

CipherEngine Enforcement Point

CipherOptics CEP1000

1Gbps Network Encryptor

PRODUCT SNAPSHOT

- 1.9Gbps full duplex line rate AES encryption
- Layer 2 Ethernet frame, Layer 3 IP packet and Layer 4 payload protection
- Preserves VLAN and MPLS tags
- Create secure network groups

SOLUTION FEATURES AND BENEFITS

- Network-wide encryption
 - Layer 2 Ethernet frame encryption
 - Layer 3 IPsec encryption
 - Layer 4 payload encryption
- Management and configuration
 - Global network security policy enforcement
 - Global encryption key creation and distribution
 - Easy to install and simple to manage
 - Highly scalable

GLOBAL DATA PROTECTION

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

CONTACT INFORMATION

CipherOptics, Inc.

701 Corporate Center Drive
Raleigh, NC 27607
Tel: +1.877.878.6655
Fax: +1.919.233.9751
info@cipheroptics.com

Product Overview

The CipherEngine Enforcement Point (CEP) is a flexible encryption appliance that provides 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 1.9Gbps using the AES encryption algorithm.



CEP1000

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

Selection of the encryption service is controlled through CipherOptics CipherEngine Services Platform. CipherEngine streamlines network security policy management and device configuration for all CipherOptics enforcement points.

Ethernet Frame Encryption

The CEP1000 provides line rate full duplex encryption for multipoint-to-multipoint Ethernet, point-to-point Ethernet, Layer 2 multicast and Layer 2 unicast topologies. Engineered with flexible policy management, the CEP1000 can encrypt data based on the VLAN ID or a range of VLAN IDs. For point-to-point Ethernet networks, the CEP1000 can simply encrypt all Ethernet frames between the two network endpoints.

IP Packet Encryption

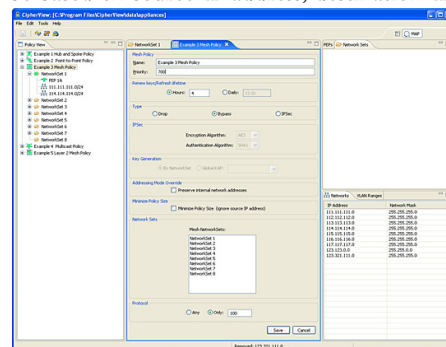
Using the IP Security protocol (IPsec), the CEP1000 provides full data encryption for 1Gbps IP networks. CipherEngine's streamlined policy management allows you to create site-to-site IPsec connections or meshed group connections over public or private IP networks.

Payload Only Encryption

Unlike standard IPsec encryption which encrypts portions of the Layer 3 header, the CEPs offer a Layer 4 "payload only" encryption option for backbone MPLS networks that require the entire Layer 2 and Layer 3 headers to be readable for traffic engineering and Service Level Agreement management. The CEPs provide the option of encrypting only the data payload, thereby providing maximum data protection while maintaining traffic engineering capabilities within the network.

Central Policy Management

The CEP1000 is managed by CipherOptics CipherEngine. CipherEngine provides you with granular control over what is encrypted on your network. Traffic encryption is set by policy definition and can be based on source IP address, destination IP address, source port number, destination port number, protocol ID, or VLAN tag ID. CipherEngine also allows the CEPs to be grouped so that every member of the group uses the same key material. This endpoint grouping allows full meshed any-to-any encryption at for any network traffic.



CipherEngine allows you to create and deploy network policies from a single user interface.

CipherEngine also provides log and audit mechanisms which allow you to collect and monitor key criteria such as CEP status, policy changes, device configuration changes, and password changes. With CipherEngine, you can perform real-time additions, changes and deletions across your global networks.

CipherEngine Enforcement Point

CipherOptics CEP1000

CipherOptics CEP Features and Benefits

Feature	Feature Description	Benefit
Ethernet frame encryption	Encrypts entire Ethernet payload	Data protection independent of the Layer 3 protocol
IP packet encryption	IPsec ESP encryption with tunnel-less option	Site-to-site IPsec over public or private networks
IP header option	IP header preservation or virtual IP address	Option to preserve the original IP address in the IPsec header allowing encrypted traffic to be load balanced
IP payload encryption	Layer 4 option	Preserves IP headers for MPLS traffic engineering
Encryption across different network layers	Define encryption rules for Layer 2, 3 and 4 payload encryption	Flexible configuration and deployment
Group policy creation	Group key distribution	Encryption for any-to-any connectivity in multicast, load balanced, or VLAN networks
Flexible policy control	Selectable policy type	Single device for Layer 2, Layer 3 or Layer 4 encryption

CEP1000 Technical Specifications

Encryption Support

- AES: FIPS 197 (256 bit keys) CBC mode

Authentication Methods

- X.509 v3 digital certificates
- Pre-shared secrets
- HMAC-SHA-1-96

Device Management

- CipherEngine
- Out-of band management (TLS and SSH)
- Alarm condition detection and reporting
- Syslog support
- SNMPv2C managed object support
- Audit log

Transforms

- CipherEngine Encapsulated Security Payload (ESP) Tunnel mode -Header preservation option
- CipherEngine Encapsulated Security Payload (ESP) Transport mode (L4 option)
- CipherEngine Ethernet Encapsulated Security Payload (L2 option)

Policy selector options

- Source IP address, destination IP address, source port number, destination port number, protocol ID (Layer 3 IP packet and Layer 4 payload options)
- VLAN ID (Layer 2 Ethernet encryption option)

Performance

- Up to 1.9Gbps full duplex AES encrypted throughput

Network Support

- Ethernet
- VLAN tag preservation
- MPLS tag preservation
- IPv4
- SNTTP

Interfaces

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

Regulatory

- Safety: UL 60950-1, First Edition (2001), CSA-C22.2 No. 60950-1 First Edition (2001), EN 60950-1:2001
- Emissions: FCC part 15 subpart B class B; CS IECS-003 Class B, ANSI C63.4 - 2003, EN 55022:2006 Class B, EN 61000-3-2:2006, EN 61000-3-3:1995/A1:2001/A2:2005, CE Marking - 2004/108/EC
- Immunity: EN 55024:1998/A1:2001/A2:2003, IEC 61000-4-2:1995/A2:2000, IEC 61000-4-3:2002, IEC 61000-4-4:2004, IEC 61000-4-5:1995/A1:2000, IEC 61000-4-6:1996/A1:2000, IEC 61000-4-8:1993/A1:2000, IEC 61000-4-11:1994 A1:2000, AS/NZS CISPR 22:2006 Class B

Environmental

- Operating temperature: 0° to 40° C (32° to 104° F)
- Operating humidity: up to 90% non-condensing
- Operating altitude: -200 to 10,000 feet AMSL
- EU WEEE
- EU RoHS-5

Physical

- 1U tamper evident chassis
- Dimensions 1.75"H x 17"W x 10"D
- Rack mountable in standard 19" rack
- Power: 100-240V A/C @ 4A, 50/60Hz, auto-sensing
- Nominal input current: 1.0A
- Weight: 6lbs

Indicators

- Power
- Alarm
- LED status

