為VPN裝置訪問控制配置基於DN的加密對映

目錄

簡介

本文檔介紹如何配置基於唯一判別名(DN)的加密對映以提供訪問控制，以便VPN裝置可以通過Cisco IOS®路由器建立VPN隧道。在本文檔的示例中，Rivest、Shamir和Adelman(RSA)簽名是IKE身份驗證的方法。除了標準證書驗證，基於DN的加密對映還會嘗試將對等體的ISAKMP身份與其證書中的某些欄位(如X.500可分辨名稱或完全限定域名(FQDN))匹配。

必要條件

需求

此功能最初是在Cisco IOS軟體版本12.2(4)T中匯入。您必須使用該版本或更新版本才能進行此配置。

還測試了Cisco IOS軟體版本12.3(5)。但是，由於Cisco錯誤ID CSCed45783(僅限註冊客戶)，基於DN的加密對映失敗。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科7200路由器
- Cisco IOS軟體版本12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

以前，在使用RSA簽名方法的IKE身份驗證期間，以及在證書驗證和可選證書撤銷清單(CRL)檢查之後，Cisco IOS繼續進行IKE快速模式協商。除了對加密對等體的IP地址進行限制外，它未提供防止遠端VPN裝置與任何加密介面通訊的方法。

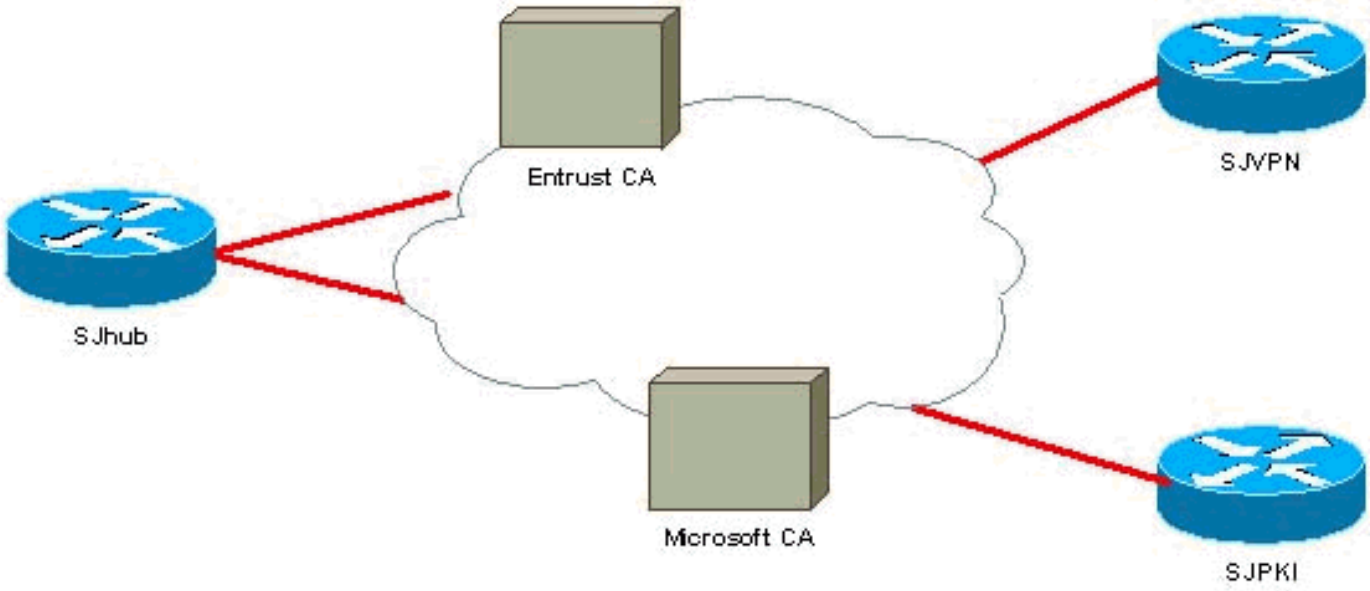
現在，使用基於DN的加密對映，Cisco IOS可以限制遠端VPN對等體僅訪問具有特定證書的選定介面。尤其是具有特定DN或FQDN的憑證。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本檔案會使用此處顯示的組態。

在本例中，使用簡單的網路設定來演示該功能。SJhub路由器有兩個身份證書，一個來自委託證書頒發機構(CA)，另一個來自Microsoft CA。請參閱相關資訊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。