

CEP100-XSA

1 Gbps Network Encryptor

Product Overview

The Certes 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 1 Gbps full-duplex (2 Gbps aggregated) using the AES encryption algorithm.

The CEP100-XSA enables organizations to standardize on one platform for small, medium or remote branch office networks. The CEP100-XSA integrates 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 CEP100-XSA, each and every Ethernet frame is authenticated. The CEP100-XSA 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 1 Gbps full duplex (2 Gbps aggregated) AES encrypted throughput (line rate for 128 Byte frame sizes and larger). The CEP100-XSA utilizes the Certes 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 CEP100-XSA 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 CEP100-XSA offers 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

The CEP100-XSA can be configured and centrally managed via the TrustNet Manager. TrustNet allows both security and network administrators to quickly and easily manage network security from a centralized interface with simple yet powerful drag and drop policy creation capability. 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. TrustNet Manager also provides logging and audit mechanisms to meet or exceed compliance and audit requirements.



PRODUCT SNAPSHOT

- 1 Gbps full-duplex (2 Gbps 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

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

CEP100-XSA

1 Gbps Network Encryptor

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

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

Transforms

- Certes Encapsulated Security Payload (ESP) Tunnel mode with header preservation option
- Certes Encapsulated Security Payload (ESP) Transport mode (L4 option)
- Certes 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

- 1 Gbps full duplex (2 Gbps aggregated) AES encrypted throughput (line rate for 128 Byte frame sizes and larger)

Network Support

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

Interfaces

- Data interfaces: Two 10/100/1000Mbps 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

Global Headquarters

300 Corporate Center Dr., Suite 140
Pittsburgh, PA 15108
Tel: +1 (888) 833-1142
Fax: +1 (412) 262-2574
www.CertesNetworks.com
sales@certesnetworks.com

EMEA Sales

emea@certesnetworks.com

Asia-Pacific Sales

apac@certesnetworks.com

Government Sales

fedsales@certesnetworks.com