

# CipherEngine Enforcement Point

## CipherOptics CEP100-XSA

### 100Mbps Network Encryptor

#### PRODUCT SNAPSHOT

- 100Mbps full-duplex (200Mbps aggregated), wire speed AES encryption
- Accommodates 18,000 Security Associations
- Layer 2 Ethernet frame, Layer 3 IP packet and Layer 4 payload protection
- Preserves VLAN and MPLS tags
- Create secure network groups
- FIPS 140-2 Level 2 Certified

#### FEATURES AND BENEFITS

- Network-wide encryption
  - Layer 2 Ethernet frame encryption
  - Layer 3 IPsec encryption
  - Layer 4 payload encryption
- Per frame/packet authentication
- Management and configuration
  - Global network security policy enforcement
  - Global encryption key creation and distribution
  - Easy installation and management
  - Seamless scalability

#### COMPREHENSIVE 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.**  
1401 Sunday Drive, Suite 109  
Raleigh, NC 27607  
Tel: +1.877.878.6655  
Fax: +1.919.233.9751  
info@cipheroptics.com  
www.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. For those networks that have several subnets at each node, the CEP100-XSA supports nearly 20,000 Security Associations and offers full-duplex line rate encryption at 100Mbps full-duplex (200Mbps aggregated) using the AES encryption algorithm.



CEP100-XSA

The CEP100-XSA enables organizations to standardize on one platform for small, medium or remote branch office networks. CipherOptics CEPs integrate easily into any existing network, operating transparently to the network and ensuring all of your data transmissions are encrypted.

#### Ethernet Frame Encryption

The CEP100-XSA 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 data based on the VLAN ID or they can simply encrypt all Ethernet frames.

#### IP Packet Encryption

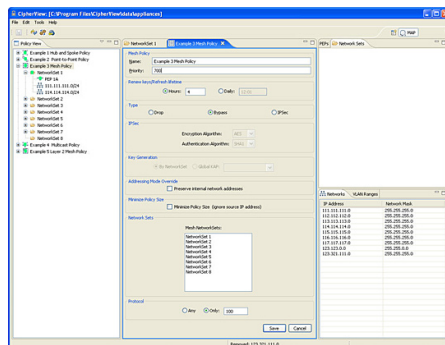
Using IP Security protocol (IPsec), the CEP100-XSA provides full data encryption for Layer 3 IP networks at 100Mbps full-duplex (200Mbps aggregated). The CEP family utilizes the CipherEngine Encapsulating Security Payload protocol (CE-ESP) to preserve the original IP packet header and encrypt just the payload. By preserving the original header information and encrypting only the payload, the CEPs can encrypt data over load-balanced, redundant and resilient 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. This unique capability allows network services such as Netflow and Network Address Translation (NAT), which utilize information in the Layer 4 header, to continue to operate while the data is encrypted.

#### Central Policy Management

Configuring and managing CEPs is easy with CipherOptics CipherEngine. Within the CipherEngine policy and key manager, CEPs can be assigned to groups, called Network Sets. Each CEP in a given Network Set is given the same encryption key material. This grouping capability greatly reduces the complexity of large-scale IP encryption deployments and enables fully meshed, any-to-any encryption for all network traffic on any network.



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

CipherEngine provides granular control over what gets encrypted on the network. Traffic encryption is set by policy definition and can be based on source IP address, destination IP address, source port number, protocol ID, or VLAN tag ID. 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 network.

# CipherEngine Enforcement Point

CipherOptics CEP100-XSA

## 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 Layer 4 encryption	Flexible configuration and deployment
Group policy creation	Group key distribution	Allows for encrypted groups based on VLAN associations or topology (any-to-any, hub and spoke, or multicast)
Flexible policy control	Selectable policy type	Single device for Layer 2, Layer 3 or Layer 4 encryption

## CEP100-XSA 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 with 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 100Mbps full-duplex (200Mbps aggregated) full-duplex AES encrypted throughput

### Network Support

- Ethernet
- VLAN tag preservation
- MPLS tag preservation
- IPv4
- SNTP

### Interfaces

- Data interfaces: Two 10/100Mbps RJ45 Ethernet ports
- Management interfaces: One 10/100 RJ45 Ethernet and one RS232 serial port
- Auxiliary interface: One 10/100Mbps RJ45 Ethernet 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 A; CS IECS-003 Class A, ANSI C63.4 - 2003, EN 55022:2006/ A1:2007 Class A, 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 A

### Environmental

- Operating temperature: 0° to 40° C (32° to 104° F)
- 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
- Thermal: In-rush 155 BTU/hr, Steady-state 140 BTU/hr
- Nominal input current: 1.0A
- Weight: 6 lbs

### Indicators

- Power
- Alarm
- LED status

### Certifications

- FIPS 140-2 Level 2



**CIPHER OPTICS**  
www.CipherOptics.com