CUBRO
NETWORK VISIBILITY
SIMPLE | SCALABLE | SUSTAINABLE

DATA SHEET

Cubro Network Security Series

PRODUCT REVIEW

In order to meet the demands of the operators and fast-developing network, Cubro delivers the network secure sockets layer analysis products – NSA. Focusing on high performance real-time SSL decryption processing, NSA provides common encryption/decryption algorithm and supports SSL3.0/TLS1.0/TLS1.1/TLS1.2. In addition, NSA can restore the TCP data flow of the decrypted data and ensure the session integrity with new TCP sequences.

Functions/Benefits:

- Built-in logical crypto acceleration engine, supporting common hash algorithms, symmetric key ciphers, and asymmetric key operations.
- SSL/TLS supported: SSL3.0, TLS1.0, TLS1.1, TLS1.2.
- Hash algorithms supported: SHA1, MD5, SHA256, SHA224, SHA384, SHA512, AES, HMAC.
- Symmetric key ciphers supported: DES CBC, 3DES CBC, AES-128 CBC, AES-256 CBC, RC4,RC2, IDEA...
- Asymmetric key operations: RSA and ECDH. Note: ECDH decryption is not supported.
- Key management: supporting key self-learning from private key list and binding specified IP address toprivate key.
- Flow restoration: when SSL/TLS is decrypted, NSA can rebuild the packets without SSL/TLS header and calculate TCP sequence and fix TCP/IP checksum.

Network Security
At a glance

Definition

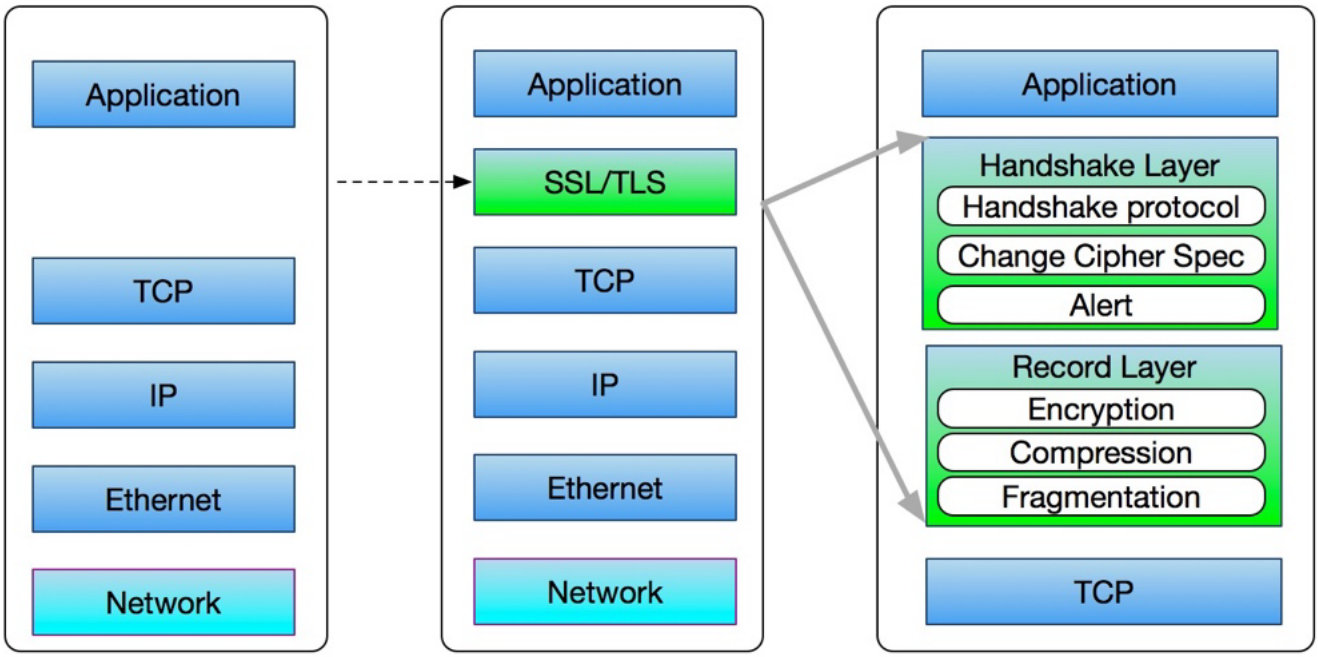
A network securty appliance is a active or passive device which receives Network traffic from TAPs and Packet Brokers or from live links.

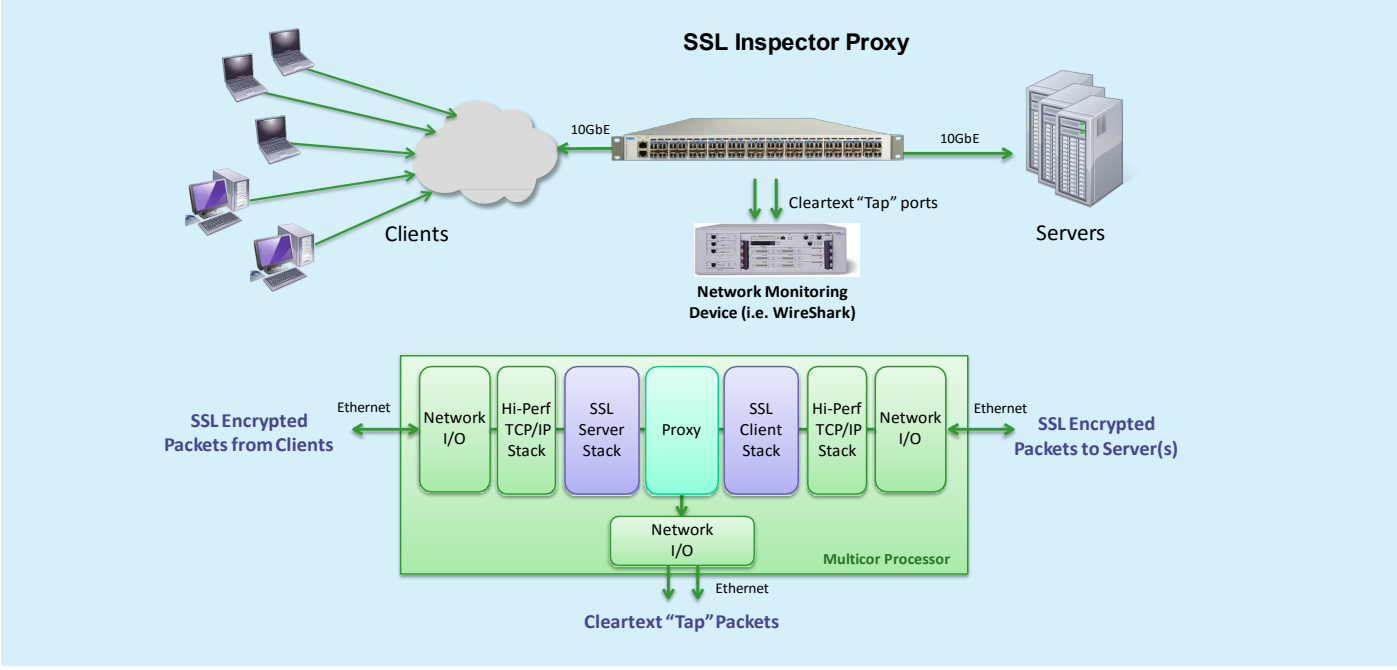
Advantages of Cubro Probe

- Small foot print
- Low power design
- Empedded Network Processor design
- Can be customized to customer's requirement
- Support of any kind of SFP and SFP+ (also 10 Gbit BASE_T),
- 40 x 1/10 Gbit

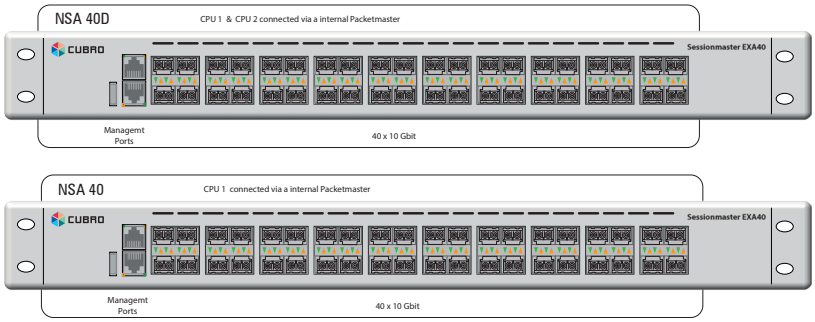
PRODUCT CAPABILITIES / FEATURES

- Packets output: NSA can output encrypted flow and plain flow separately. Optionally, TCP port info can be modified from 443 to 80 as decryption is done.
- Session management: supporting TCP-reassembly such as out-of-order packets, TCP state tracking.
- SSL/TLS session correlating: correlating SSL/TLS sessions with session id or ticket when keys can be reused.
- Performance: decryption performance is 5Gbps with 10 millions of sessions online for NSA40





TECHNICAL DATA / SPECIFICATIONS



Operating specifications:

Operating Temperature: 0°C to 45°C
Storage Temperature: -10°C to 70°C
Relative Humidity: 10% min, 95% max
Non-condensing

Mechanical specifications:

Dimension (HxWxD): W=440.00 mm, L=532 mm, H=44,4 mm
Weight: 9,4 kg

Electrical specifications:

Input Power: 100-240V, 2A, 47-63 Hz
36 - 72 V DC
Maximum Power Consumption: 184 - 270 W

Certifications:

Fully RoHS compliant
CE compliant
Safety - UL 60950-1 / CSA C22.2 60950-1-07 / IEC 60950-1 (2005) EN 60950-1 (2006)

INPUTS*

Several 1, 10 , interfaces can be used as inputs from TAPs or NPB.

On EXA40 and EXA40D a NPB is build in the probe.

OUTPUTS*

Several 1, 10 , interfaces can be used as inputs from TAPs or NPB.

On EXA40 and EXA40D a NPB is build in the Network Security Appliance.

PERFORMANCE

Advanced multi core CPU design

Lowest power usage per Gbit traffic processing in the Industry.

MANAGEMENT

Management Port: (1)
RJ45 10/100/1000 Mbit

Configuration (CLI) Port: (1) RS-232 DB9

USB 3.0 for software update

INDICATORS

Per RJ45 port: Speed, Link/ Activity

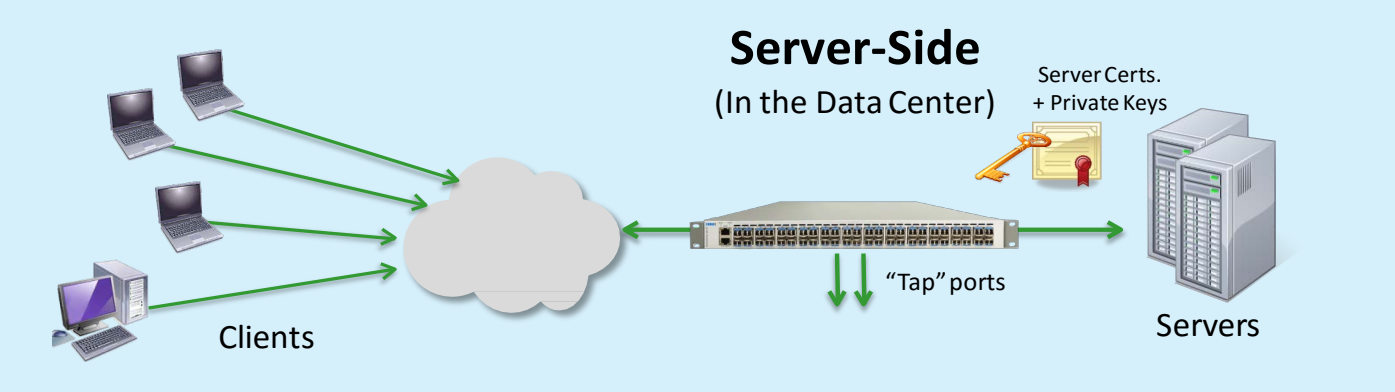
Per SFP+ port: Status, Rx, Tx, Link

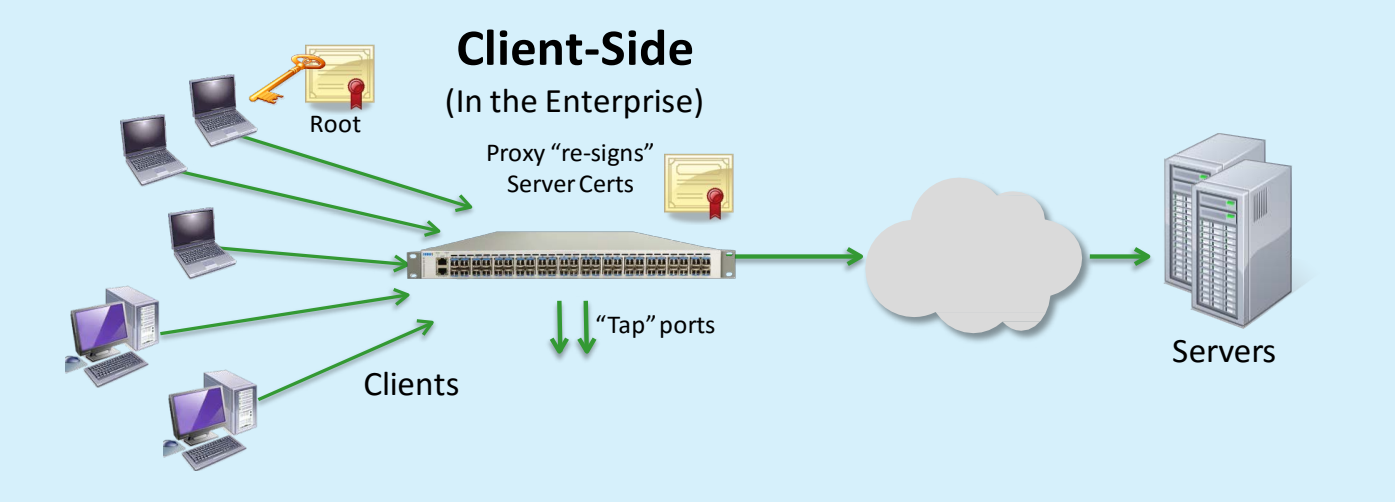
Per Device: Power, Status

AVAILABLE NSA UNITS

Product Type		NSA40	NSA40D
Hardware Specs	Monitoring Ports	40 x 10 Gbit SFP+	40 x 10 Gbit SFP+
	Management Ports	1 x RS 232 RJ45 & 1 x FE RJ45 & USB 2.0	
	Memory	64G DDR3 1333MHz ECC	128G DDR3 1333MHz ECC
	CPU	MIPS 64 32-Core multi-core processor	MIPS 64 64-Core multi-core processor
Performance Specs	Throughput	20Gbps	40Gbps
	Decryption Performance	5Gbps	10Gbps
	Sessions	10M online (maximum)	20M online (maximum)
Decryption Feature	SSL/TLS Protocol	SSL3.0, TLS1.0, TLS1.1, TLS1.2	
	Key Ciphers & Operations	Symmetric: DES CBC, 3DES CBC, AES-128 CBC, AES-256 CBC, RC4, RC2, IDEA, etc. Asymmetric: RSA.	
	Hash Algorithms	SHA1, MD5, SHA256, SHA224, SHA384, SHA512, AES, HMAC	
Monitoring Feature	Packet Preprocessing	IP-reassembly Tunnel identification such as GTP/GRE, supporting protocol processing inside the tunnel	
	Session Management	TCP-reassembly such as out-of-order packets, TCP state tracking Correlating SSL/TLS sessions with session id or ticket	
	Flow Restoration	Rebuilding the packets without SSL/TLS header and calculating TCP sequence and fixing TCP/IP checksum, supporting GTP-U tunnel	

TYPICAL APPLICATION





ORDERING INFORMATION

Product Components:

- Cubro Security Appliance
- AC/DC power supply
- European power cord
- (no SFPs included)

Part Number	Description

For more information please check our website **www.cubro.com**