思科電子郵件安全裝置(ESA)上的證書驗證演算法是什麼？

目錄

簡介

使用TLS通過思科郵件安全裝置(ESA)傳送郵件時，您可以選擇使用「驗證」或「託管驗證」選項執行證書驗證。 這是通過TLS保護電子郵件傳送安全性的一個重要部分，而且知道如何執行驗證非常重要。

思科電子郵件安全裝置(ESA)上的證書驗證演算法是什麼？

實際上有兩種演算法，一種用於「驗證」選項，另一種用於「託管驗證」選項。 通常，建議使用「託管驗證」選項，因為它與多種方案相容。

背景資訊

- 本文檔基於AsyncOS 8.0.1及更高版本。 早期版本的AsyncOS可能有一些不同的行為。
- 除非另行指定，否則支援萬用字元匹配
- 每個演算法都會在匹配成功後停止，並且不會評估後續檢查
- CLI命令**tlsverify**使用「Verify Algorithm」

定義

- CN:這是公共名稱，是證書使用者的一部分
- SAN:這是X.509的使用者替代名稱擴展。 在本檔案中使用時，我們特別指的是包含在SAN欄位中的任何DNS名稱。
- 電子郵件域：這是收件人電子郵件地址的域部分。 例如，傳送到「user@example.com」時，電子郵件域為「example.com」
- MX主機名：這些是電子郵件域的MX記錄的主機名
- PTR主機名：這是DNS PTR查詢所返回的主機名，該查詢將查詢ESA所連線的IP地址
- SMTP路由主機名：如果為此目標配置了SMTP路由，則這是SMTP路由中使用的主機名

託管驗證演算法

1. 如果證書包含SAN屬性，*將僅*使用這些屬性，且將忽略CN。 僅當證書中沒有SAN屬性時，才會使用CN。 這符合RFC 6125。
2. 已針對電子郵件域檢查證書。
3. 系統將根據可能存在的任何SMTP路由主機名檢查證書。
4. 根據MX主機名檢查證書。
5. 如果之前的所有檢查均未成功，則驗證失敗。

驗證演算法

1. 針對電子郵件域檢查了SAN屬性。
2. CN根據電子郵件域進行檢查。 **附註**：不支援萬用字元匹配。
3. 將根據PTR主機名檢查SAN屬性。
4. 如果之前的所有檢查均未成功，則驗證失敗。