Solution Brief

Thales CN6010 Network Encryptor

Cost-Effective Scalable Network Encryption

thalestct.com

THALES
Building a future we can all trust

The Thales CN6010 Network Encryptor (CN6010) is an easy to use platform that is user configurable to provide transparent and high-assurance FIPS and Common Criteria certified network encryption at full line rate speeds up to 1 Gbps. CN6010 is available for sale to the U.S. Federal Government through Thales Trusted Cyber Technologies.

Performance

Using Field Programmable Gate Array (FPGA) technology, the CN6010's architecture enables real-time data processing and high throughput. This ensures consistent low latency across all packet sizes for maximum performance—less than 8μS at 1 Gbps Ethernet Layer 2. Throughput is maximized in a zero protocol overhead mode. A 1U unit, it operates with minimal power and rack space consumption.

Scalability

The CN6010's simple 'bump in the wire' design and variable speed licenses up to 1 Gbps ensures ease of implementation 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 support all network topologies including point-to-point, hub and spoke, and fully meshed environments, and can be field upgraded on site with ease for maintenance, feature enhancements, and security updates. The CN6010 also supports unicast, multicast, and broadcast domains.

Trusted Security

The tamper resistant CN6010 is certified to Common Criteria and FIPS 140-3 Level 3 requirements, 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.

Metro Ethernet or Wide Area Ethernet Services

With the pervasive growth of Ethernet services, CN6010 is the ideal solution for all organizations from small to large enterprises and government or service provider clouds.

The CN6010 addresses the need for highly secure, highly resilient wire speed encryption of Ethernet traffic across both dark fibre and metro or wide area Ethernet services.

Supporting over 500 concurrent encrypted connections, the CN6010 operates at full line speed without packet loss to ensure the confidentiality of encrypted data regardless of frame size or application.

The intrinsic key generation and distribution capability in CN6010 removes reliance on external key servers and provides robust fault-tolerant security architecture, whilst its rugged tamper resistant chassis gives uncompromising protection to key material held in the encryptor.

Full interoperability with the Thales Network Encryptor family of products means customers can standardize on one platform to secure data in motion across large hub and spoke or meshed networks from the branch to head office.

Why CN6010 Encryptors?

Trusted Security

- True end-to-end, authenticated encryption
- State-of-the-art automatic zero-touch key management
- Certified for FIPS 140-3 L3, Common Criteria,NATO, DoDIN APL
- Preferred by market leading commercial and government enterprises in over 35 countries

Maximum Network Performance

- Microsecond latency (<8 μS)
- 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

State-of-the-Art Key Management

The CN6010 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 CN6010 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

CN6010 Encryptor At-A-Glance

Model	CN6010
Protocol and Connectivity:	
Maximum Speed	1 Gbps
Support for Jumbo frames	Yes
Protocol and application transparent	Yes
Encrypts Unicast, Multicast and Broadcast traffic	Yes
Automatic network discovery and connection establishment	Yes
Security:	
Tamper resistant and evident enclosure, anti-probing barriers	Yes
Flexible encryption policy engine	Yes
Per packet confidentiality and integrity with AES-GCM encryption	Yes
Automatic key management	Yes
Encryption and Policy	
AES 128 or 256 bit keys	128/256
CFB, CTR, GCM Encryption modes	Yes
Quantum random generator	Yes
Policy based on MAC address or VLAN ID	Yes
Supports optional 3rd party quantum key distribution (QKD)	Yes
Self-healing key management in the event of network outages	Yes
Certifications:	
Common Criteria, FIPS, DoDIN APL	Yes
Performance:	
Low overhead full duplex line-rate encryption	Yes
FPGA based architecture	Yes
Latency (microseconds per encryptor)	<8 µS
Management:	
Front panel access for all interfaces	Yes
Centralized configuration and management using SMC/ CM7	Yes
Support for external (X.509v3) CAs	Yes
Remote management using SNMPv3 (in-band and out-of-band)	Yes
NTP (time server) support	Yes
CRL and OCSP (certificate) server support	Yes
Maintainability/Interoperability:	
In-field firmware upgrades	Yes
Dual hot-swappable AC/DC power supplies	Yes
Pluggable optical SFP	Yes

Specifications

Cryptography

- AES 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
- Supports Syslog
- Alarm, event & audit logs
- Command line serial interface

Installation

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

Interfaces

- SFP and RJ45 interfaces
- Front panel network connections
- Front panel LED display status indications
- Color backlit LCD display
- RJ-45 serial console
- Dual USB ports
- RJ45 LAN/AUX connectors

Power Requirements

- AC Input: 100 to 240V AC;1.5A; 60/50Hz
- DC Input: 40.5 to 60 VDC, 2.0A
- Power Consumption: 14W Max

Physical Security

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

Regulatory

- EN 60950-1 (CE)
- IEC 60950-1 Second Edition
- AS/NZS 60950.1
- UL Listed
- EMC (Emission and Immunity)
- FCC 47 CFR Part 15 (USA)
- 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

- RoHS Compliant
- Max operating temperature: 50°C / 122°F
- 0 to 80% RH at 40°C/104°F operating

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com