

ST Engineering NetCrypt Administrative Management

ST Engineering - NetCrypt Series 網路加密系列方案，利用一系列高性能 IP 加密器作為辦公室企業 LAN、站點到站點 VPN、移動車輛、堅固部署或無線辦公室間連接的安全網關。使用 NetCrypt 系列，您可以安全地連接到多個站點(由 AES 算法和內置防火牆提供支持)。

方案特點：

- 通過我們的密鑰管理系統使用獨特的加密密鑰增強安全性
- 可定制的算法可用於保護傳輸中的數據
- 可部署為辦公室企業 LAN、站點到站點 VPN、移動車輛、堅固部署或無線辦公室間連接的安全網關
- 能夠配置為第 3 層或第 2 層加密隧道設備以滿足所需的各種基礎設施要求

NetCrypt Administrative Management 是一套全面的管理軟體，提供安全管理員能夠為被管理的設備 (NetCrypt Family Series) 定義特定的網路和安全政策。此軟體安裝在筆記型電腦/PC 中，可提供對設備的即時安全管理，並提供強身驗證選項。

經過身分驗證的安全 Session 採用 AES 256-bit 加密和 SHA2 512-bit，以保護資料完整性。密鑰協商採用類似 SSL 的協定，使用短期的 Diffie-Hellman (2048-bit) 進行金鑰交換，並使用 RSA 簽名對 Session 密鑰協商進行身分驗證。設備可以直接從管理埠進行管理，也可以透過設備的可信任/外部介面進行遠端系統管理，在外部介面的情境下，將會通過現有的 IPsec tunnel 進行管理。

透過可信任/外部介面進行存取必須採用基於 PKI 的認證，即 PKCS12 文件 (soft token) 或 PKCS11 (加密設備)。這種設計的基本原理是為了避免重複猜測密碼，對基於密碼的帳號進行阻斷服務攻擊 (DoS)，導致帳號被鎖定，拒絕授權管理員管理登錄到設備上。被封鎖的時間取決於連續登錄失敗嘗試的次數，並以指數增加，此解決方案用於阻止密碼猜測或字典檔攻擊。

基於角色的管理員存取控制

管理工具提供：

- 基於 PKI 和密碼的身分驗證
- 根據管理員帳號授予權限
- 允許對所有部署的設備進行安全的遠端管理
- 管理所有設備功能，包括金鑰管理