

NETRONOME SSL INSPECTOR™

TRANSPARENT SSL PROXY APPLIANCE



SSL: Private and Secure Communications for IP Networks

Secure Sockets Layer (SSL)-encrypted communications have enabled a variety of secure, web-based communications, online transactions and VPN services. SSL has become the dominant client-based encryption protocol and now constitutes a significant and growing percentage of the traffic in the enterprise LAN and WAN, as well as throughout service provider networks. The privacy benefits provided by SSL can quickly be overshadowed by the risks it brings to the enterprise. Network-based threats, such as spam, spyware and viruses—not to mention phishing, identity theft, accidental or intentional leakage of confidential information and other forms of cyber crime—have become commonplace. To combat these threats, network security appliances have become standard issue in the enterprise data center. In most instances, though, these sophisticated security devices are blind to the payloads of SSL-encrypted communications, leaving a hole in any enterprise security architecture.

Existing methods to control SSL include severely limiting its use, preventing its use entirely, deploying host-based IPS systems or installing proxy SSL solutions that significantly reduce network performance. In many instances, these methods are successful at examining encrypted SSL, but they typically suffer other major problems that limit their effectiveness.

Netronome SSL Inspector Solution

The Netronome SSL Inspector™ Appliance is the industry's highest-performance transparent proxy for SSL network communications, providing existing sniffing, recording and filtering security appliances with access to the plaintext of SSL-encrypted connections. This provides assurance that common network-based threats are identified within SSL flows that previously could not be examined by installed network and security appliances. The SSL Inspector was designed to provide support for a broad range of target market segments, spanning enterprise deployments at many network locations from the perimeter to the network core.

The SSL Inspector provides industry-leading SSL inspection at a fraction of the cost of other solutions. Without compromising any aspect of enterprise or government-regulated compliance, the SSL Inspector allows network security appliances to be deployed with the highest levels of flow analysis and SSL visibility while still maintaining multi-gigabit, line-rate network performance. The SSL Inspector is the first transparent SSL proxy that both increases network security and significantly minimizes deployment



and operational costs by removing costly user and network configuration.

SSL Inspector Solution Architecture

The Netronome SSL Inspector enables existing security and network appliances to obtain access to the plaintext within SSL-secured flows via dedicated gigabit Ethernet links, thereby extending the benefits of the appliance to SSL-encrypted traffic. At the same time, the SSL Inspector can mirror, firewall or divert non-SSL traffic to the appliance, allowing a single device to deal with both SSL and non-SSL traffic.

Netronome's solutions enable the identification and elimination of risks, such as regulatory compliance violations, viruses/malware, and intrusion attempts normally hidden within SSL. The privacy and integrity of SSL-encrypted communications are maintained by making the plaintext available only within a controlled environment while also exempting certain traffic from inspection based on enterprise policy settings.

Features and Benefits

The Netronome SSL Inspector allows SSL to continue to be used for secure and private communications. Its unique capabilities remove risks arising from lack of visibility into SSL traffic while also increasing the performance of security and network appliances.

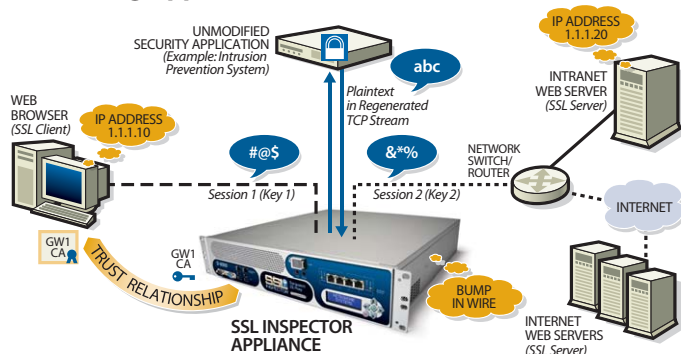
- **Line-rate Network Performance:**
 - Non-SSL flows can be sent to the adjacent appliance or cut-through in less than 40 microseconds by the hardware, minimizing delay for applications, such as VoIP.
 - Supports proxying for up to 1Gbps of SSL traffic for a variety of SSL versions and cipher suites.
- **Scalable Flow-based Processing:** At up to 4Gbps, the Netronome SSL Inspector supports the analysis of over 1,000,000 simultaneous flows.
- **High Connection Rate/Flow Count:** The SSL Inspector supports 50,000 concurrently active SSL sessions. The setup and teardown rate of 2,900 SSL sessions per second is 10x higher than other solutions

The Netronome SSL Inspector Appliance provides existing sniffing (IDS), filtering (IPS) and data loss prevention security appliances with access to the decrypted plaintext of SSL flows. This equips network appliance manufacturers with a mechanism to provide their security applications with visibility into both SSL and non-SSL network traffic and increase their application performance to avoid becoming the source of reduced network throughput. This also allows end-users to add SSL inspection capabilities to their network security architecture immediately to close the security loophole that SSL creates.

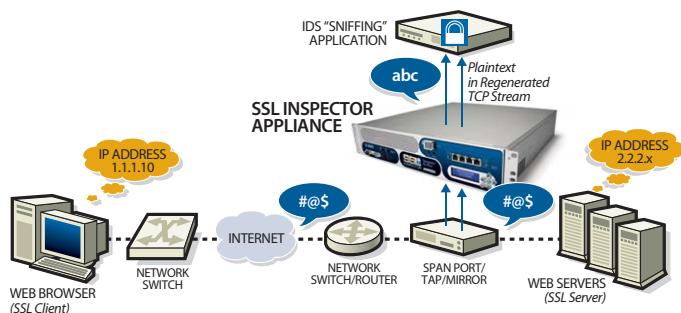
Intelligent
to the Core™

For more information about other Netronome products, please visit netronome.com.

Transparently Decrypting SSL for Existing Applications (In-line Mode)



Transparently Decrypting SSL for Existing Applications (Passive Mode)



- **Network Transparency:** The SSL Inspector 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 allows applications and appliances, such as IDS, IPS, UTM and Data Loss Prevention, to expand their scope to provide benefits for SSL encrypted traffic.
- **Flexibility:**
 - Supports both sniffing/recording devices like Intrusion Detection Systems (IDS) and filtering appliances (such as in-line firewalls) and Intrusion Prevention Systems (IPS).
 - In-line and passive modes of operation
 - Inbound and outbound SSL inspection
- **Policy-based Control:** 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-to-wire/fail-to-open hardware, traffic bypass filters and configurable link state monitoring and mirroring for guaranteed network availability and network security.
- **Web-based Management:** The SSL Inspector 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.

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 bits

Modes of Operation

- IDS Passive Mode
- IDS In-line Mode
- IPS In-line Fail-to-network Mode
- IPS In-line Fail-to-appliance Mode

Proxying Modes

- Controlled-Client (Resign) Mode (in-line only)
- Controlled-Server (Key-Known) Mode

Performance

Throughput 4 Gbps (line-rate)
 Cut-through Latency <40µs
 Total Flows 1,000,000
 SSL Flow Inspection Rate 30,000/sec.
 Concurrent SSL Flow States 50,000
 SSL Flow Setups/Teardowns 2,900/sec.
 Traffic Diversion Policies 32,000
 SSL Session Log Entries 10,000,000

Specifications

Model Number SI-8000
 Netronome Flow Engine NFE-i8000
 Network Ports Four Gigabit Ethernet ports
 Media Types Twisted-pair copper or fiber
 Port Speeds 1000Mbps
 Connectors SFPs—RJ-45 or Duplex LC
 Media 1000 BaseT, CAT 5 or better 1000 Base-SX
 Data Storage 80GB SATA hard drive 32MB compact flash
 Management Interfaces 2 x RJ-45 Gigabit Ethernet
 Power Two 430W redundant power supplies
 High Availability 2x2 Fail-to-wire/fail-to-open card (copper or optical interfaces)
 MTBF 30,000 Hours minimal at 25° C
 Diagnostic LEDs Hard Drive Activity, Power, Fail-to-wire/open, and Link/Activity status LEDs
 Display LED 16 x 2 character display

Environmental

Operating Temperature 0°-40° C
 Storage Temperature -10-70° C

Physical Specifications

Height (inches/mm) 3.5 inches / 88.9 mm (2RU)
 Width (inches/mm) 17.5 inches / 444.5 mm
 Depth (inches/mm) 19.5 inches / 495.3 mm
 Weight (lbs./kg) 29 lbs. / 13.15 kg

Regulatory and Environmental Standards Compliance

CE (EN55022, EN55024, EN60950), FCC part 15 class 2, CSA 22.2 #60950, UL65090-1



Intelligent to the Core.™

Netronome has operations in:
 USA (Pittsburgh [HQ], Santa Clara & Boston), UK (Cambridge), Malaysia (Penang),
 South Africa (Centurion) and China (Shenzhen, Hong Kong)

info@netronome.com 877.638.7629 netronome.com