

Netronome SSL Inspector Appliance Prevents Blind Spots

Security and compliance without compromise

Encrypted traffic is exploding and as an integral part of cloud computing, it is often used to secure e-commerce, Web 2.0 applications, email, and VPN. This ever-increasing secure sockets layer (SSL) traffic has resulted in an ever-increasing number of new threats and potential problems for network security. Netronome SSL Inspector Appliance provides McAfee® intrusion prevention system, data loss prevention (DLP), email and web security, firewall, and data protection offerings with access to decrypted SSL traffic, allowing the network and security services to be performed on what has arguably become one of the largest security threats to a network.

McAfee Compatible Solution

Netronome SSL Inspector Appliance and McAfee intrusion prevention system, data loss prevention (DLP), email and web security, firewall, and data protection offerings

Benefits of the joint solution

- Visibility into decrypted SSL traffic
- Elimination of network traffic blind spots
- Improved functionality of security services by addressing potential threats hidden within encrypted SSL traffic
- Greater DLP effectiveness by eliminating the potential of data loss through SSL communications
- Line-rate speeds to avoid any potential network bottleneck
- Increased security by providing the enterprise with decrypted SSL traffic for logging and forensics
- Provides clients with the ability to deploy SSL policy enforcement
- Eliminates the client's exposure to untrusted SSL servers and certificates
- Increased assurance of compliancy adherence with the elimination of "blind" network traffic

The Benefits and Risks of SSL

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.

Everyday applications—such as Microsoft SharePoint, Salesforce.com, SAP, Oracle, WebEx, Google business applications, instant messaging, and social media sites—all utilize SSL. However, 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, as well as phishing, identity theft, accidental or intentional leakage of confidential information, and other forms of cybercrime—have become commonplace. Network security appliances designed to mitigate these threats are typically blind to the payloads of SSL-encrypted communications and cannot inspect these flows at network speeds, potentially leaving a hole in an enterprise's security architecture.

Achieve security without compromising performance

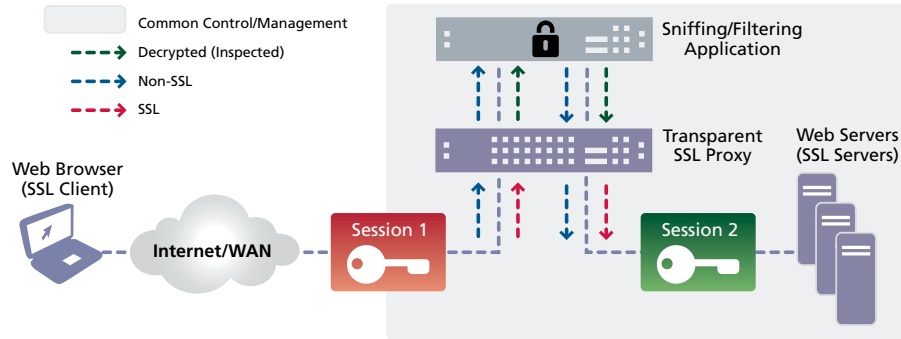
Netronome SSL Inspector Appliance and McAfee provide industry-leading security solutions without network performance compromise. The Netronome SSL Inspector Appliance provides McAfee solutions with the visibility of decrypted SSL traffic, allowing the services to be performed at line-rate network speeds, preventing the security service from becoming a bottleneck in the client's network. The Netronome SSL Inspector Appliance provides McAfee-based solutions with 1 Gbps of inspected traffic, supporting 50,000 concurrent active SSL sessions and 2,900 SSL sessions per second.

Don't be blind to SSL-encrypted communications

Network security appliances are blind to the payloads of SSL-encrypted communications. 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. These methods are successful at examining encrypted SSL but typically suffer other major problems that limit their effectiveness.

The Netronome SSL Inspector Appliance is among the industry's highest-performance transparent proxy for SSL network communications, allowing network security appliances to be deployed while still maintaining multigigabit, line-rate network performance.

Inbound (Outside-In) SSL Inspection—Controlled-Server Mode



"[Netronome] SSL Inspector has the most comprehensive feature set and the best overall performance of any of its competitors.

What we didn't like: nothing. This is the best of breed for this type of product."

—SC Magazine Review of Netronome's SSL Inspector November 1, 2010

Outbound (Inside-Out) SSL Inspection—Controlled-Client Mode

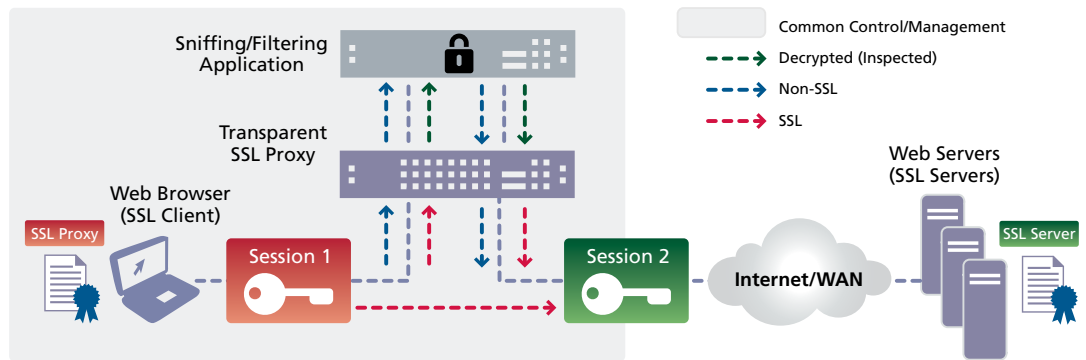


Figure 1. Typical deployment scenarios.

SSL Policy Enforcement

As a standalone solution, the Netronome SSL Inspector Appliance provides an in-line point where SSL can be inspected, allowing the same device to enforce policy on all SSL traffic. These policies can be enforced even when the SSL traffic is not being inspected, and the policies can reject sessions based on information within the SSL certificate and SSL flows. The appliance supports detection of invalid certificates allowing the compromised SSL traffic to be blocked. This eliminates the client's exposure to untrusted SSL servers and certificates.

About Netronome

Netronome is a leading developer of highly programmable semiconductor products that are used for intelligent flow processing in network and communications devices. Netronome's solutions include network flow processors and acceleration cards that scale from 10 to 100 Gbps. They are used in carrier-grade and enterprise-class communications products that require deep packet inspection, flow analysis, content processing, virtualization, and security. Netronome's products are developed in labs in Santa Clara, CA, Boxborough, MA, and Pittsburgh, PA. To learn more, visit www.ssl-inspector.com.

