Sourcefire SSL Appliance

Strengthen Security with Secure Sockets Layer (SSL) Inspection

The Sourcefire SSL Appliance decrypts SSL traffic at 1Gbps line rate to enable existing security appliances to effectively inspect SSL traffic. The SSL Appliance operates transparently on the network and supports both passive and inline network configurations.

Surveys show 25-35% of enterprise traffic is SSL-encrypted, and this number is up to 70% for select verticals.

SSL-encrypted communications are an easy vehicle for the following cybersecurity attacks:

- Inbound attacks
- Spam
- Spyware and malware
- Viruses and worms
- Phishing
- Identity theft
- Information leaks

SSL-ENCRYPTED TRAFFIC—AN EASY VEHICLE FOR CYBERSECURITY ATTACKS

SSL-encrypted traffic is exploding due to the enterprise-wide usage of cloud computing, secure e-commerce, Web 2.0 applications, email, and VPNs. Surveys show 25-35% of enterprise traffic is SSL-encrypted, and this number is up to 70% for select verticals. If not managed properly, SSL can leave a hole in any enterprise security architecture. Existing approaches to SSL-encrypted traffic range from passing everything to blocking everything. In some cases, companies deploy host-based Intrusion Prevention Systems (IPS) or install proxy SSL solutions, which can effectively inspect SSL but suffer from bottleneck issues and reduced network performance.

SOURCEFIRE SSL APPLIANCE

Decrypts SSL Traffic at 1Gbps Line Rate

The Sourcefire SSL Appliance decrypts SSL traffic and sends it to existing security and network appliances via dedicated gigabit Ethernet links. This enables existing IPS appliances to identify risks normally hidden by SSL such as regulatory compliance violations, viruses, malware, data loss, and intrusion attempts. Once the SSL traffic has been inspected and approved, the SSL Appliance places the SSL-encrypted traffic back on the network for its final destination—all with minimal latency and without altering SSL packets. Unlike on-box SSL decryption solutions that use shared hardware resources for SSL decryption and IPS inspection, the Sourcefire architecture permits the SSL and IPS processes to run on separate systems, offloading all decryption and encryption requirements from the IPS. This provides users with greater IPS performance and scalability.

Operates Transparently on Network

The SSL Appliance is deployed as a transparent proxy and detects SSL sessions on all ports, not just the traditional port 443. It can run as a “bump-in-the-wire” and does not require network configuration, IP addressing or topology changes, or modification to client IP and web browser configurations. Further, transparent SSL proxies see all network traffic, not just SSL, and have the ability to cut-through non-SSL flows. Traditional SSL proxies, by comparison, require IP address configuration and possibly network topology changes to inspect traffic. These SSL proxies are now vulnerable to all attacks just as any other host or network element would be. Also, these proxies often assume that all SSL traffic is directed to port 443 and ignore SSL traffic on other ports.

Security Functions:

- Encryption: TLS 1.0, TLS 1.1, SSL3, partial SSL2
- Proxy Mode: Transparent
- Public Key Algorithms: RSA, DSA, DH
- Symmetric Key Algorithms: AES, 3DES, DES, RC4
- Hashing Algorithms: MD5, SHA-1
- RSA Keys: 512, 1024, 2048, 4096, 8172 bits

Supports Passive and Inline Configurations

The SSL Appliance supports both passive and inline configurations. When deployed passively, it sends traffic to a Sourcefire IPS™ also running in passive mode. Passive deployment is most useful for gaining full visibility into network traffic and what vulnerabilities may be exploited. The SSL Appliance can also be deployed inline as a "bump-in-the-wire" and operate with an IPS running in either passive or inline mode. When both the SSL Appliance and the IPS are deployed inline, they can block malicious exploit traffic. All Sourcefire SSL Appliances ship with fail-open 4-port 1G copper or fiber interfaces. The SSL Appliance is versatile enough to inspect SSL traffic in both inbound and outbound configurations. With inbound SSL inspection, the appliance inspects traffic destined for an enterprise's web servers hosting SSL applications. With outbound SSL inspection, the appliance inspects SSL application traffic destined outside of the enterprise, such as Google Gmail traffic.

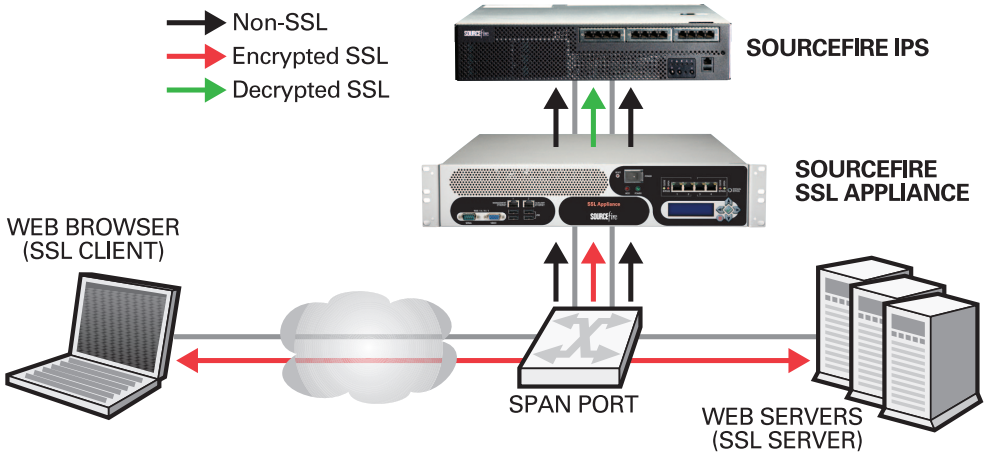

Figure 1. Passive IDS Configuration

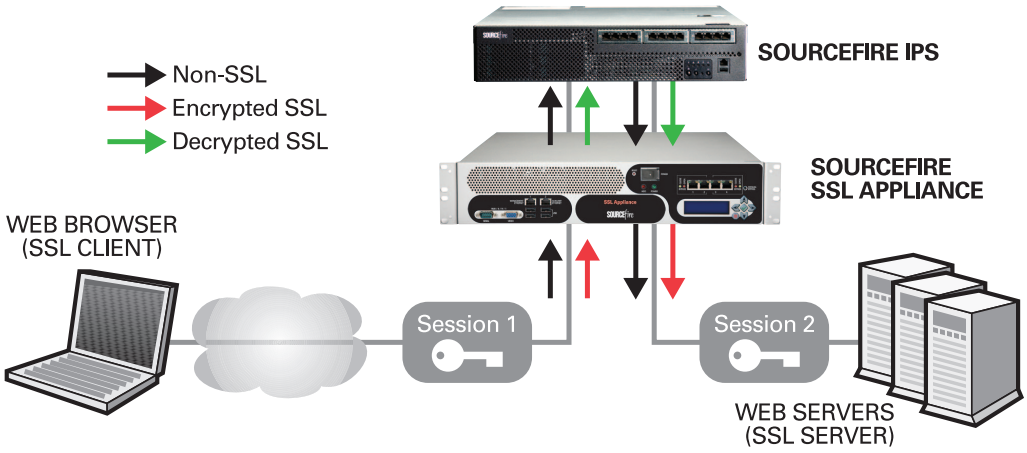

Figure 2. Inline IPS Configuration

UNIQUE CAPABILITIES

The unique capabilities of the Sourcefire SSL Appliance remove risks arising from lack of visibility into SSL traffic while also maintaining the performance of security and network appliances.

- **Scalable Flow-based Processing:** At up to 1Gbps, the Sourcefire SSL Appliance supports the analysis of over 1,000,000 simultaneous flows.
- **High Connection Rate/Flow Count:** The Sourcefire SSL Appliance supports 50,000 concurrent SSL sessions. The setup and teardown rate of 2,900 SSL sessions per second is 10x higher than other solutions.
- **Line-rate Network Performance:**
  - » Non-SSL flows can be sent to the adjacent appliance or cut-through in less than 40 microseconds, minimizing delay for applications such as VoIP.
  - » Supports proxying for up to 1Gbps of SSL traffic for a variety of SSL versions and cipher suites.
- **Network Transparency:** The Sourcefire SSL Appliance can be deployed transparently to both end systems and intermediate networking elements and does not require network configuration, 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 regenerated TCP stream with the packet headers as they were received. This enables applications and appliances, such as Intrusion Detection System (IDS), IPS, Unified Threat Management (UTM), and Data Loss Prevention (DLP), to expand their scope to provide benefits for SSL-encrypted traffic.
- **Flexibility:**
  - » Supports both sniffing/recording devices, such as IDS, and filtering appliances, such as inline firewalls and IPS
  - » Inline and passive modes of operation
  - » Inbound and outbound SSL inspection
- **Policy Configuration:** Fine-grained policy control provides the ability to cut-through non-SSL flows via 7-tuple classification and to control which SSL flows are inspected, passed through or blocked.
- **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.
- **High Availability:** Integrated fail-open hardware, traffic bypass filters, and configurable link state monitoring and mirroring enable guaranteed network availability and network security.
- **Web-based Management:** The Sourcefire SSL Appliance is configured and managed via an SSL-secured web-based graphical user interface, keeping administration simple.
- **Email Alerting:** Logs can be configured to trigger alerts that can be forwarded via email immediately or at intervals to designated network administrators.

To learn more about Sourcefire's award-winning cybersecurity solutions, visit us at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Global Security Alliance today.

Product Specifications:

- Up to 1Gbps throughput for SSL traffic
- Less than 40µs cut-through latency
- 1,000,000 simultaneous flows
- 30,000/second SSL flow inspection rate
- 50,000 concurrent SSL flow states
- 2,900/second SSL flow setups/teardowns
- 32,000 traffic diversion policies
- 10,000,000 SSL session log entries
- 2U rack space height
- Available configurations
  - » 4-port (fail-open) 1G copper
  - » 4-port (fail-open) 1G fiber
- Modes of Operation
  - » Passive IDS
  - » Inline IDS
  - » Inline IPS
  - » Inbound inspection
  - » Outbound inspection

sourcefire.com | snort.org