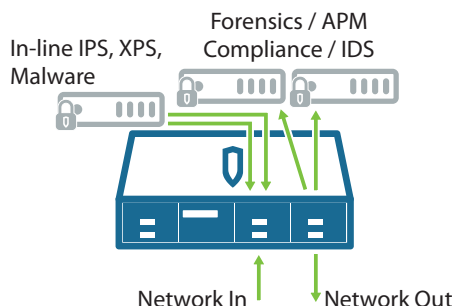
Support for multiple re-signing CAs, as well as server keys, allowing rules based per-flow signatures and keys.

Network 1 In   Network 2 Out
Network 1 Out   Network 2 In
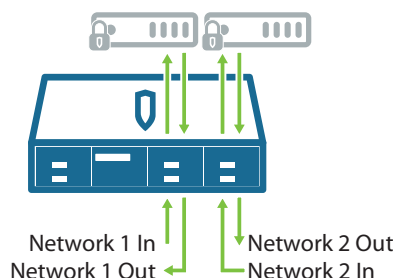
Port Mirroring
Decrypt once, feed many

Capable of sending copies out to many devices over the additional ports on the SSL Visibility Appliances. This allows you to feed all traffic (decrypted and non-SSL) to additional passive devices on the network.

In-line IPS, XPS, Malware

Forensics / APM Compliance / IDS

Network In   Network Out

Security Solution

ProxyAV, DLP, etc.

SSL Visibility Appliance

ProxySG

CN: Gmail
CA: ProxySG Cert

CN: Gmail
CA: ProxySG Cert

CN: Gmail
CA: Verisign

— Encrypted Traffic
— Decrypted Traffic

	SV1800	SV2800	SV3800
PERFORMANCE			
Total Throughput	4 Gbps (line rate)	20 Gbps (line rate)	40 Gbps
SSL Inspection Throughput	1.5 Gbps	2 Gbps	4 Gbps
Cut-through Latency	<40µs	<40µs	<40µs
Concurrent SSL Flow States	100,000	200,000	400,000
SSL Flow Setups/Teardowns	6,500 per second	9.500 per second	11,500 per second
SSL Session Log Entries	50,000,0000	50,000,0000	50,000,0000
SPECIFICATIONS			
Configurations	Network Interfaces: Fixed 8 x 1 Copper or 8 x 1 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+1 Redundant 450W	1+1 Redundant 650W	1+1 Redundant 750W
Management Interfaces	2 x RJ45	2 x RJ45	2 x RJ45
Display	LCD 20 x 2 Char. Display	LCD 20 x 2 Char. Display	LCD 20 x 2 Char. Display
Operating Temperature	5°-40°C	10°- 35°C	10°-35°C
Storage Temperature	-10-60° C	-10-60° C	-10-60° C
Dimensions (in.) H x W x D	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		
Modes of Operation (per network segment)	Passive Tap, Passive In-line, Active In-line (Fail-to-wire), Active In-line (Fail-to-Appliance)		
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, 3DES, DES, RC4, Camellia		
Hashing Algorithms	MDS, SHA-1, SHA-2		
RSA Keys	512-8192 bits		