CERTES NETWORKS

Datasheet

CEP10G VSE

FIPS Validated 10Gbps Multi-Layer Encryptor

Product Overview
The CEP10G VSE is a multi-layer 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 IP and MPLS networks. Like other members of the Certes Variable Speed Encryptor (VSE) product family, the CEP10G VSE offers a range of encryption speeds based on software licenses using AES-256 at speeds of 500Mbps, 650Mbps and 1, 2.5, 5 or 10Gbps (full duplex).

The CEP10G VSE enables organizations to standardize on one platform for any large campus or data center network. The CEP10G integrates easily into any existing network, operating transparently to the network and ensuring all of your data transmissions are encrypted. And unlike many other encryption appliances, the CEP10G provides per frame and per packet authentication on an ongoing basis to ensure that both the data and the communication streams are uncompromised.

Scalable and Secure Group Encryption
The CEP 10G uses Certes Networks' web-based management platform, TrustNet Manager, to securely generate and distribute group keys to authorized endpoints. By avoiding the use of IPsec tunnels, group encryption greatly reduces deployment complexity and provides fully meshed encryption that is easy to manage. The solution is also compatible with load balancing, highly available network designs, QoS and network monitoring tools.

Ethernet Frame Encryption
The CEP10G is compatible with all Layer 2 unicast, multicast, point-to-point, and multipoint-to-multipoint topologies. It also authenticates all Ethernet frames, preventing man in the middle attacks. Encryption polices can be based on VLAN ID's for cryptographic segmentation of data, or can be set to encrypt all Ethernet frames.

Persistent authentication of frames ensures that the data received at the remote end of a connection originated from a trusted source. While encryption directly protects data, without authentication, data streams remain vulnerable to modification from man in the middle attacks. Unlike many encryption solutions, the CEP10G provides continuous authentication to ensure that both the data and the communication streams are uncompromised. Without both, the network and data are less than secure.

IP Packet Encryption
Using the IP Security (IPsec) protocol, the CEP10G provides full data encryption for Layer 3 IP networks. The CEP10G utilizes the Certes Networks Encapsulating Security Payload protocol (CN-ESP) to encrypt the IP packet, while preserving the original IP header. This unique functionality maintains network transparency, while providing maximum data protection. By preserving the original header and encrypting only the payload, the CEP10G can protect data over any IP 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 CEP10G 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, to be maintained through the service provider network while the payload itself is encrypted.

Central Policy Management
The CEP10G VSE can be configured and centrally managed via the Certes TrustNet Manager™. TrustNet Manager 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 FAMILY
- Encrypted throughput from 500Mbps to 10Gbps
- Layer 2 Ethernet frame, Layer 3 IP packet, and Layer 4 payload protection
- Per-frame/packet authentication
- Microsecond latency
- Preserves VLAN and MPLS tags

FEATURES AND BENEFITS
- Multiple encrypted throughput options
- Transparent to network and applications
- Seamless scalability
- Infrastructure neutral
- Easy installation and management
- Create secure network groups
- FIPS 140-2 Level 2 Validated
- Common Criteria EAL4+ Certified

COMPREHENSIVE DATA PROTECTION
- IPsec site-to-site networks
- MPLS meshed networks
- Metro Ethernet and VPLS networks
- Voice and video over IP applications

CERTES NETWORKS

Datasheet

CEP10G VSE

10Gbps Multi-Layer Encryptor

Performance (Encrypted Throughput)
- 500, 650 Mbps and 1, 2.5, 5 or 10 Gpbs

Security
- Encryption: AES-CBC (256 bit) (FIPS 197), Triple-DES-CBC (168 bit) (NIST 800-67)
- Authentication (Message Integrity): HMAC- SHA-256-96 (FIPS 180-3, FIPS 198)
- Signature generation and verification: ANSI X9.31, RSASSA-PS, RSASSA-PKCS v1.5, DSA FIPS 186-2
- Management session authentication: RSA, DSS
- Automatic or manually triggered hitless key rotation
- Group keying with TrustNet Manager SSL/TLS (bilateral authentication) based on certificates
- Certificate revocation: OCSP (RFC 2560), CRL (RFC 5280)
- IPSec (RFC 2401) for Layer 3 encryption
- IKE in Layer 2 peer-to-peer mode (RFC s 2407, 2408, 2409)

Network Support
- Ethernet
- VLAN tag preservation
- MPLS tag preservation
- IPv4
- IPv6 (Layer 2 Ethernet encryption mode)
- Secure 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
- Certes Networks ESP Tunnel Mode (header preservation option)
- Certes Networks ESP Transport Mode (L4 option)
- Certes Networks Ethernet ESP Mode

Indicators
- Power
- LED Status
- Link Status
- Encrypting
- 2x8 segment diplay

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

Device Management
- TrustNet Manager
- Command Line Interface
- Out-of-band management
- SNMPv2c and SNMPv3 managed object support
- Alarm condition detection and reporting (traps and SNMP alarm table)
- Syslog support
- Audit Log

Management Communication Security Options
- X.509 v3 digital certificates
- TLS (full bilateral authentication)
- SSH

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

Physical
- 2U tamper resistant chassis
- Dimensions: 3.5" x 17" x 15" (89mm x 432mm x 381mm)
- Rack mountable in standard 19 inch rack
- Dual hot-swappable AC power: 100-240 V AC, 350 W max output (per supply), 50-60 Hz auto-sensing
- Maximum AC input current: 8 A (per supply)
- Dual hot-swappable DC power: -36 V DC to -72 V DC, 350 W max output (per supply)
- Maximum DC input current: 15 A (per supply)
- Customer replaceable fan assemblies
- FIPS 140-2 level 2 validated (Certificate # 1797)
- Common Criteria EAL4+ Certified
- Hardware designed to meet FIPS 140-2 Level3 requirements
- Weight: 22 lbs
- MTBF: 106,376 hours

Interfaces
- Data: Two full-duplex 10 Gigabit Ethernet ports with
- SFP+ interfaces (single mode or multimode)
- Management: One 10/100/1000 Ethernet RJ45, one Gigabit Ethernet (SFP) and one RJ45 serial port
- Three full-duplex Gigabit Ethernet ports with SFP interfaces (single mode, multimode or copper) or three full-duplex 10/100/1000 Ethernet ports with RJ45 interfaces (reserved for future use)
- Two USB ports (reserved for future use)

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

North America Sales
sales@certesnetworks.com

Government Sales
fedsales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
cala@certesnetworks.com

Europe, Middle East and Africa Sales
emea@certesnetworks.com