在ESA上建立證書簽名請求

目錄

簡介

本檔案介紹如何在電子郵件安全裝置(ESA)上建立憑證簽署請求(CSR)。

在ESA上建立CSR

從AsyncOS 7.1.1開始，ESA可以建立自簽名證書供您自己使用，並生成CSR以提交至證書頒發機構並獲得公共證書。證書頒發機構返回由私鑰簽名的可信公共證書。使用GUI中的**Network > Certificates**頁面或CLI中的**certconfig**命令以建立自簽名證書、產生CSR並安裝受信任的公用證書。

如果首次獲取或建立證書，請在Internet中搜尋「證書頒發機構服務SSL伺服器證書」，並選擇最能滿足組織需要的服務。請按照服務的說明獲取證書。

GUI上的配置步驟

1. 要建立自簽名證書，請在GUI的Network > Certificates頁面上按一下**Add Certificate**(或在CLI中按一下**certconfig**命令)。 在「新增證書」頁上，選擇**建立自簽名證書**。
2. 為自簽名證書輸入以下資訊： 公用名 — 完全限定域名。組織 — 組織的確切法定名稱。組織單位 — 組織部分。城市（地區）— 組織合法所在的城市。州（省）— 組織合法所在的州、縣或地區。國家/地區 — 國際標準化組織(ISO)法定所在國家/地區的縮寫。到期前的持續時間 — 證書到期之前的天數。Private Key Size — 為CSR生成的私鑰的大小。僅支援2048位和1024位。
3. 按一下「**Next**」以檢視憑證和簽署資訊。
4. 輸入證書的名稱。預設情況下，AsyncOS分配公用名。
5. 如果要將自簽名證書的CSR提交給證書頒發機構，請按一下**Download Certificate Signing Request**，將CSR以Privacy Enhanced Mail(PEM)格式儲存到本地或網路電腦。
6. 按一下「**Submit**」以儲存憑證並提交變更內容。如果不提交更改，則私鑰將丟失，並且無法安裝簽名的證書。

當證書頒發機構返回由私鑰簽名的可信公共證書時，按一下「證書」(Certificates)頁面上的證書名稱，然後輸入本地電腦或網路上檔案的路徑以上載證書。確保您收到的受信任公共證書是PEM格式，或者是在上傳到裝置之前可以轉換為PEM的格式。OpenSSL中包含完成此操作的工具，免費軟體可從http://www.openssl.org獲得。

如果從證書頒發機構上傳證書，則會覆蓋現有證書。您還可以上傳與自簽名證書相關的中間證書。可以將證書與公共或專用偵聽程式、IP介面的HTTPS服務、輕型目錄訪問協定(LDAP)介面或到目標域的所有傳出傳輸層安全(TLS)連線一起使用。

相關資訊

- ESA上的TLS綜合設定指南
- 技術支援與文件 - Cisco Systems