CERTES NETWORKS

Product Brochure

vCEP: Virtual Certes Enforcement Point

Multilayer Encryption Virtual Appliance

Overview

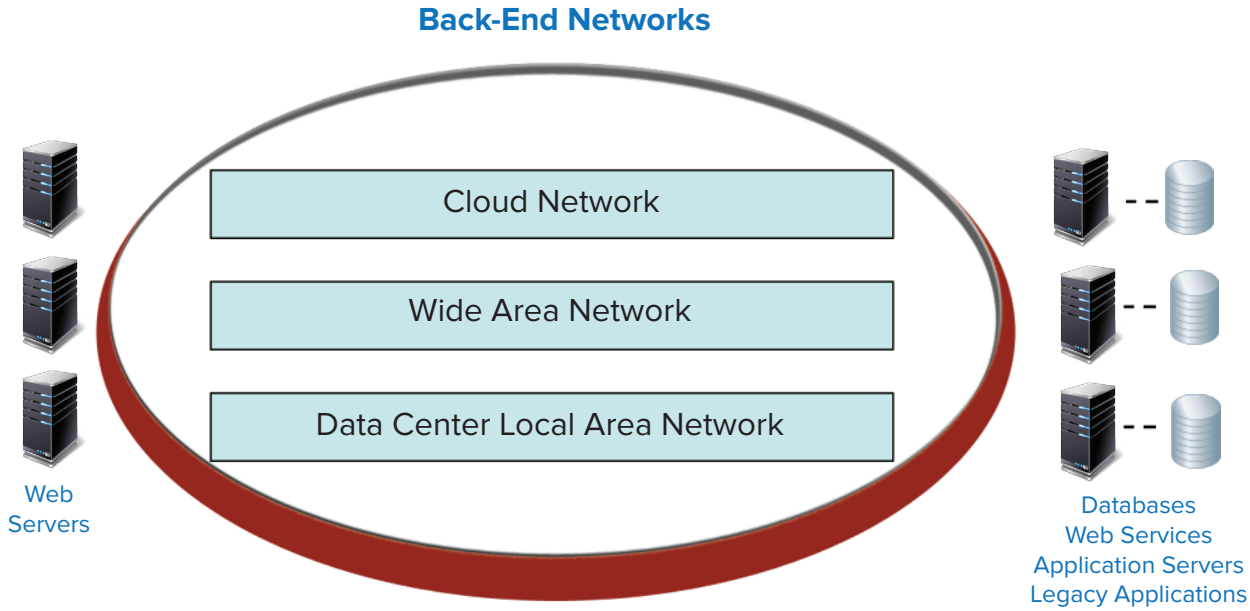
Utilizing cloud infrastructures provides a compelling case for cost savings, agility and operational efficiency that cannot be ignored. However, executing IaaS (Infrastructure as a Service) workloads in the cloud while protecting sensitive information has been challenging in the past. The virtual Certes Enforcement Point (vCEP) solves the problem of keeping sensitive information secure in shared cloud or virtualized environments. The vCEP preserves the cost savings, agility and operational efficiency of the cloud while securing the data. In so doing, it extends the use of IaaS clouds to sensitive or regulated workloads that were previously off limits due to security concerns.

What is the vCEP?

The vCEP is a virtual appliance for VMware ESX/ESXi environments that enables sensitive workloads to execute and communicate securely in untrusted networks. The vCEP provides data confidentiality and integrity for sensitive data in motion in shared environments and prevents one tenant from monitoring the network traffic or attacking the virtual servers of another tenant. Furthermore, the vCEP allows the data owner or a trusted third party to control the encryption keys without the need to share the encryption keys to the infrastructure provider.

How is the vCEP used?

The vCEP protects back-end networks where secure full mesh connectivity among many virtual and physical servers is required. In combination with TrustNet physical CEPs, the vCEP is used to protect communication among multiple data center sites and virtual servers in cloud environments.

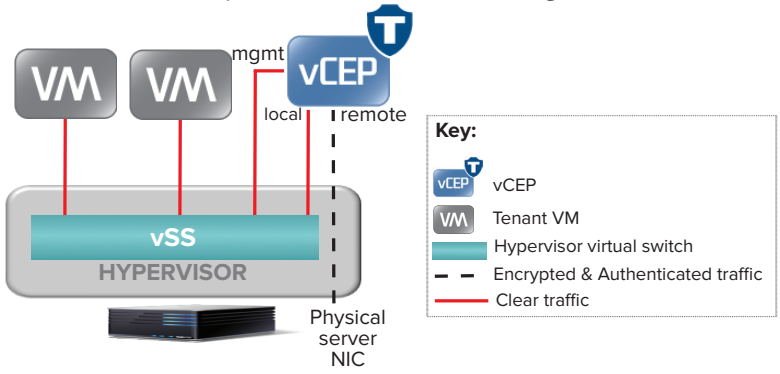


vCEP

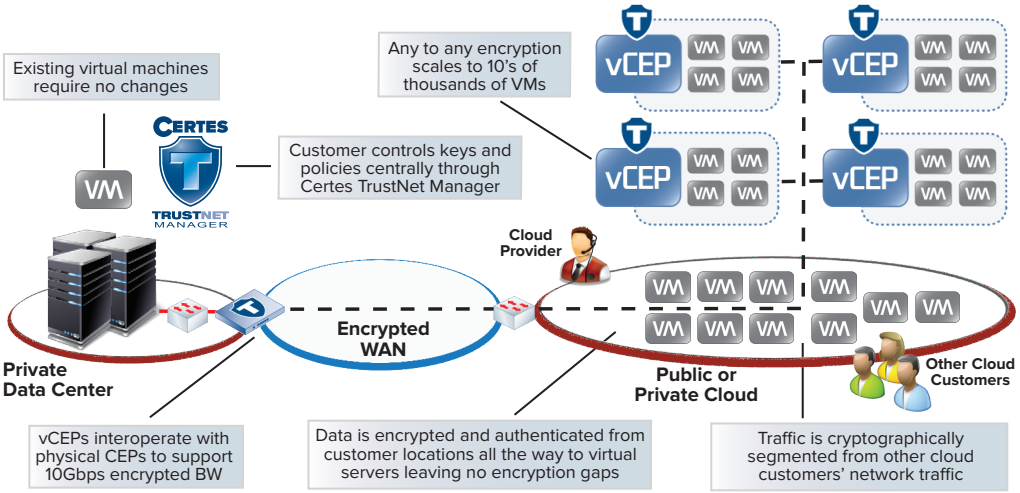
How does it work?
The vCEP uses proven Certes TrustNet group encryption technology to provide scalable network encryption without tunnels. The vCEP protects one or more virtual servers by enforcing the encryption and isolation policies specified in Certes TrustNet Manager (the centralized key and policy management system for TrustNet appliances). TrustNet Manager is designed for automated policy provisioning and integration with cloud operating environments.

The vCEP is a bump in the virtual wire that connects between tenant VMs and the rest of the network using virtual network switches that are built into the hypervisor. This allows the vCEP to protect VMs without adding software to the VMs and without requiring custom hypervisor changes.

The diagram below illustrates how the vCEP is typically connected to the rest of the network. The vCEP has three network interfaces: Local, Remote, and Management. The Local interface of the vCEP connects to the trusted network on which the protected VMs reside using a Virtual Standard Switch (vSS) to switch all of the traffic to and from the protected VMs through the vCEP. This allows the vCEP to apply encryption and authentication policies to the traffic. The vCEP's Remote interface connects to the shared (untrusted) network. The vCEP remote interface can be connected directly to the physical server's network interface card (NIC), or it can be connected to a different vSS or even a Virtual Distributed Switch (vDS). The vCEP's Management interface is used to manage the vCEP and it can be bridged to the trusted network or connected to a separate out-of-band management network.



What are the benefits?
The vCEP solves a number of problems with protecting sensitive information in shared cloud environments. These are illustrated in the diagram below and further explained in the following sections.



The vCEP provides full-mesh encrypted and authenticated connectivity for back-end virtual servers, regardless of where they are deployed. As a virtual appliance that resides on the same server as the virtual servers that it protects, the vCEP protects sensitive network traffic inside the cloud provider's network without leaving gaps where the data is not protected.

Scalable Group Encryption
With TrustNet group encryption, the same group encryption keys are centrally generated and securely distributed to all of the authorized group members. Each group member can communicate securely with the other group members without the performance and maintenance overhead of tunnels. Group encryption is designed to scale to protect thousands or even tens of thousands of servers.

Protect without Gaps
IPSec tunnels protect network traffic between client data centers and the front door of the cloud, but data inside the cloud network remains vulnerable to attack. Given the issues with scalability, management and performance that IPSec tunnels cause, they have limited applicability within cloud networks. Similarly, SSL/TLS encryption provides point-to-point encryption between the web browser and web server, but it does not protect the back-end network used by web servers, application servers and databases. In fact, many network encryption solutions for cloud environments do not encrypt traffic within the cloud environment.

The vCEP provides full-mesh encrypted and authenticated connectivity for back-end virtual servers, regardless of where they are deployed. As a virtual appliance that resides on the same server as the virtual servers that it protects, the vCEP protects sensitive network traffic inside the cloud provider's network without leaving gaps where the data is not protected.

Control of the Keys
An important benefit of the vCEP is its ability to allow the client to maintain control of their own policies and encryption keys. This is essential for regulatory compliance and it protects both the data owner and the infrastructure provider. The vCEP provides a safe harbor for most data privacy regulations by leveraging Certes TrustNet standards-based encryption, which has been deployed and proven across a broad range of industries to achieve compliance for data privacy including finance, healthcare, government, retail and utilities. This also benefits the cloud provider by removing the potential legal burden associated with being in possession of the encryption keys.

Regulatory Compliance
While maintaining control of the encryption keys is essential for regulatory compliance, it is not enough. TrustNet and the vCEP also provide auditing and logging capabilities that allow you to monitor security events and prove encryption is enabled in untrusted networks.

Cryptographic Isolation from other Tenants
As part of the Certes TrustNet solution the vCEP provides persistent authentication to ensure continuous data integrity. Authentication and encryption provide cryptographic isolation among cloud tenants. Cloud providers today typically offer only logical isolation, which can break down and allow one tenant to attack another due to misconfiguration, unauthorized wiretaps or man-in-the-middle attacks. Data that is encrypted and authenticated using keys managed by the cloud customer is not susceptible to these types of attacks.

No Changes to Virtual Servers
The vCEP is a bump in the virtual wire, so tenant VMs execute in the cloud with no changes. There is no need to add new endpoint software nor is there a need to use a custom hypervisor version. This makes it easy to migrate workloads from virtualized data centers and private clouds to public cloud environments.

Interoperate with Wire-Speed Physical CEPs
In some cases physical encryption appliances are more appropriate than virtual appliances. Certes TrustNet CEP (physical) appliances provide line rate bidirectional encrypted and authenticated throughput up to 10 Gbps with only microseconds of latency. The vCEP interoperates with high-performance CEP appliances to provide flexibility in choosing combinations of virtual or physical appliances. A TrustNet solution combining vCEPs and CEPs is ideal for securing sensitive workloads between data centers and untrusted or shared cloud or virtualized environments.

vmware READY

Multi-layer Encryption: Protect any Network
The vCEP and CEP family can encrypt at Layer 2, Layer 3 or Layer 4 of the OSI network stack. This unique multi-layer encryption capability provides tremendous flexibility in protecting network traffic in the data center local area network (LAN), wide area network (WAN), and private, hybrid, public or community IaaS cloud networks.
As high bandwidth and low latency Ethernet connectivity becomes more widely available, it will likely become the most cost-effective option for many organizations to connect existing data centers to the cloud. Multi-layer encryption provides the flexibility to choose the best network connectivity without requiring a forklift upgrade.

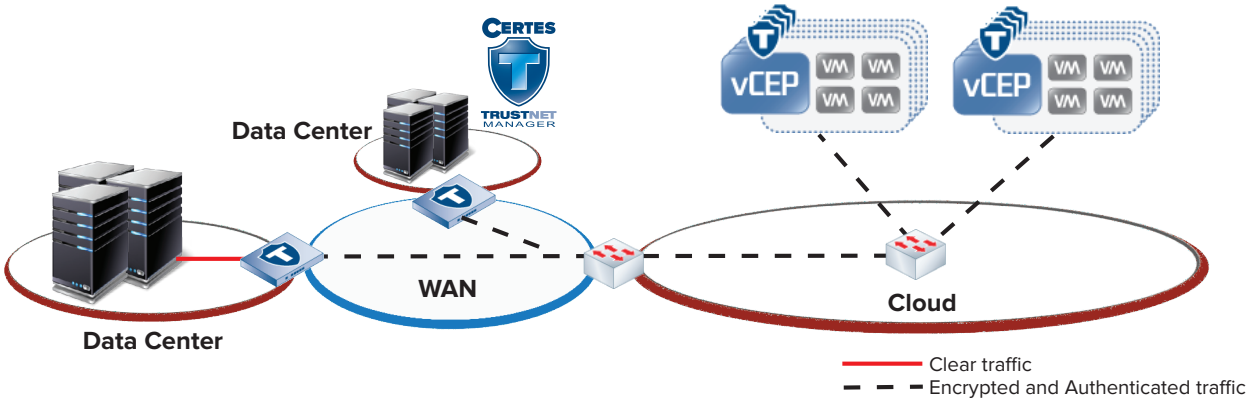
Central Policy Management
The vCEP can be configured and centrally managed via Certes TrustNet Manager. TrustNet Manager allows both security and network administrators to quickly and easily manage network security from a centralized interface with simple yet powerful drag and drop policy creation. Encryption policies can be based on flexible combinations of 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.

Use Cases

Cloud Migration

Application: Extend data centers to execute workloads in IaaS cloud environments

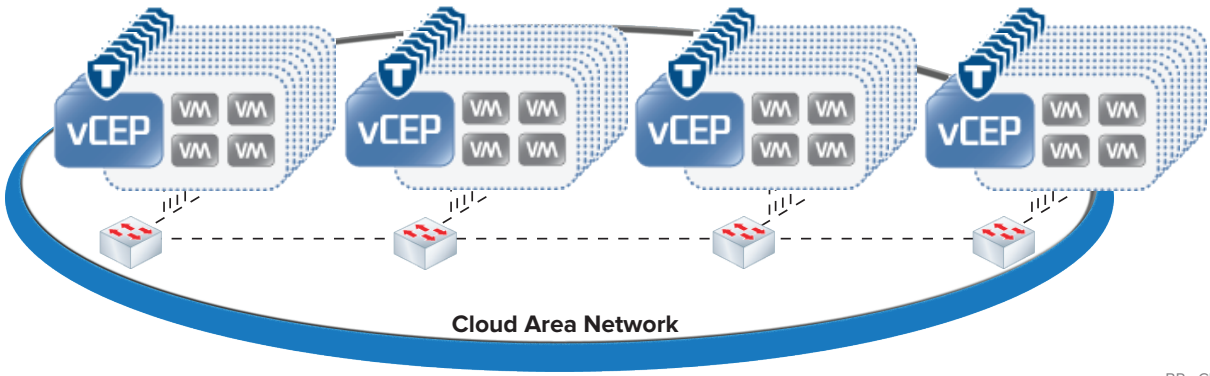
Solution: Protect sensitive traffic among data centers and virtual servers in the cloud using full-mesh connectivity among vCEPs and CEPs.



IaaS Cloud

Application: Protecting traffic among VMs in an untrusted cloud network

Solution: Encrypt at Layer 2 among virtual servers on the same VLAN in the cloud network or encrypt at Layer 3 or Layer 4 among virtual servers that are not on the same VLAN.

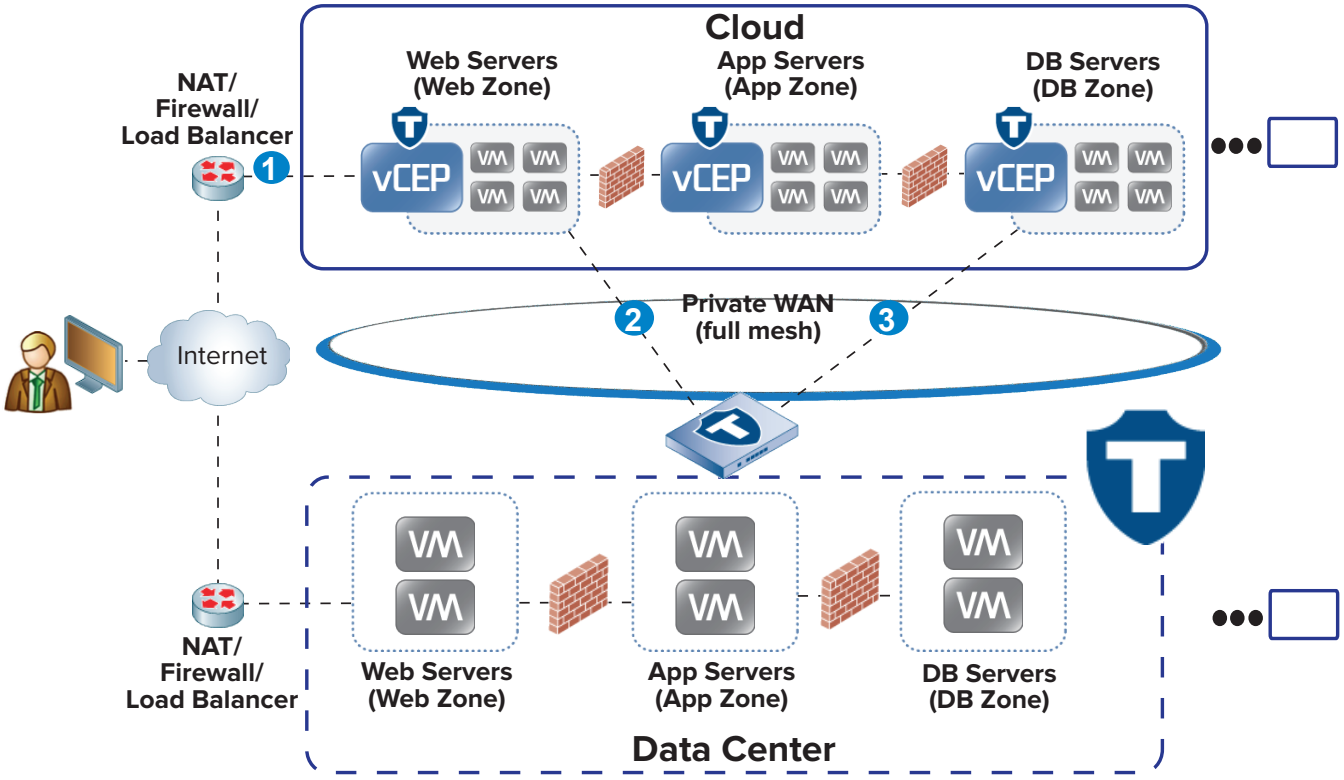


Cryptographic Segmentation
The vCEP provides cryptographic and policy-based isolation and encryption among security zones (for example: web, application and database zones) among multiple sites. This solution protects the Back-End network (behind the Web Servers) with full-mesh encryption, without the need to establish new SSL/TLS sessions for every new connection. This allows cloud-based servers to operate in the same way as they do in the data center. An example is shown in the figure below.

1. Web browser connects to Web server (in the cloud) via SSL/TLS (encrypted)

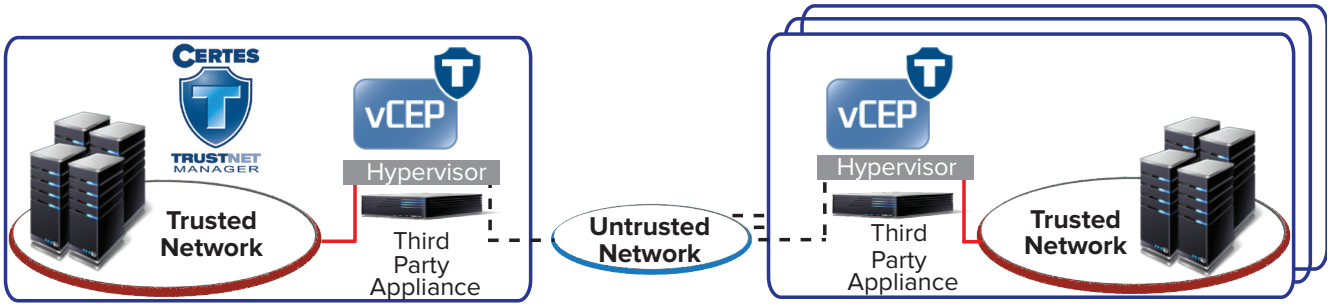
2. Web browser connects to App server (in the data center) protected by vCEP/CEP

3. App connects to DB server (in the cloud) protected by vCEP/CEP



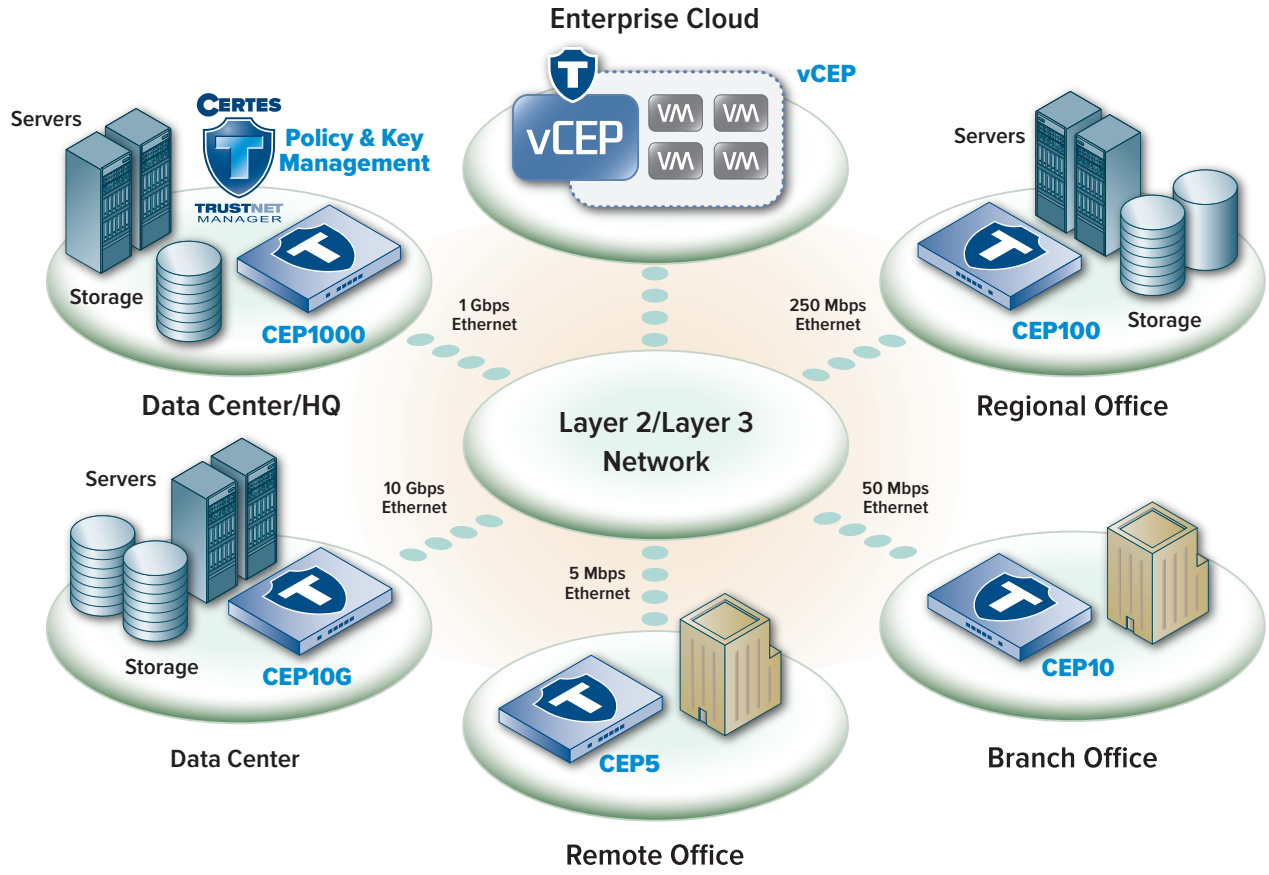
Third party appliances

There are a number of physical appliances on the market today that allow virtual appliances to be connected in series with the functional blocks of the appliance. Examples include firewalls, load balancers, and WAN optimization appliances. The vCEP supports this deployment scenario as shown in the diagram below, where the vCEP is loaded on a third party appliance. If the appliance uses the VMware hypervisor with a vNetwork Standard Switch (vSS), then the vCEP can be loaded onto the appliance in order to implement TrustNet group encryption.



Certes TrustNet Solution

The vCEP is a fully interoperable part of the Certes Networks family of products. In combination with Certes TrustNet Manager and the full line of CEP encryption appliances, organizations can ensure complete data protection across their entire network regardless of scale, scope or technology.



Technical Specifications

Performance

- Up to 570 Mbps for 1024 Byte packets of encrypted and authenticated traffic using AES-256 encryption *
- Encryption Acceleration using AES-NI Instructions
- Multi-CPU/Multi-core Support

* Actual performance may vary depending on the network traffic and system configuration. Performance results were observed using a Dell PowerEdge R210 server that cost less than $1500 (3.4 GHz Quad-core Xeon processor with AES-NI support and GigE NICs) running ESXi 5.0 Update 1

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

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

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
- IKE/IPsec

System Requirements

- CPU: Any x86 architecture supported by VMware
- Hypervisor: VMware ESX 4.1 U2, VMware ESXi 5.0 U1, or VMware ESXi 5.0
- Memory (RAM): 128 MB (minimum)
- Hard Drive Space (footprint): 2 GB (minimum)
- CPU: Any x86 architecture supported by VMware

Interfaces

- Virtual network interface to the local trusted network
- Virtual network interface to the external untrusted network
- Virtual management interface (out of band)
- May be bridged to the Local interface for in-band management
- vNetwork Standard Switch (VSS) compatible

CERTES NETWORKS

Product Brochure

vCEP

vCEP Features, Benefits and Value

Feature	Benefit	Value
Communicate securely between data centers and among virtual servers running in IaaS clouds	Makes the cloud safe for sensitive workloads	**Reduce IT costs** by using shared cloud and virtualized environments for sensitive workloads **Migrate smoothly to cloud services** while encrypting between data centers and cloud networks
Scalable group encryption	Secure full-mesh connectivity among servers and networks without tunnels	**Scale to cloud proportions** by starting with a scalable architecture and avoiding a costly re-architecture later
Virtual appliance to protect virtual servers	Protection extends to the virtual servers within the cloud network	**Protect the network without gaps** that expose sensitive data
Control the encryption keys and policies centrally from Certes TrustNet Manager	**Retain control of sensitive information** by controlling the encryption keys	**Comply with regulatory requirements** and security best practices to protect sensitive information in shared environments
Packet-by-packet continuous authentication	**Isolate** assets with cryptographic separation (vs. logical separation)	**Block traffic and attacks from other cloud tenants** to protect cloud assets
Virtual appliance acts as a bump in the virtual wire	Tenant VMs run in the cloud without changes (No software or drivers to load and maintain on tenant VMs and no hypervisor modifications required)	**Simplify migration** to cloud environments
The vCEP interoperates with Certes high-performance CEP appliances (up to 10 Gbps)	Choose a combination of virtual or physical appliances	**Cost-effective** solution to achieve network design goals
Multi-layer encryption (Layer 2, Layer 3, Layer 4)	Flexible solution for VLAN-based L2 networks in virtualized data centers or IP networks of public IaaS clouds	**Protect any network**
Centralized key and policy management with TrustNet Manager	Simplify encryption management	**Reduce operational expenses** while maintaining the encrypted network

Ordering Information

The vCEP is distributed as a perpetual software license with support for up to thirty -two virtual CPUs (vCPUs). Adding vCPUs to the vCEP typically increases peak bandwidth performance, but performance is extremely dependent on the host server configuration. Increasing the number of vCPUs allocated to the vCEP VM may or may not improve peak bandwidth.

vCEP Virtual Appliance	Max. vCPUs Supported	Description
VCEP-CPU-01	1	vCEP virtual appliance for multi-layer encryption and authentication. Delivered as an Open Virtualization Archive (.OVA) file. Includes one perpetual software license to operate a single vCEP virtual appliance on a single server with [1-32] virtual CPU(s) allocated to the vCEP virtual appliance. vCEP-CPU-xx licenses include one license for TrustNet Manager (TRUSTNET-MGR-SW).
VCEP-CPU-02	2	
VCEP-CPU-04	4	
VCEP-CPU-08	8	
VCEP-CPU-16	16	
VCEP-CPU-32	32	

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