Introduction

SafeNet CN high speed network data encryption devices are purpose built hardware appliances that secure data transmitted across Layer 2 networks. The CN series platforms provide highly secure, full line rate transparent encryption for data moving across both dark Fibre and metro, or wide area Ethernet networks in point-point, hub & spoke, or any meshed environment.

Providing the world’s only triple-certified encryptors of their type - Common Criteria, FIPS and CAPS (UK) certifications*, the CN series has been deployed to protect sensitive data in thousands of locations in more than twenty-five countries.

The CN platform is optimized to secure information transmitted over a diverse range of Layer 2 network protocols including: Ethernet, Synchronous Optical Network (SONET) and Fibre Channel networks at data speeds up to 10 Gigabits per second (Gbps). The CN series encryptors’ latency and overhead are the lowest in the marketplace.

Encryption occurs at the data link Layer (Layer 2); the payload of the received network traffic is scrambled and the protocol header is left in the clear so that it can be switched through the network as intended.

Encryption at Layer 2 solves many of the underlying problems of traditional Layer 3 encryption such as complexity, reduced performance and a lack of support for multiple traffic types.

CN encryptors are fully autonomous and operate independently in point to point or large meshed environments with no reliance on external servers.

Supporting fully automatic key management with unique encryption keys per connection, these encryptors offer the most secure, resilient and highest performance method of securing sensitive voice, video and data.

The remainder of this document focuses on the CN series Ethernet encryptors to describe the SafeNet Layer 2 approach to protecting critical sensitive information.

*For details about specific models, please contact SafeNet
Product Architecture

CN series encryptors are in-line devices located on the edge of a network between a local private network, and a remote public network.

CN encryptors provide access control, authentication and confidentiality of transmitted information between secured sites. The encryptors are added to an existing network providing complete transparency to the end user and network equipment. An example installation is shown in Figure 1

![Figure 1–Ethernet Mesh Deployment](image)

The encryptor receives frames on its ingress port; valid frames are classified according to the Ethernet header then processed according to the configured policy.

The frame processing policy is highly configurable and supports operation in point-to-point, hub and spoke and fully meshed environments.

In a meshed environment, each encryptor supports over 500 concurrent connections to peer devices with per connection policy tied to either remote MAC address or to VLAN ID.

Allowable policy actions are:

- Encrypt–payload of frame is encrypted according to the defined policy
- Discard–drop the frame, no portion is transmitted
- Bypass – transmit the frame without alteration

Selective policy control allows mixed traffic profiles which permits specified traffic types to be bypassed or discarded through the device (for example, bypassing core switch operation or maintenance frames) with policy resolution down to the ether-type level.

The Ethernet transmitter module calculates and inserts the Frame Check Sequence (FCS) at the end of the frame. The frame is then encoded and transmitted.

Multicast traffic and VLANs

Multicast encryption is used to encrypt traffic that is sent from a host to all members of a multicast group and operates at Layer 2 with no requirement to modify core switch operation. Policy is tied to a multicast MAC address.

VLAN encryption is used to encrypt all members of a VLAN community and to provide cryptographic separation between VLANs. Policy is tied to the VLAN identifier(s).

In both cases a group key encryption scheme is used to ensure that encrypted data from a single sender can be successfully received and decrypted by all members of the VLAN or multicast community. Group key encryption uses the AES CTR encryption mode.
**Key Management**

The SafeNet group key management scheme is responsible for ensuring group keys are maintained across the visible network and is designed to be secure, dynamic and robust; with an ability to survive network outages and topology changes automatically. It does not rely on an external key server to distribute group keys as this introduces both a single point of failure and a single point of compromise.

The CN high-speed encryptor series is developed with designed-in features necessary to maximize performance, flexibility and dependability.

For robustness and security a group key master is automatically elected amongst the visible encryptors within a mesh based on the actual traffic. Using an elected key master from within the group allows:

- Automatic discovery of multicast/VLAN encryption groups
- Automatic ageing/deletion of inactive groups
- Secure distribution and updates of keys to all members of multicast groups
- New members to securely join or leave the group at any time
- Fault tolerance to network outages and topology changes

**Figure 2 - Data flow through the Encryptor**

**Performance**

Encryption is implemented in dedicated silicon using cut-through encryption architecture. This has the benefit that only a portion of the frame needs to be received before encryption and re-transmission of the frame can begin. This approach ensures both very low latency and consistently low latency (in the order of 7uS for a 1 Gbps Ethernet encryptor) independent of frame size. This consistency is an important attribute in many business applications.

In Cipher Feedback Mode (CFB) encrypted frames are the same size as plaintext frames and no packet expansion is performed.

In Counter mode (CTR) an 8 byte shim is appended to encrypted frames to ensure counter values are synchronized at both ends.

The CN encryptors are capable of full duplex, full line rate operation independent of packet size or higher Layer protocol.
An encryptor will also generate a very small amount of traffic between devices for key updates and management purposes. To distinguish it from other network frames this traffic is sent using the SafeNet registered ether-type (0xFC0F).
Compatibility
The SafeNet CN encryptors have proven interoperability with Ethernet switches from all the well-known vendors and provide transparent support for:

- All Ethernet frame formats
- MPLS shims (multiple nested)
- VLAN tags (multiple nested)
- 802.1P class of service priority

Key Management
The encryption algorithm used in CN encryptors is AES in cipher feedback mode (CFB) or counter mode (CTR) with a key size of 256 bits.

Encryption keys are derived internally to FIPS standards from true hardware random number generators.

Public key cryptography and X.509 certificates are used to provide a fully automated key management system. Master (key encrypting) keys are transferred between encryptors using authenticated RSA public key cryptography. Session (data encrypting) keys are transferred periodically between encryptors using master keys.

Any combination of encrypted or unencrypted virtual circuits can be configured up to a maximum of 509 active connections for a standard Ethernet frame format.

Interoperability with 3rd party Certificate Authorities and OCSP/CRL servers is permitted and a full CA capability is also provided in the companion management platforms.

Tamper Protection
The CN series is manufactured in a tamper proof 19” steel case suitable for rack mounting.

Physical security is ensured by an active tamper protection mechanism that operates in the presence or absence of power. The tamper detection mechanism is triggered if an attempt is made to remove the interface card or remove the lid of the enclosure.

A tampered encryptor will actively delete all sensitive material such as encryption keys and user passwords and will revert to a known factory default configuration.

Holographic tamper evident seals are used to provide visibility of tampered units.

Additionally, more recent encryptors now include hardware design features that prevent physical interference with the hardware.

Management
CN series encryptors are supplied with two options for management. Security Management Center (SMC) is an enterprise manager, whereas CM7 (CypherManager) is an “element manager” more suited for small deployments.

Both offer a simple to use local and remote encryptor management application that provides users with comprehensive and intuitive management functionality.
Role based management access is used for both local (RS232 CLI) and remote (SNMPv3) management. All users must be authenticated before being granted access to a CN series encryptor.

Various privilege levels and different accounts are supported.

The encryptor logs all configuration changes to a non-volatile audit log and also records all events to a non-volatile event log. Any alarm conditions are reported in the logs and in the alarm table, they are also indicated on the front panel LEDs and may optionally trigger SNMP trap messages that can be sent to independent trap handlers (e.g. OpenView, NetView) as well as being received by SMC/CM7.

The CN encryptor can be managed securely and remotely using SNMPv3 via a dedicated management port on the front panel, this being referred to as out-of-band management.

Remote management can also be enabled over the encrypted network itself so that the encryptor is managed over the network interface port; this is called in-band management.

The management platform not only functions as a device manager but also as a root Certificate Authority for a network of SafeNet CN encryptors.

The management platforms provide private, authenticated access to encryptors to enable secure remote management. They can also be used to remotely upgrade the encryptors' firmware over the network.

**About SafeNet, Inc.**

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet’s data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.