

Certes Networks CEP1000

FIPS Validated 1 Gbps Network Encryptor

Product Overview

The CipherEngine Enforcement Point (CEP) is a flexible encryption appliance providing Ethernet frame encryption for Layer 2 Ethernet networks, IP packet encryption for Layer 3 networks and Layer 4 data payload encryption for MPLS networks. The CEP1000 offers full-duplex line rate encryption at 1 Gbps (2 Gbps aggregated), using the AES 256 bit encryption algorithm.

The CEP1000 enables organizations to standardize on one platform for large campus, data center and branch office networks. The CEPs integrate easily into any existing network, operating transparently to the network and ensuring all of your data transmissions are encrypted.

Scalable and Secure Group Encryption

The CEP1000 uses scalable group encryption to provide encrypted and authenticated low-latency any-to-any connectivity. The CEP1000 uses Certes Networks' centralized management solution (CipherEngine) to securely generate and distribute group keys to authorized endpoints. By avoiding the use of tunnels, group encryption greatly reduces deployment complexity and provides fully-meshed encryption that is easy to manage.

Ethernet Frame Encryption

The CEP1000 is compatible with all multipoint-to-multipoint Ethernet, point-to-point Ethernet, and Layer 2 multicast or unicast topologies. As part of the encryption process with the CEPs, each and every Ethernet frame is authenticated. The CEPs can encrypt all Ethernet frames or encrypt selectively based on VLAN ID.

IP Packet Encryption

Using IP Security protocol (IPsec), the CEP1000 provides full data encryption for Layer 3 IP networks. The CEP1000 CC IP packet encryption works with IP and MPLS IP-VPN networks. The CEP1000 supports the CipherEngine Encapsulating Security Payload protocol (CE-ESP) to preserve the original IP packet header and encrypt just the payload. This unique functionality maintains network transparency, while providing maximum data protection. By preserving the original header information and encrypting only the payload, the CEP1000 can protect data over any IP network infrastructure including multi-carrier, load-balanced and high availability networks.

Payload Only Encryption

In addition to standard IPsec encryption, (which encrypts the Layer 4 header), the CEP1000 offers a Layer 4 compatible "payload only" encryption option. This unique, patent-pending capability allows network services, such as Netflow/Jflow, and Class of Service (CoS) based traffic shaping and Network Address Translation (NAT) to be maintained through the service provider network while the payload itself is encrypted.

Central Policy Management

The CEP1000 can be configured and centrally managed via the CipherEngine Policy and Key Manager. CipherEngine allows both Security and Network Administrators to quickly and easily manage network security from a centralized interface with simple drag and drop functionality.

Encryption policies can be based on source or destination IP addresses, source or destination port numbers, protocol IDs, or VLAN tags. Policies can be quickly and easily modified in seconds on even the largest networks, without traffic disruptions or interaction with remote personnel. CipherEngine also provides logging and audit mechanisms to meet or exceed compliance and audit requirements.



PRODUCT SNAPSHOT

- FIPS 140-2 Level 2 validated
- Wire-rate encrypted throughput at 1 Gbps (full duplex)
- Layer 2 Ethernet frame, Layer 3 IP packet, and Layer 4 payload protection
- Per-Frame/Packet Authentication
- Preserves VLAN and MPLS tags

FEATURES AND BENEFITS

- Transparent to network and applications
- Seamless scalability
- Infrastructure neutral
- Easy installation and management
- Create secure network groups

COMPREHENSIVE DATA PROTECTION

- IPsec site-to-site networks
- MPLS meshed networks
- Metro Ethernet and VPLS networks
- Voice and Video over IP applications
- Multicast streams

Certes Networks CEP1000

FIPS Validated 1 Gbps Network Encryptor

Encrypted Throughput

- 1 Gbps (full duplex)

Encryption Support

- AES 256

Authentication and Integrity

- HMAC-SHA-1-96

Network Support

- Ethernet
- VLAN tag preservation
- MPLS tag preservation
- IPv4
- IPv6 (Layer 2 Ethernet encryption mode)
- Multicast streams
- NTP

Policy Selector Options

- Source or destination IP address
- Source or destination port number
- Protocol ID (L3 and L4 options)
- VLAN ID (L2 option)
- Multicast address

Transforms

- CipherEngine ESP Tunnel Mode (header preservation option)
- CipherEngine ESP Transport Mode (L4 option)
- CipherEngine Ethernet ESP Mode

Device Management

- CipherEngine
- Command Line Interface
- Out-of-band management
- Alarm condition detection and reporting
- Syslog support
- SNMPv2c and SNMPv3 managed object support
- Audit Log

Regulatory

- Safety: UL 60950-1
- FCC part 15 subpart B class A

Management Communication Security Options

- X.509 v3 digital certificates
- TLS (full authentication)
- SSH
- IKE/IPsec

Environmental

- Operating temperature: 0° to 40° C (32° to 104° F)
- EU WEEE
- EU RoHS-5

Indicators

- Power
- Alarm
- LED Status

Physical

- 1U tamper evident chassis
- Dimensions 1.75”H x 17”W x 10”D
- Rack mountable in standard 19” rack
- Power: Dual A/C hot swappable 100V@3.A - 240V@1.5A, 47-63Hz, auto-sensing
- Thermal: In-rush 380 BTU/hr, Steady-state 140 BTU/hr
- Nominal input current: .65A@110V
- Weight: 9 lbs
- MTBF: 158,520 hours

Interfaces

- Data: Two full-duplex Gigabit Ethernet ports with SFP interfaces (single mode, multimode or copper)
- Management: One 10/100 RJ45 Ethernet and one RS232 serial port
- Management SFP port and Aux1 SFP port are for future use