PRODUCT BRIEF

SafeNet Ethernet Encryptor CN6100

10 Gbps scalable, high-assurance data in motion encryption

Safeguard data in motion with high speed Layer 2 encryption proven to meet network performance demands for real-time low latency and near-zero overhead, providing security without compromise for data traversing networks across data centers and the cloud.

With the rapid growth of 10 Gbps Ethernet services, the Safenet Ethernet Encryptor CN6100 (CN6100) is the ideal solution for organizations from small to large enterprises and government or service provider clouds. The CN6100 is a versatile, high-assurance encryptor designed to provide up to 10 Gbps highly secure, full line rate transparent encryption of 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

Scalability

Supporting over 500 concurrent encrypted connections, the CN6100 ensures the confidentiality of encrypted data in point-point, hub and spoke, or any meshed environment. The CN6100 supports unicast, multicast and broadcast domains.

Ethernet standards compliant, 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 Ethernet 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 interoperability with the CN series of encryptors including all the lower bandwidth devices provides end-users with secure data transmission across any Ethernet network environment.

Certified Security

Preferred by the world's most secure organizations, the tamper resistant CN6100 is certified Common Criteria and FIPS 140-2 Level 3 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 misconfigured traffic. For high-assurance environments, the encryptors also support nested encryption.

Trusted Security

- True end-to-end, authenticated encryption
- State-of-the-art client side key management
- Certified FIPS 140-2 L3, Common Criteria, NATO, UC APL
- Preferred by market leading commercial and government enterprises in over 30 countries

Maximum Network Performance

- Microsecond latency
- Near-zero overhead including zero overhead mode
- Self-Healing capabilities for maximum up time

Scalable and Simple

- Point to Point, Hub and Spoke or Full Mesh deployments
- Fully auditable alarm and event logs from 3rd party management tools
- Field serviceable with hot swappable supplies

State-of-the-Art Key Management

The CN6100 removes reliance on external key servers and provides a robust fault-tolerant security architecture and rugged 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. SafeNet High Speed Encryptors support hardware based random number generators and can use externally generated entropy for intrinsic key generation and distribution.

User-Friendly Encryptor Management

SafeNet High Speed Encryptors are easily managed through a simple to use local and remote encryptor management application that provides users with comprehensive and intuitive management functionality. The encryptors 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.

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, NTP
> 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)
> AS/NZS 60950-1, CISPR 22 (C-Tick)

Environmental

> RoHS Compliant
> Max operating temperature: 50°C /122°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.

CN6100 Encryptor At-A-Glance

MODEL	CN6100
Protocol	**Ethernet**
PROTOCOL AND CONNECTIVITY:	
Maximum Speed	10 Gbps
Link/Rate Limiting	✓
Support for Jumbo frames	✓
Protocol and application transparent	✓
Encrypts Unicast. Multicast and Broadcast traffic	✓
Automatic network discovery and connection establishment	✓
Network interfaces	XFP
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	✓
Traffic flow analysis protection	✓
ENCRYPTION AND POLICY:	
AES 128 or 256 bit keys	128/256
Encryption modes	CFB, CTR, GCM
Policy based on MAC address or VLAN ID	✓
Self healing key management in the event of network outages	✓
CERTIFICATIONS:	
Common Criteria, FIPS, NATO, UC APL	✓
PERFORMANCE:	
Low overhead full duplex line-rate encryption	✓
FPGA based cut-through architecture	✓
Latency (microseconds per encryptor)	< 9.8
MANAGEMENT:	
Front panel access for all interfaces	✓
Centralized configuration and management using SMC, CM7 and SNMPv3	✓
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 hot-swappable AC and/or DC power supplies	✓
User replaceable fans and batteries	✓

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free