Hardware-Based IPsec Tunnel Acceleration on Dedicated Cryptographic Cards - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

Hardware-Based IPsec Tunnel Acceleration on Dedicated Cryptographic Cards represents a purpose-built architecture that offloads compute-intensive IPsec operations from general-purpose CPUs to specialized cryptographic silicon. By integrating dedicated cryptographic cards directly into the routing or security platform, the system delivers line-rate encryption, authentication, and key exchange processing without compromising packet forwarding performance. This approach eliminates the throughput bottlenecks, latency jitter, and CPU exhaustion commonly observed in software-only IPsec implementations.

The solution is engineered for enterprise WAN aggregation, carrier-grade VPN gateways, and multi-tenant datacenter interconnect scenarios where scalable, deterministic cryptographic performance is mandatory. Each dedicated cryptographic card operates as an independent acceleration engine, supporting high-concurrency tunnel establishment and sustained encrypted throughput across thousands of simultaneous IPsec sessions.



HARDWARE ARCHITECTURE & SILICON

The platform combines a high-performance multi-core network processor with one or more dedicated cryptographic acceleration cards installed in modular expansion slots. Each cryptographic card contains a purpose-designed ASIC or FPGA-based crypto engine that handles the complete IPsec packet processing pipeline, including ESP encapsulation/decapsulation, AES-GCM or AES-CBC encryption, SHA-1/SHA-256 authentication, and anti-replay window management.

The host network processor retains control-plane responsibilities such as IKEv2 negotiation, security association management, and routing protocol operation. Data-plane IPsec traffic is redirected to the cryptographic card via a high-bandwidth internal interconnect, typically PCI Express or a proprietary

switch fabric, ensuring minimal latency and zero CPU contention. Hardware-based random number generation and secure key storage are embedded within the cryptographic card to satisfy FIPS 140-2 or FIPS 140-3 Level 2/3 requirements.

KEY FEATURES & ROUTING LOGIC

- Dedicated IPsec Offload: All ESP processing, including encryption, authentication, and integrity verification, is performed entirely within the cryptographic card, freeing host CPU cycles for routing and services.
- Line-Rate IPsec Throughput: Sustained encrypted forwarding at up to 100 Gbps per cryptographic card, with near-zero performance degradation as tunnel count scales.
- High-Concurrency Tunnel Support: Supports up to 32,000 simultaneous IPsec tunnels per card, with IKEv2 session scalability for hub-and-spoke and mesh topologies.
- Deterministic Low Latency: Hardware pipeline delivers consistent sub-50 microsecond added latency for encrypted traffic, independent of packet size or tunnel count.
- Flexible Cryptographic Algorithms: Accelerates AES-128/192/256-GCM, AES-CBC, 3DES, SHA-1, SHA-256, SHA-384, and Galois Message Authentication Code (GMAC).
- Redundant Card Architecture: Supports 1+1 active/standby cryptographic

card redundancy with automatic failover in sub-second intervals.

- Secure Boot and Key Isolation: Cryptographic card firmware is measured and verified during boot; keys never leave the card boundary in plaintext.

- Routing Integration: Seamless interoperability with OSPF, BGP, IS-IS, and static routing, with IPsec policy enforcement at the interface or VRF level.

COMPLIANCE & STANDARDS

The platform conforms to the following standards and certifications:

- IPsec: RFC 4301, RFC 4302, RFC 4303, RFC 4306 (IKEv2), RFC 7296

- Encryption: FIPS 140-2 / FIPS 140-3 validated cryptographic module (Level 2 or Level 3)

- Networking: IEEE 802.1Q, IEEE 802.1ad, IEEE 802.3ae, IEEE 802.3ba

- Routing: RFC 4271 (BGP-4), RFC 2328 (OSPFv2), RFC 5340 (OSPFv3), RFC 1195 (IS-IS)

- Management: SNMPv3, NETCONF, RESTCONF, Syslog, TACACS+, RADIUS

- Safety and EMC: UL 60950-1, IEC 62368-1, FCC Part 15 Class A, CE Mark, VCCI Class A

TECHNICAL SPECIFICATIONS

Parameter	**Specification**

Form Factor	Modular 4RU or 8RU chassis, redundant power and cooling
Cryptographic Card Slots	4 or 8 dedicated crypto acceleration slots
IPsec Throughput per Card	100 Gbps / 200 Gbps / 400 Gbps (model dependent)
Maximum IPsec Tunnels	32,000 / 64,000 / 128,000 per card
Encryption Algorithms	AES-GCM, AES-CBC, 3DES, SHA-1, SHA-256, SHA-384, GMAC
IKE Version	IKEv2 (RFC 7296), IKEv1 (RFC 2409) legacy support
Latency (Added)	< 50 microseconds per encrypted packet
Redundancy	1+1 active/standby cryptographic card failover, < 1 second
Host Interfaces	100GE QSFP28, 400GE QSFP-DD, 10GE SFP+ (module dependent)
Internal Interconnect	PCI Express Gen4 x16 or proprietary switch fabric
Power Supply	Dual hot-swappable redundant AC/DC, 2000W per PSU
Cooling	Hot-swappable redundant fan trays,

	front-to-back airflow
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Relative Humidity	5% to 95% non-condensing
MTBF	> 250,000 hours (system, Telcordia SR-332)
FIPS Validation	FIPS 140-2 Level 2/3 or FIPS 140-3 Level 3 (model dependent)
Management	SNMPv3, NETCONF, RESTCONF, CLI, Web UI
Regulatory Compliance	UL, IEC, FCC, CE, VCCI, RoHS, WEEE

ORDERING SKU INFORMATION

Base System:

- CRYPTO-ROUTER-CHASSIS-4SLOT: 4-slot routing chassis with dual redundant power supplies and dual fan trays

- CRYPTO-ROUTER-CHASSIS-8SLOT: 8-slot routing chassis with dual redundant power supplies and dual fan trays

Dedicated Cryptographic Cards:

- CRYPTO-CARD-100G-A: Single-width cryptographic card, 100 Gbps IPsec throughput, 32,000 tunnels, FIPS 140-2 Level 2

- CRYPTO-CARD-200G-A: Double-width cryptographic card, 200 Gbps IPsec throughput, 64,000 tunnels, FIPS 140-2 Level 3

- CRYPTO-CARD-400G-A: Double-width cryptographic card, 400 Gbps IPsec throughput, 128,000 tunnels, FIPS 140-3 Level 3

Host Network Processor Modules:

- NPU-MODULE-800G: 800 Gbps forwarding capacity, 4x 100GE QSFP28 or 16x 10GE SFP+ interfaces

- NPU-MODULE-1.6T: 1.6 Tbps forwarding capacity, 8x 100GE QSFP28 or 4x 400GE QSFP-DD interfaces

