Accelerated Inline IPsec Communication with T7

Chelsio Terminator 7

The Terminator 7 (T7) ASIC from Chelsio Communications, Inc. is a seventh generation, high performance 1/10/25/40/50/100/200/400 Gbps, Unified Wire Data Processing Unit (DPU) which offers offload support for a wide range of Crypto (IPsec, TLS/SSL), TCP, UDP, NVMe/TCP, NVMe-oF, iSCSI, RDMA (iWARP and RoCEv2) and FCoE protocols. It is designed specifically to perform computationally intensive cryptographic operations more efficiently than general-purpose CPUs. Servers with system load, comprising of cryptographic operations, see great performance improvement by offloading crypto operations on to the Chelsio T7 adapters. With concurrent support for offloading multiple protocols and crypto operations, Chelsio has taken the Unified Wire solution to the next level.

Chelsio Inline IPsec Acceleration

Internet Protocol Security (IPsec) is an end-to-end security scheme that provides protocols to ensure the authenticity, privacy, and integrity of data in transit. Chelsio's T7 Inline IPsec solution uses the standard crypto API framework provided by the operating system and enables the offloading of encryption/decryption operations on to the adapter. It provides an accelerated Inline IPsec tunnel which is well suited for site-to-site security over WAN. Both Tunnel and Transport modes of IPsec are supported with ESP protocol. It supports both Tx and Rx Offload. Additionally, the Public Key Exchange (PKE) mechanism can be offloaded to the adapter.

Inline IPsec for L2 NIC traffic

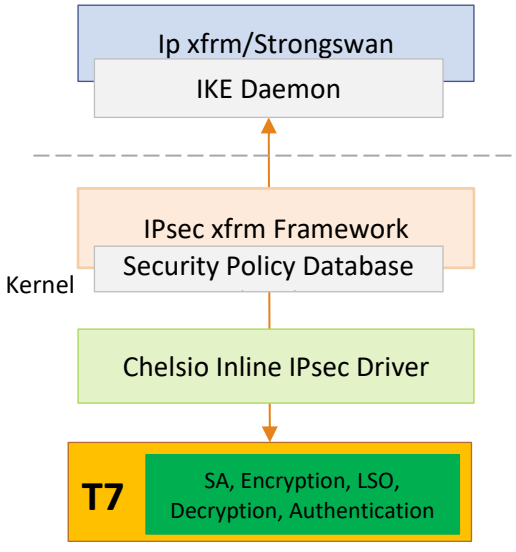

Figure 1 – Inline IPsec for L2 NIC traffic

The Kernel IPsec (xfrm framework) will maintain the security policy database (SPD), which will classify the packets to be processed by IPsec. The IKE Daemon will perform the key exchanges and the driver will store the SA (security association) information and encryption/decryption keys in the Hardware.

In transmit, the Kernel will form the ESP Header and the packet will reach the hardware. The Hardware will segment the packets (LSO), encrypt them using the stored keys, and will send on the wire.

In Receive, the hardware will decrypt and authenticate the received packets using the stored keys. On successful authentication, the packets will be delivered to the host (without modifying the header fields).

Inline IPsec for Offload traffic

With T7, Inline IPsec is supported for Chelsio Offload protocols like TOE, iSCSI, RDMA (iWARP and RoCEv2), NVMe/TCP etc.

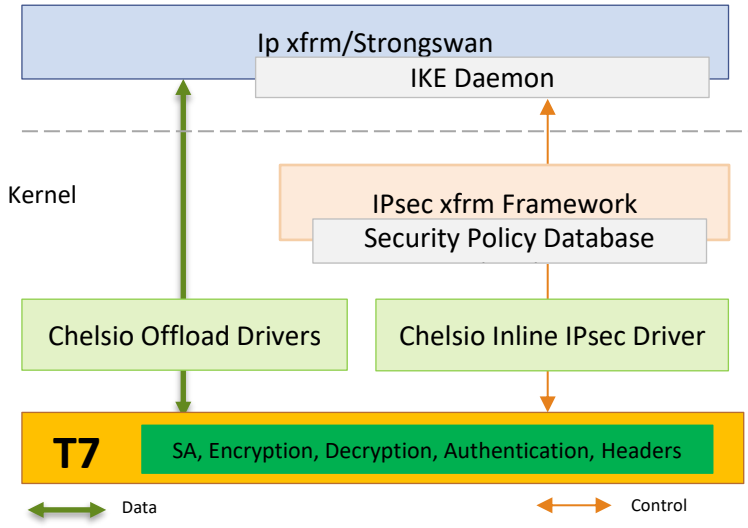

Figure 2 – Inline IPsec for Offload traffic

The Kernel IPsec xfrm framework will maintain the security policy database (SPD), which will classify the packets to be processed by IPsec. The IKE Daemon will perform the key exchanges and the driver will store the SA (security association) information and encryption/decryption keys in Hardware.

In transmit, the hardware will form all the headers (including ESP), encrypt the packets using the stored keys and will send on the wire.

In Receive, the hardware will decrypt and authenticate the received packets using the stored keys. On successful authentication, the packets will be further processed by the offload drivers.

The data is offloaded directly from the application to the Hardware and vice-versa, completely bypassing the kernel stack.

Conclusion

Chelsio T7 Inline IPsec solution provides enterprises with secure remote connection to access corporate applications and resources without sacrificing on performance and speed. T7 delivers an unmatched feature set combined with a single-chip design. No other vendor offers a single SKU for offloading multiple protocols with concurrent Crypto support.

Related Links

T7 Product Brief
Offload Protocols with Inline IPsec demonstration on T7 Emulation Platform