用於HTTPS解密的WSA證書用法

目錄

簡介

本檔案介紹在思科網路安全裝置(WSA)上用於HTTPS解密的憑證型別。

憑證概觀

WSA能夠使用當前證書和私鑰進行HTTPS解密。但是，可能會混淆應使用的證書型別，因為並非所有x.509證書都起作用。

憑證有兩種主要型別：**伺服器證**書和**根證書**。所有x.509證書都包含Basic Constraints欄位，該欄位標識證書型別：

- **Subject Type=End Entity** -伺服器證書
- **Subject Type=CA** — 根證書

> **附註**：您必須使用根證書(也稱為證書頒發機構(CA)簽名證書)來進行WSA上的HTTPS解密。

根證書

專門建立根證書以對伺服器證書進行簽名。您可以建立和操作自己的CA並簽署自己的伺服器證書。

> **附註**：由於根憑證僅簽署其他憑證，因此不能在Web伺服器上使用它來執行HTTPS加密和解密。

WSA必須使用根證書以主動生成用於HTTPS解密的伺服器證書。根證書的使用有兩種選項：

- 在WSA上生成根證書。WSA建立自己的根證書和私鑰，它使用此金鑰對來簽署伺服器證書。

- 您可以將當前根證書及其私鑰上傳到WSA。根證書中的Common Name(CN)欄位標識信任包含其簽名的任何伺服器證書的實體（通常為公司名稱）。

  附註：伺服器證書必須由Web瀏覽器中存在公鑰的根證書簽名才能受信任。

伺服器證書

伺服器證書專門用於進行HTTPS加密和解密，以及驗證特定伺服器的真實性。伺服器證書由CA使用CA根證書進行簽名。CA的一個常見示例是VeriSign或Thawte。

> **附註**：伺服器證書不能用於簽署其他證書；因此，如果在WSA上安裝伺服器證書，則HTTPS解密不起作用。

伺服器證書中的CN欄位指定使用證書的主機。例如，**https://www.verisign.com**使用CN為**www.verisign.com**的伺服器證書。

相關資訊

- **網路安全裝置(WSA)證書使用情況（HTTPS解密、GUI登入、憑據加密）**
- **在WSA和證書簽名請求(CSR)選項上啟用HTTPS代理的步驟**
- **在(WSA)上啟用HTTPS代理的步驟和上傳根/中間證書選項**
- **技術支援與文件 - Cisco Systems**