Thales CN6100 Network Encryptor

10 Gbps scalable, high-assurance data in motion encryption

Safeguard data in motion with high speed network encryption proven to meet network performance demands for realtime low latency and near-zero overhead, providing security without compromise for data traversing networks across data centers and the cloud.

The Thales CN6100 Network Encryptor (CN6100) is the ideal solution for small and large enterprise, government, and service provider clouds. The CN6100 is a versatile, high-assurance encryptor designed to provide up to 10 Gbps of highly secure, full line rate transparent encryption for all voice, video and data communications moving across dark fibre, and metro or wide area Ethernet networks (MAN or WAN).

Performance

The CN6100 is a high-performance encryptor, operating in full-duplex mode at full speed without loss of packets. Using Field Programmable Gate Array (FPGA) technology, the CN6100's cut-through architecture processes data frames as they are received. This ensures consistent low latency across all packet sizes for optimal performance. Throughput is maximized in a zero protocol overhead mode. A 1U unit, it operates with 30–60% less power consumption than typical 10 Gbps encryptors.

Why CN6100 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,NATO, UC APL
- Preferred by market leading commercial and government enterprises in over 35 countries

Maximum Network Performance

- Microsecond latency (<6µS)
- Near-zero overhead
- Self-healing capabilities for maximum up time

Scalable and Simple

- Point-to-point, hub & spoke, and full mesh
- Fully auditable alarm and event logs from 3rd party management tools
- Field serviceable with hot swappable fans and supplies

Scalability

The CN6100 is fully interoperable with industry standard network equipment from leading vendors. The 'Bump in the Wire' design and variable speed licenses up to 10 Gbps make the CN6100 easy to install and highly cost-effective. "Set and forget" simplicity, and application and protocol transparency are underlying design themes, ensuring easy implementation, operation and management, and minimal resource requirements. Devices can be field upgraded on site with ease, for maintenance, feature enhancements and security updates. Full compatibility with the entire Thales Network Encryptor family of products provides end-users with secure data transmission across any network environment.

Certified Security

Preferred by the world's most secure organizations, the tamper resistant CN6100 is certified to Common Criteria and FIPS 140-2 Level 3 requirements and supports standards-based, end-to-end authenticated encryption and client-side key management. Advanced security features include traffic flow security, support for a wide range of elliptic curves (Safe Curves, Brainpool, NIST). VLAN based encryption provides unique key pairs in hub and spoke environments to protect against mis-configured traffic. For high-assurance environments, the encryptors also support nested encryption.

State-of-the-Art Key Management

The CN6100 removes reliance on external key servers and provides a robust fault-tolerant security architecture and tamper-resistant chassis. Physical and virtual separation of duties ensures that only authorized users can access the keys. Encryption keys are generated and stored securely in hardware within the device's tamper-resistant enclosure, and any unauthorized attempts to physically extract the keys will result in device zeroization.

The CN6100 supports hardware based random number generators and can use externally generated entropy for intrinsic key generation and distribution. For future-proofing, the encryptors support Quantum Key Distribution (Quantum Cryptography) and Quantum random number generation.

Next Gen High Speed Encryption

Crypto-Agility

Thales Network Encryptors are crypto-agile, meaning they support customizable encryption for a wide range of elliptic and custom curves support. The appliances also allow bring your own entropy capabilities. The crypto-agile platform is future proof, allowing for responsive deployment of next-gen or custom algorithms. In response to the Quantum threat, Thales Network Encryptors already leverage Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) capabilities for future-proof data security.

Transport Independent Mode

Transforming the network encryption market, Thales Network Encryptors are the first to offer Transport Independent Mode (TIM) - network layer independent (Layer 2, Layer 3, and Layer 4) and protocol agnostic data in motion encryption. By supporting Layer 3, Thales Network Encryptors offer network operators more configuration options using TCP/IP routing for securing critical data.

CN6100 Encryptor At-A-Glance

Model	CN6100
Protocol	Ethernet
Protocol and Connectivity	
Maximum Port Speed	10 Gbps
Maximum chassis throughput	10 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
CTR, GCM Encryption modes	✓
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)	<5@ 10 Gbps
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 XFP	XFP

Specifications

Physical security

- Active/Passive tamper detection and key erasure

Cryptography

- AES 128 or 256 bit key X.509 certificates (CFB, CTR or GCM modes)
- Hardware based random number generator

Device Management

- Dedicated management interface (out-of-band)
- Encrypted interface (in-band)
- SNMPv3 remote management
- IPv4 & IPv6 capable
- Supports Syslog
- Alarm, event & audit logs
- Command line serial interface
- TACAS+ support
- RADIUS support

Installation

- Size: 447mm, 43mm (1U), 328mm / 17.6", 1.7", 12.9"
- 19" rack mountable
- Weight: 8.5kg / 18.7 lbs

Power Requirements

- AC Input: 100 to 240V AC; 1.5A; 60/50Hz
- DC Input: 40.5 to 60 VDC, 2.0A
- Power Consumption: 50W typical

Regulatory Safety

- UL Listed
- EMC (Emission and Immunity)
- FCC 47 CFR Part 15 (USA)
- EN 55024 (CE, 60950-1 (CE), 61000-3-2 (CE), 61000-3-3 (CE)
- IEC 60950-1 Second Edition
- ICES-003 (Canada)

Environmental

- RoHS Compliant
- Max operating temperature: 50°C / 122°F
- 0 to 80% RH at 40°C / 104°F operating
- AS/NZS 60950-1, CISPR 22 (C-Tick)

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

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us