

虛擬傳輸加密解決方案

The virtual encryption solution

Certes 虛擬傳輸加密解決方案為多層加密架構，可針對Layer 2 乙太網路Frame加密、Layer 3 網路IP封包加密和Layer 4通訊協定加密於 IP與MPLS (多協定標籤交換) 網路。採用AES-256bits演算法支援1Gbps網路加密頻寬，企業不需另外添購設備即可應付日漸增加的網路流量。

》具可擴充性的安全群組加密

透過中央網管平台可達成：

1. 建立加密群組 (Group) 。
2. 設定加密規則 (Policy) 。
3. 產生與派送金鑰 (Key) 給群組內的加密器。
4. 隨時可新增或移除群組內的加密器。

有別於傳統的IPSec加密產品，Certes 虛擬解決方案並非使用IPSec通道，可建立全網狀加密，真正達成Any-to-any connectivity，大幅減低佈署的複雜性。此解決方案也相容於負載平衡、高可用性網路設計、服務品質 (QoS) 和網路監控工具。

》集中式加密規則 (Policy) 管理

透過中央網管平台進行配置和集中管理。採用拖曳式建立加密規則 (Policy) 功能，直覺式操作既省時又便利。在大型的網路上，仍可快速方便地在幾秒鐘內進行加密規則 (Policy) 修改，而無流量中斷或需遠端人員的互動。

加密方式 Encryption Support

- > AES-GCM-256
- > AES-CBC-256

網路 Network

- > 乙太網路
- > VLAN標籤保護
- > MPLS(多協定標籤交換)標籤保護
- > IPv4
- > NTP

認證和完整性 Authentication and Integrity

- > HMAC-SHA2-256
- > HMAC-SHA2-512

資源需求Hypervisors

- > KVM
- > VMware ESXi 5.5 and higher

規格需求 Transforms

- > 建議規格
2vCPUs、4G RAM、30GB Disk Size
- > 最低規格
2vCPUs、2G RAM、10GB Disk Size

產品特色

- ▣ 傳輸速率1GBPS
- ▣ Layer 2 乙太網路Frame、Layer 3 IP封包、Layer 4 Payload保護
- ▣ Per-Frame/Packet認證
- ▣ 微秒等級的延遲
- ▣ 保留VLAN和MPLS (多協定標籤交換) 標籤

特點及效益

- ▣ 多重加密傳輸量
- ▣ 低延遲、零負載透過模式
- ▣ 無縫的可擴充性
- ▣ 易於安裝與管理
- ▣ 建立安全的網路群組

全面性保護

- ▣ IPSec點對點網路
- ▣ MPLS網狀網路
- ▣ 都會區乙太網路及 VPLS (虛擬私有區域網路服務) 網路
- ▣ 語音及VoIP應用