

SafeNet Multi-Link Encryptor CN8000

10 x 10 Gbps—100 Gbps Total Encrypted Bandwidth



The quantum powered SafeNet Multi-Link Ethernet Encryptor CN8000 (CN8000) enables ultra-secure multi-link encryption of Layer 2 network Ethernet traffic, up to 100 Gbps in one compact chassis, with no overhead and minimum latency. The CN8000 also offers Fibre Channel support for LANs, MANs, or WANs.

Performance

Encrypting data at up to 100 Gbps of Ethernet Layer 2 network traffic, the Swiss-manufactured CN8000 delivers the performance capabilities of ten 10 Gbps encryptors in one appliance. Using Field Programmable Gate Array (FPGA) technology, the CN8000's architecture enables real-time data processing and high throughput. This ensures consistent low latency across all packet sizes for maximum performance - less than 8 μ S at 10 Gbps Ethernet Layer 2, and less than 1 μ S at 8 Gbps for Fibre Channel.

Scalability

The CN8000's simple 'bump in the wire' design and variable speed licenses up to 10 Gbps ensures Ethernet and 8 Gbps Fibre Channel ensures ease of installation and allows an organization to scale as more bandwidth is needed. "Set and forget" simplicity and application and protocol transparency are underlying design themes, ensuring simple operation and management, and minimal resource requirements. Devices can be field upgraded on site with ease, for maintenance, feature enhancements and security



Why CN8000 Encryptors?

Trusted Security

- True end-to-end, authenticated encryption
- State-of-the-art automatic zero-touch key management
- Certified for FIPS 140-2 L3, Common Criteria
- Preferred by market leading commercial and government enterprises in over 35 countries

Maximum Network Performance

- Microsecond latency (Ethernet= $\leq 8 \mu$ S, Fibre= $\leq 1 \mu$ S)
- Near-zero overhead
- Self-Healing capabilities for maximum up time

Scalable and Simple

- Point to Point, Hub and Spoke, and Full Mesh
- Fully auditable alarm and event logs from 3rd party management tools

updates. Compliant with Ethernet standards, the CN8000 is fully interoperable with industry standard network equipment from leading vendors. Working in point-to-point, point-to-multi-point, and fully meshed multi-point modes, the CN8000 supports the encryption of uni-cast, broadcast, and multi-cast communications. Compatible with the SafeNet High Speed Encryptor family of products, CN8000 encryption cards can be connected in a meshed network to multiple encryptors in a campus or wide area network. This enables customers to standardize on one platform to secure data in motion across large hub and spoke or meshed networks. Advanced group key encryption ensures easy management of such multi-point environments, with separate keys for different VLANs or MAC addresses. Supporting over 500 concurrent encrypted connections, the CN8000 operates at full line speed without packet loss to ensure the confidentiality of encrypted data regardless of frame size or application.

Trusted Security

The tamper resistant CN8000 is certified Common Criteria and FIPS 140-2 Level 3, and supports standards based, end-to-end authenticated encryption, automatic key management, and utilizes robust AES 256-bit algorithms. For future-proofing, the appliance can interface with an external Quantum Key Distribution (Quantum Cryptography) for enhanced key protection, and can internally support an optional Quantum random number generator. Advanced security features also include granular policy management and separation of duties on a per-card and per-device level. This is ideal for multi-tenant environments, enabling crypto separation between data center clients or divisions within an organization.

Data Center Interconnect and WAN/ MAN/LAN Ethernet Services

With the pervasive growth of Ethernet services, the CN8000 is a high-assurance solution for enterprises, government, and service providers, addressing the need for highly secure, highly resilient line-speed encryption of Ethernet network traffic for data center interconnect and metro or wide area Ethernet services. In addition, the CN8000 can support Fibre Channel networks at up to 8 Gbps.

User-Friendly Encryptor Management

SafeNet High Speed Encryptors are easily managed through a simple to use encryptor management application, with local and remote access capabilities, that provides users with comprehensive and intuitive management functionality. The devices can be securely managed either out-of-band—using a dedicated Ethernet management interface or in-band—using the encrypted Ethernet port. Local management using a command line interface is available via a serial console connector.

TACAS+ and RADIUS protocols are supported to allow for Authentication, Authorization, and Accounting (AAA) operations. This provides end users with additional flexibility and security for day to day operations and large scale deployments.

The built-in operational flexibility provides customers the ability to avoid the additional costs of third party optical transport equipment in their network (e.g. OTN provider backbone).

CN8000 Encryptor At-A-Glance

Model	CN8000	
Protocol	Ethernet	Fibre Channel
Protocol and Connectivity		
Maximum Port Speed	10 Gbps	8 Gbps
Maximum chassis throughput	100 Gbps	80 Gbps
Support for Jumbo frames	✓	✓
Protocol and application transparent	✓	✓
Encrypts Unicast, Multicast and Broadcast traffic	✓	✓
Automatic network discovery and connection establishment	✓	✓
Security		
Tamper resistant and evident enclosure, anti-probing barriers	✓	✓
Flexible encryption policy engine	✓	✓
Per packet confidentiality and integrity with AES-GCM encryption	✓	✓
Automatic key management	✓	✓
Encryption and policy		
AES 128 or 256 bit keys	128/256	256
Encryption modes	CFB, CTR, GCM	CFB
Quantum random generator	✓	✓
Supports optional 3rd party quantum key distribution (QKD)	✓	✓
Policy based on MAC address or VLAN ID	✓	✓
Self healing key management in the event of network outages	✓	✓
Certifications		
Common Criteria, FIPS	✓	✓
Performance		
Low overhead full duplex line-rate encryption	✓	✓
FPGA based cut-through architecture	✓	✓
Latency (microseconds per encryptor)	< 8µS	< 1µS

Management		
Front panel LED display notifications	✓	
Centralized configuration and management using SMC and CM7	✓	✓
Support for external (X.509v3) CAs	✓	✓
Remote management using SNMPv3 (in-band and out-of-band)	✓	✓
NTP (time server) support	✓	✓
CRL and OCSP (certificate) server support	✓	✓
Maintainability & Interoperability		
In-field firmware upgrades	✓	✓
Dual redundant AC/DC power supplies	✓	✓
Pluggable optical SFP	✓	✓

Specifications

Cryptography

- AES 128-bit or 256-bit key, X.509 certificates

Device management

- Dedicated management interface (out-of-band)
- Or via the encrypted interface (in-band)
- SNMPv3 remote management
- SNMPv2c traps
- SNMPv1 read only monitoring
- IPv4 & IPv6 capable
- Alarm, event, and audit logs
- Command line serial interface
- Supports Syslog

Installation

- Size: (4U), 430,460,175mm / 17.2, 18.1, 6.9 inches (WxHxD)
- Rack mountable
- Maximum Weight: 22kg / 49lbs.

Interfaces

- SFP+
- Front panel network connections
- Front panel LED display status

Indications

- Color backlit LCD display
- RS-232 serial console for CLI connection
- USB port
- RJ45 SNMP management port
- RS-232 serial console for quantum key channel for (QKD connection)

Power Requirements

- Input: 100 to 240V AC; 1.5A; 60/50Hz
- Power: 300 watts for 10 links

Physical Security

- Active/passive tamper detection and key erasure
- Tamper-evident markings
- Anti-probing barriers

Regulatory Safety (In Process)

- EN 60950-1 (CE)
- IEC 60950-1 Second Edition
- AS/NZS 60950.1
- UL Listed
- EMC (Emission and Immunity)
- ICES-003 (Canada)
- EN 55022 (CE)
- AS/NZS CISPR 22 (C-Tick)
- EN 61000-3-2 (CE)
- EN 61000-3-3 (CE)
- EN 55024 (CE)
- EN 61000-3-3 (CE)
- EN 55024 (CE)
- Environmental (in process)
- RoHS compliant
- Max operating temperature: 40°C / 104°F
- 0 to 80% RH at 40°C / 104°F operating

All specifications are accurate as at the time of publishing and are subject to change without notice.

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.