

NETRONOME SSL INSPECTOR™ TRANSPARENT SSL PROXY SDK

SSL: PRIVATE AND SECURE COMMUNICATIONS FOR IP NETWORKS

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 LANs and WANs, 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.

NETRONOME SSL INSPECTOR SOLUTION

The Netronome SSL Inspector changes this landscape with the introduction of the industry's highest-performance transparent SSL proxy. The Netronome SSL Inspector Appliance, SI-8000 provides 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 inside SSL flows that previously could not be examined by installed network and security appliances.

In addition to offering SSL inspection capabilities by adding an adjacent SI-8000 appliance, network security application and appliance manufacturers can now integrate the functionality of the Netronome SSL Inspector directly into their solutions, creating a single-box offering combining SSL inspection with their security application. The Netronome SSL Inspector Software Development Kit (SDK) is available to network appliance manufacturers, extending the benefits of the SSL Inspector to other platforms. The Netronome SSL Inspector SDK is supported across Netronome's entire family of hardware acceleration solutions, including the Open Appliance Platform™.

The Netronome SSL Inspector SDK is a software package that combines the high-performance data-plane implementation of the Netronome SSL Inspector Appliance with the SSLIA management server and a web-based user interface. This version of the Netronome SSL Inspector operates in a standard Linux/Intel Architecture server environment, with or without Netronome Flow Engine (NFE)-i8000 acceleration hardware. It can quickly and easily be integrated with existing security applications, providing them visibility into the plaintext of SSL-encrypted communications.



The Netronome SSL Inspector SDK provides security and network appliance manufacturers with a way to access the extracted plaintext of SSL-encrypted payloads, thereby extending their application benefits to both SSL and non-SSL network traffic.



FEATURES AND BENEFITS

The Netronome SSL Inspector SDK provides a way for SSL to continue to be used for legitimate secure and private communications while assuring that SSL-encrypted traffic meets enterprise security policies as well as regulatory compliance standards. Its unique combination of capabilities removes the risks arising from the lack of visibility into SSL traffic while simultaneously increasing the performance of security and network appliances.

- **Line-rate Network Performance:** By combining the SSL Inspector SDK with the NFE acceleration hardware, all non-SSL flows can be cut-through the system in hardware in less than 10 microseconds, eliminating unnecessary delay for time-sensitive applications, such as VoIP.
- **Network Transparency:** Unlike existing SSL proxies, the SSL Inspector is completely transparent to both end systems and intermediate networking elements. It does not require network configuration, IP addressing or topology changes, or modification to client IP and web browser configurations.
- **Scalable Flow-based Processing:** At up to 4 gigabits per second, the SSL Inspector supports the analysis of over 1,000,000 simultaneous flows.
- **High Connection Rate:** The SSL Inspector provides more than ten times the setup and teardown rate of other SSL proxy solutions, at over 50,000 non-SSL and 2,500 SSL sessions per second.
- **Application Preservation:** Plaintext generated from inspected SSL flows, as well as non-SSL flows, can be delivered to applications as a regenerated TCP stream, through standard linux network interfaces, or made available through an API. This allows applications, such as IDS, IPS, UTM and HTTP, and WAN load balancing, to expand their scope to also provide benefits for SSL-encrypted traffic.
- **Flexibility:**
 - With support for both sniffing/recording devices like IDS and filtering appliances (such as in-line firewalls) and IPS, the SSL Inspector can offer decrypted SSL content to appliances used in enterprise security architectures.
 - The SSL Inspector supports several proxying modes of operation with regard to SSL client and server locations to provide inspection of both inbound SSL connections destined to SSL servers and outbound client SSL traffic.

- **Policy-based Control:** Fine-grained policy control provides the ability to cut-through non-SSL flows via 7-tuple classification and allow valid or acceptable uses of SSL encryption that should not be decrypted.
- **SSL Session Identification:** SSL session Log is a database detailing the SSL flows through the system so certain trends or patterns and suspicious SSL use can be identified.
- **Web-based Management:** The SSL Inspector is configured and managed via an SSL-secured web-based graphical user interface, keeping administration simple.
- **Open Application Programming Interface:** Netronome's solution is the only probe with API programmability that provides a simple way to integrate SSL inspection capabilities into new applications. The SSL Inspector can also be used with existing unmodified applications.
- **Multiple Interface Support:** Applications can access the plaintext version of SSL streams through Netronome's zero-copy API or via standard Linux networking interfaces, such as Virtual Network Interface Cards (VNICs).

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

PERFORMANCE

Throughput..... 4 Gbps (line-rate)
SSL Throughput..... 1 Gbps
Total Flows..... 1,000,000
Non-SSL Flow Setups/Teardowns Per Second..... 50,000
SSL Flows..... 50,000
SSL Flow Setups/Teardowns Per Second..... 2,500
Latency..... <40µs

SUPPORTED HOST PLATFORMS

The Netronome SSL Inspector is supported across a wide range of server motherboards, including those from leading manufacturers, such as Intel, Dell™, HP, AMD and other compatible systems. Please contact Netronome for a current list of supported host platforms.

SUPPORTED HOST OPERATING SYSTEMS

The Netronome SSL Inspector is supported in all leading Linux environments, including Fedora, CentOS, and Gentoo in both 32- and 64-bit variants. Please contact Netronome for a current list of supported operating systems and versions.

SUPPORTED ACCELERATION CARDS (OPTIONAL)

Netronome Flow Engine NFE-i4010, NFE-i8000

TM Netronome, the Netronome Logo, "Total Performance. Total Control.", Netronome SSL Inspector, the Netronome SSL Inspector Logo and Open Appliance Platform are trademarks of Netronome Systems, Inc.

All other trademarks are the property of their respective owners.

© 2008 Netronome Systems, Inc. All rights reserved.

Specifications are subject to change without notice. (3-08)



Total Performance. Total Control.™

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
+1 877 NETRO A-Z
netronome.com