vCEP: Virtual Certes Enforcement Point

Multi-Layer Encryption Virtual Appliance

Certes vCEP 為 VMWare vSphere 或 ESX/ESXi 環境中運作的虛擬裝置，確保在不受信任的網路環境中，機敏的資料能夠安全地進行傳遞。在動態及共用的環境裡，vCEP 提供機敏資料的保密性與完整性。向租用雲服務供應商的虛擬環境中，vCEP 能夠有效地防止雲服務租用者對另一個雲服務使用者進行網路流量監測或是攻擊虛擬伺服器。此外，vCEP 將加密金鑰的所有權掌握在資料的所有者或是受信任的協力廠商，而不是交由雲服務供應商來控制與持有加密金鑰。

Certes vCEP 使用經過驗證的 TrustNet 群組加密技術，提供可擴充的加密範圍，而無需事先建置加密通道（Tunnel）。vCEP 透過 TrustNet Manager 中央網管平台統一進行金鑰與加密規則管理，能夠指定加密或隔離單一或多個虛擬伺服器。在雲運行環境下，TrustNet Manager 中央網管平台能夠自動化進行配置與整合加密規則。

Certes vCEP 具有以下幾點優勢：

》 Scalable Group Encryption

無通道全網狀（Full-mesh）網路加密

》 Protection without Gaps

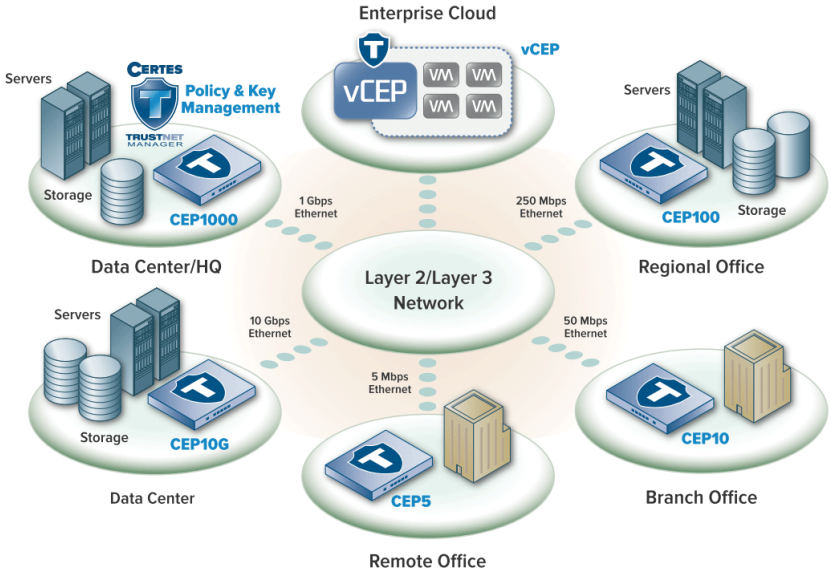
無縫進行虛擬伺服器間網路傳輸加密

》 Control of the Keys

可自行控管加密金鑰與加密規則，不需透過與雲端或虛擬服務供應商

》 Regulatory Compliance

具備日誌記錄以符合稽核需求，並且證明加密正常運作



》 Multi-layer Encryption

資料安全防護涵蓋任何網路，LAN、WAN 、私有雲、混合雲、公有雲或 IaaS 雲

》 Cryptographic Isolation from other Tenants

持續性身分驗證可防止從其他雲服務租用者在共享的網路或多重雲服務租用者的環境中進行以網路為基礎的攻擊事件

》 Simplify Migration to the Cloud

對於原有虛擬機器無需改變任何現有環境。不需載入與安裝軟體或驅動程式，無需修改系統管理程式

》 Physical CEP interoperability

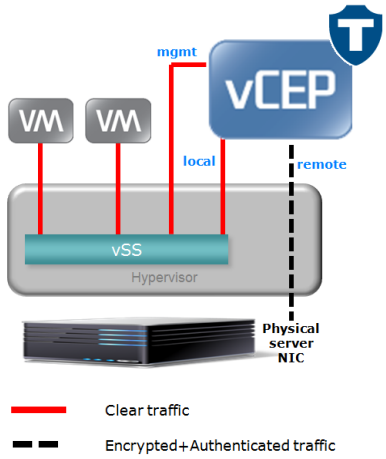
可與實體加密設備（CEP）整合使用，提供並加強雲端及資料中心之間的網路傳輸安全

》 Central Management

透過中央控管平台（web-based）迅速管理網路傳輸加密狀態

代理商 瑞奇數碼股份有限公司
台北市內湖區港墘路 26 巷 9 號 1 樓
TEL 02-26581786 | www.richsmt.com

vCEP 如何運作？



vCEP 透過三個網路介面：本地(Local)、遠端(Remote)和管理(Management)介面運行於虛擬網路中。

首先，本地介面連接到可信任的網路上，透過 Virtual Standard Switch（vSS）將同一 Hypervisor 的流量導入 vCEP，如此一來，流量可透過 vCEP 進行加密以及資料驗證並且符合 vCEP 上所制定的加密規則。而 vCEP 遠端介面連接到共用的（不受信任的）網路上，直接連接到實體的伺服器網路介面卡（NIC），或連接到不同的 Virtual Standard Switch（vSS），甚至是 Virtual Distributed Switch（vDS）上。

vCEP 管理介面則是用於管理 vCEP，能夠橋接到可信任的網路或者是連接到單獨的頻外管理網路。

技術規格

效能

- 傳輸效能高達 570Mbps，使用 AES-256bits 加密以及 SHA-1 雜湊演算法驗證於封包大小 1024bytes。 * 註
- 可透過 AES-NI 指令加速加密效能。
- 支援多 CPU 及多核心虛擬機器

* 註 實際效能會因網路流量及系統組態有所影響。
Performance results were observed using a Dell PowerEdge R210 server that cost less than $1500 USD (3.4 GHz Quad-core Xeon processor with AES-NI support and GigE NICs) running ESXi 5.0 Update 1

安全性

- 加密方式：AES-CBC (256 bits) (FIPS 197)
  3DES (168 bits) (NIST 800-67)
- 資料驗證（資料完整性）: HMAC-SHA-1-96,
  HMAC- SHA-256-96 (FIPS 180-3, FIPS 198)
- 簽章產生與驗證：ANSI X9.31, RSASSA-PS, RSASSA-PKCS v1.5,
  DSA FIPS 186-2
- Management Session 驗證：RSA, DSS
- 可自動或手動觸發金鑰交換，交換過程不會中斷連線。
- 群組金鑰由 TrustNet Manager 透過憑證經由 SSL/TLS（雙邊認證）配送。
- 憑認證撤銷：OCSP (RFC 2560), CRL (RFC 5280)
- Layer 3 採用 IPSec (RFC 2401)加密方式
- 在 Layer 2 點對點加密模式可採用 IKE (RFC s 2407, 2408, 2409)

系統需求

- 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)

網路支援

- 乙太網路
- VLAN 標籤保護
- MPLS (多協定標籤交換)標籤保護
- IPv4
- NTP
- IPv6 (L2 乙太網路加密模式)

管理

- TrustNet Manager
- 命令列介面
- 頻外（Out-of-band）管理
- 告警狀況偵測和回報
- 支援系統記錄 （Syslog）
- SNMP v2c / v3 管理物件支援
- 稽核日誌（Audit log）

加密規則（Policy）選項

- 來源或目的 IP address
- 來源或目的 Port number
- 通訊協定 ID（L3 和 L4 選項）
- VLAN ID（L2 選項）
- Multicast 位址

管理通訊安全選項

- X.509 V3 數位認證
- TLS（全認證）
- SSH
- IKE/ IPSec

轉換

- Certes Networks ESP 通道模式
  （header 保存選項）
- Certes Networks ESP 傳輸模式
  （L4 選項）
- Certes Networks 乙太網路 ESP 模式

代理商 瑞奇數碼股份有限公司
台北市內湖區港墘路 26 巷 9 號 1 樓
TEL 02-26581786 | www.richsmt.com