NETRONOME

PRODUCT BRIEF

SSL and SSH Visibility

TRANSPARENT SSL/SSH PROXY AS SMARTNIC OR APPLIANCE

Pervasive Adoption of SSL and TLS

SSL has become the dominant stream-oriented 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. It has proven popular as it is easily deployed by software vendors, while offering privacy and integrity protection.

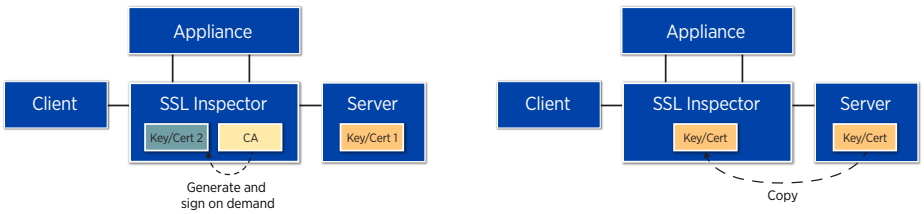
The privacy benefits provided by SSL can quickly be overshadowed by the risks it brings to enterprises. Network-based threats, such as spam, spyware and viruses - not to mention phishing, identity theft, accidental or intentional leakage of confidential information and other forms of cyber crime - have become commonplace. Network security appliances, though, are often blind to the payloads of SSL-encrypted communications and cannot inspect this traffic, leaving a hole in any enterprise security architecture.

Existing methods to control SSL include limiting or preventing its use, preventing its use entirely, deploying host-based IPS systems or installing proxy SSL solutions that significantly reduce network performance.

Netronome SSL and SSH Visibility Technology

Netronome's SSL and SSH Visibility technology enables standard unmodified software and appliances to inspect the contents of SSL while not compromising the use of SSL or reducing performance. The technology is available as software running on standard x86/Arm servers, as SmartNICs designed to be deployed in standard servers, and as appliances that are deployed as traffic decrypting front-ends attached to inline or passive security/monitoring appliances.

Keys can be imported from your servers. Certificates can also be re-signed, thereby supporting servers owned or controlled by third parties.



SSL/SSH Visibility

KEY FEATURES

- Decrypts SSH, SSL 3, TLS 1.0, 1.1, 1.2 and 1.3
- Unmodified attached software and appliances gain visibility into SSL traffic
- Known key and certificate re-signing modes
- Offloads and accelerates SSL processing
- Delivers traffic to software via kernel netdev, DPDK, PCAP or netmap interfaces
- Delivers traffic to physical appliances via dedicated Ethernet links
- Logs sessions and enforces SSL encryption policies
- Low latency cut through of non-SSL traffic
- Web/command line UIs
- REST and C/C++ APIs
- Throughput up to 100Gb/s
- Supports millions of concurrent sessions
- Option to OEM and embed technology in existing virtual or physical appliances

FEATURES	BENEFITS
SSL detection is content-based (TCP port independent)	Supports arbitrary protocols on SSL, (e.g., SMTP/POP3 with STARTTLS, SIPS, FTPS, various chat protocols)
Re-signs CA/self-signed certificates, and imports known server keys	Compatibility with own servers and Internet/third party servers
Leverages SmartNICs and custom SSL stack	Higher performance, lower latency, lower resource usage
Supports latest TLS + SSH versions and encryption algorithms	Excellent compatibility and good security with high performance
Verifies server certificates	No reduction in security
Detailed session log and statistics	Insight into usage of SSL and SSH
Decryption policy rule system	Option to exempt traffic/users from decryption

SPECIFICATIONS	
Form Factors	Software library for 64-bit Linux systems (x86/Arm) NIC with accompanying 64-bit Linux (x86/Arm) software library Physical appliance
Physical Interfaces (NIC/Appliance)	Four 10G/25G (SFP+/SFP28) ports -other media (40G etc.) available on request Direct Attach Cables, copper (1GBASE-T/10GBASE-T) and optical transceivers
Operating Systems	Red Hat Enterprise Linux (RHEL) and CentOS 7.x/8.x, Ubuntu 16.04/18.04
Packet Delivery Interfaces	Physical Ethernet ports Kernel: netdev (including XDP) User mode: DPDK, netmap, PCAP
Management Interfaces	Command line (text dialog) interface, accessible from local console or SSH Web (HTML/Javascript) interface, accessible over HTTPS RESTful API, as plain HTTP JSON API or as OpenAPI/Swagger
Policy Engine	Rules are configured using management user interfaces or APIs Rules match packet (5-tuple) and SSL (certificate and message) fields, e.g. common name, SAN, SNI, ALPN, TLS version, etc. Actions invoked by rules include drop, reject (TCP RST), decrypt, cut through Option for finer grained control via C/C++ callbacks invoked by dataplane
SSL / TLS Versions	SSL 3, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3
Symmetric Algorithms	AES-CBC, AES-GCM, ChaCha20-Poly1305, DES, 3DES, RC4, CAMELLIA
Hashing Algorithms	SHA1, SHA2 (224/256/384/512), MD5
Asymmetric Algorithms	RSA, DSA, DH, DHE, EC (NIST, 25519 and 448 curves)
Key Sizes	AES: 128/256-bit, RSA: up to 8K-bit, EC: up to 448-bit
SSH Versions	SSHv2
SSH Inspection Details	Password authentication, multiple channels (port forwarding/file transfers)

NETRONOME

Netronome Systems, Inc.
2903 Bunker Hill Lane, Suite 150
Santa Clara, CA 95054
Tel: 408.496.0022 | Fax: 408.586.0002
www.netronome.com

PB-SSL-SSH-2/20