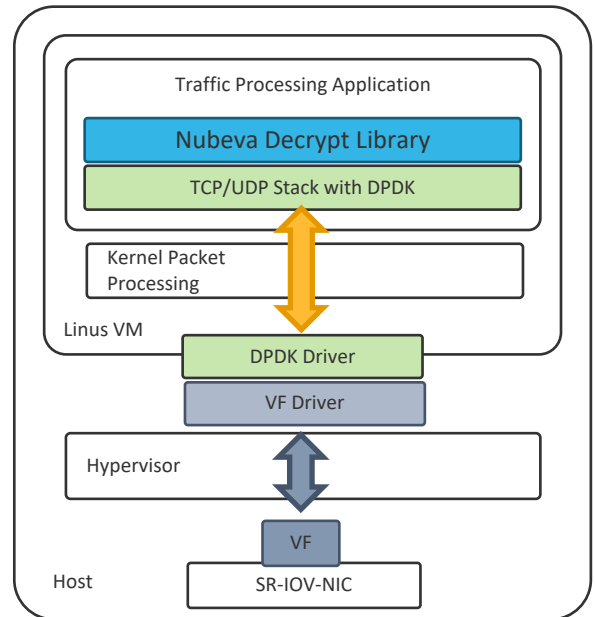
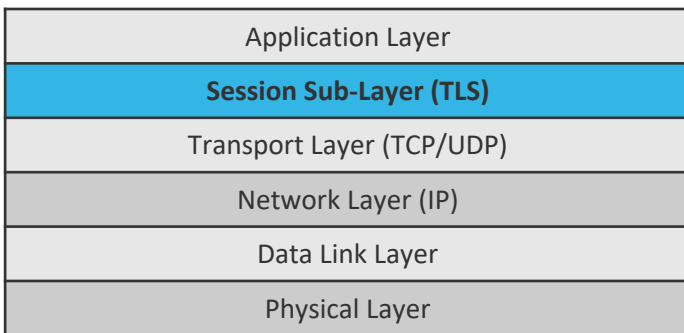


SKI Decrypt Library

Nubeva’s Decryption Library supports high speed TLS 1.3 and TLS 1.2 PFS decryption using final session encryption secrets extracted by Nubeva Discovery Sensors or other source able to obtain TLS master keys to decrypt.

Product Overview

The decryption library is a static C library designed to provide high decryption throughput of TLS records. The library receives TCP payloads from the data path and operates independently of packet acceleration custom architectures.



SR-IOV hypervisor bypass
DPDK VM Kernel Bypass

Product Applications

Inline Systems

Enables inline security systems such as Firewalls, IPS’s, Proxies, Secure Web Gateways, SD-WAN and DLP systems with low-latency, line-rate decryption

Passive Systems

Enables out-of-band, monitoring systems such as IDS’s, NDR’s, and Application Performance Monitoring systems to “see” into PFS traffic at scale.

5G and Service Mesh

Enables 360-degree container traffic inspection in 5G packet cores, Service-Mesh and general Kubernetes environments with micro resource load and impact

- For appliances (physical and virtual) and embedded services
- For datacenter, cloud, and hybrid

Performance

The decryption library is designed to work seamlessly with high throughput packet processing configurations, including NICs, SRI-OV, and customized packet processing using DPDK. The library supports TLS 1.2, TLS 1.2 PFS, and TLS 1.3 ciphers. The library provides high decryption throughput at 80% of an [OpenSSL speed test](#). The following table shows decryption throughput in Gbps on an AWS m4.xlarge AWS Linux 2, with an Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz, with AES-NI support enabled. Throughput is shown for a single thread. Multi threading enables 40G, 100G and higher throughput.

Cipher	Block Size	Decrypt Gbps	Cipher	Block Size	Decrypt Gbps
AES-1280-GCM Mac=AEAD	1024	13.95	AES-128-CBC-HMAC=SHA1	1024	4.01
AES-258-GCM Mac=AEAD	1024	11.12	AES-128-CBC-HMAC=SHA256	1024	2.04
CHACHA20-POLY1305	1024	5.86	AES-256-CBC-HMAC=SHA1	1024	3.80
			AES-256-CBC-HMAC=SHA256	1024	1.97

Supported Ciphers

TLS 1.3	DHE-RSA-AES128-GCM-SHA256	ECDHE-PSK-CHACHA20-POLY1305
TLS_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-SHA384	RSA-PSK-AES256-GCM-SHA384
TLS_CHACHA20_POLY1305_SHA256	ECDHE-RSA-AES256-SHA384	DHE-PSK-AES256-GCM-SHA384
TLS_AES_128_GCM_SHA256	DHE-RSA-AES256-SHA256	RSA-PSK-CHACHA20-POLY1305
TLS 1.2	ECDHE-ECDSA-AES128-SHA256	DHE-PSK-CHACHA20-POLY1305
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE-RSA-AES128-SHA256	RSA-PSK-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES128-SHA256	DHE-PSK-AES128-GCM-SHA256
DHE-RSA-AES256-GCM-SHA384	AES256-GCM-SHA384	
ECDHE-ECDSA-CHACHA20-POLY1305	AES128-GCM-SHA256	ECDHE-ECDSA-AES256-SHA
ECDHE-RSA-CHACHA20-POLY1305	AES256-SHA256	ECDHE-RSA-AES256-SHA
DHE-RSA-CHACHA20-POLY1305	AES128-SHA256	ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE-PSK-CHACHA20-POLY1305	ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-GCM-SHA256	RSA-PSK-AES256-GCM-SHA384	ECDHE-RSA-AES256-SHA384

TLS Parsing and Decryption

The underlying packet processing system need not be aware of TLS records, or perform any TLS parsing operations. The underlying packet processing system should perform standard TCP layer termination and re-assembly and eliminate packet deduplication that could occur if traffic is tapped at multiple points. The Decryption library parses and decrypts all possible TLS encapsulations in TCP payloads containing:

- a single complete TLS record
- multiple TLS records:
- one or more TLS records followed by the first fragment of the next TLS record
- a fragment of a TLS record which is not the last fragment
- the last fragment of a TLS record and one or more TLS records

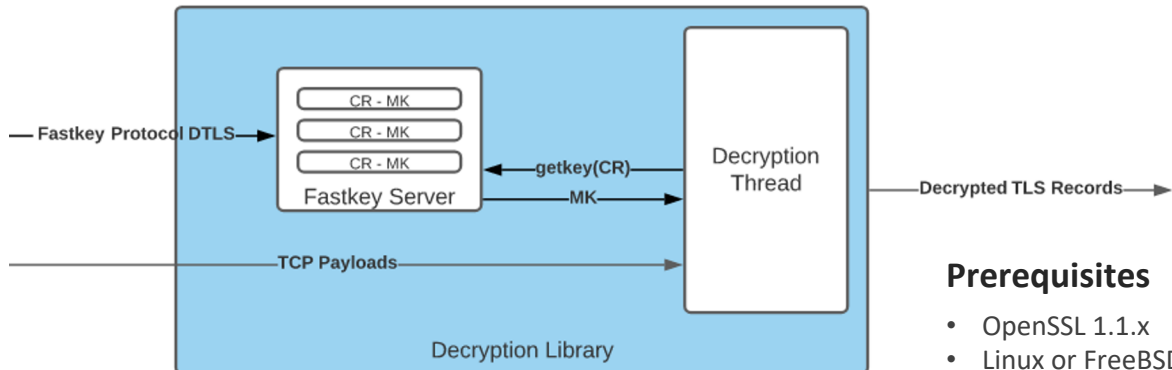
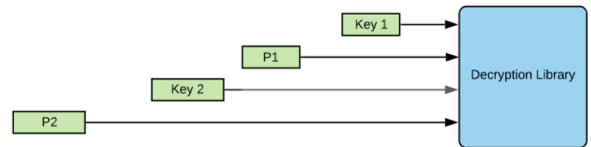
Lost Frame Recovery

The decryption library attempts to continue decrypting a TLS session when TCP packets containing TLS records or TLS record fragments are lost. Recovery is supported for TLS 1.3 AES_128_GSM, TLS 1.3 AES_256_GSM, TLS 1.2 AES_128_GSM, and TLS 1.2 AES_256_GSM ciphers.

FastSKI™ Delivery Protocol

Nubeva Sensors send session master secrets 200µs after the secrets are created, and 500µs before the first encrypted application data is received.

The Key Server receives and buffers these keys until they are requested for decryption. The use of the Key Server is optional and can be enabled or disabled when the decryption library is initialized. If users choose to manage keys independently, they should provide the library with a key-lookup function to the Decryption Library.



Prerequisites

- OpenSSL 1.1.x
- Linux or FreeBSD8

Core Benefits

- Decrypt more traffic without complicating architecture or compromising security
- Execute with high performance by eliminating latency and throughput issues
- Reduce operational inefficiencies for you users with no more certificate and exception management
- Eliminate current limitations in your product suite to speed adoption
- Lead the way to competitive advantage with better functionality, ease, price performance and a solution for universal use

SKI (Session Key Intercept) – Product Suite:

The SKI Decryption library is a key component in the Nubeva Session Key Intercept solution architecture for the decryption of modern TLS, enabling deep packet inspection for inline and passive applications. SKI's model is to learn and capture TLS session secret keys from TLS clients or servers in real-time, using next-generation agents and containers (Nubeva SKI Sensors). Then to security and quickly forward them to inspection systems for decryption. SKI offers an alternative to the legacy methods of man-in-the-middle, proxy termination, and passive decryption offering superior capability, price/performance, and simplicity.