瞭解EAP-PEAP的ISE有狀態TLS會話恢復

目錄

簡介

本文檔介紹思科身份服務引擎(ISE)中的傳輸層安全(TLS)會話恢復。

必要條件

需求

- 傳輸層安全(TLS)握手流程知識。
- 受保護的可擴展身份驗證協定(PEAP)流知識
- 思科身份服務引擎知識

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據

- 思科身分識別服務引擎3.2
- ISE虛擬機器(VM)
- Windows 10 PC

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

TLS會話恢復是一種用於消除初始TLS握手開銷的技術。它允許以前建立TLS會話的客戶端和伺服器恢復該會話，而無需重複資源密集型握手過程。

優勢

- 它通過避免初始握手的資源密集型步驟和所需的時間來減少延遲。
- 它還通過跳過密集的金鑰交換和證書驗證過程來減少伺服器上的計算負載。

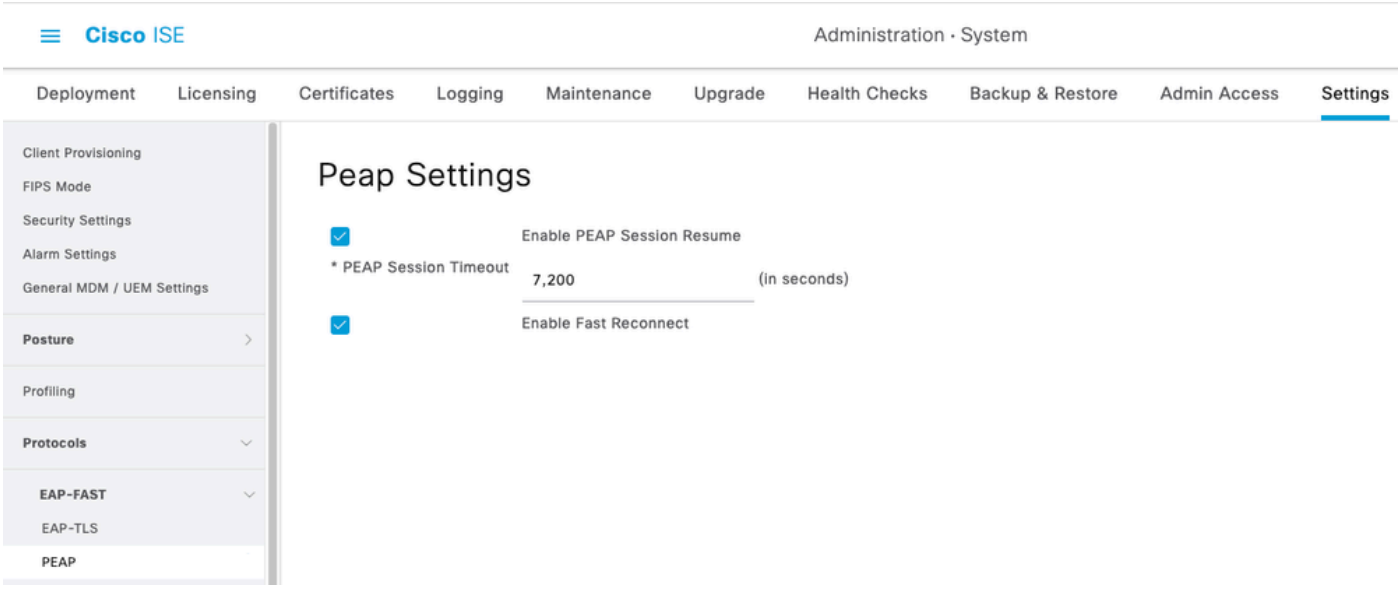
設定

在ISE上，要啟用TLS會話，請恢復PEAP:

Administration > System > Settings > Protocols > PEAP > check the Enable PEAP Session Resume

預設情況下，ISE將會話保留7200秒。

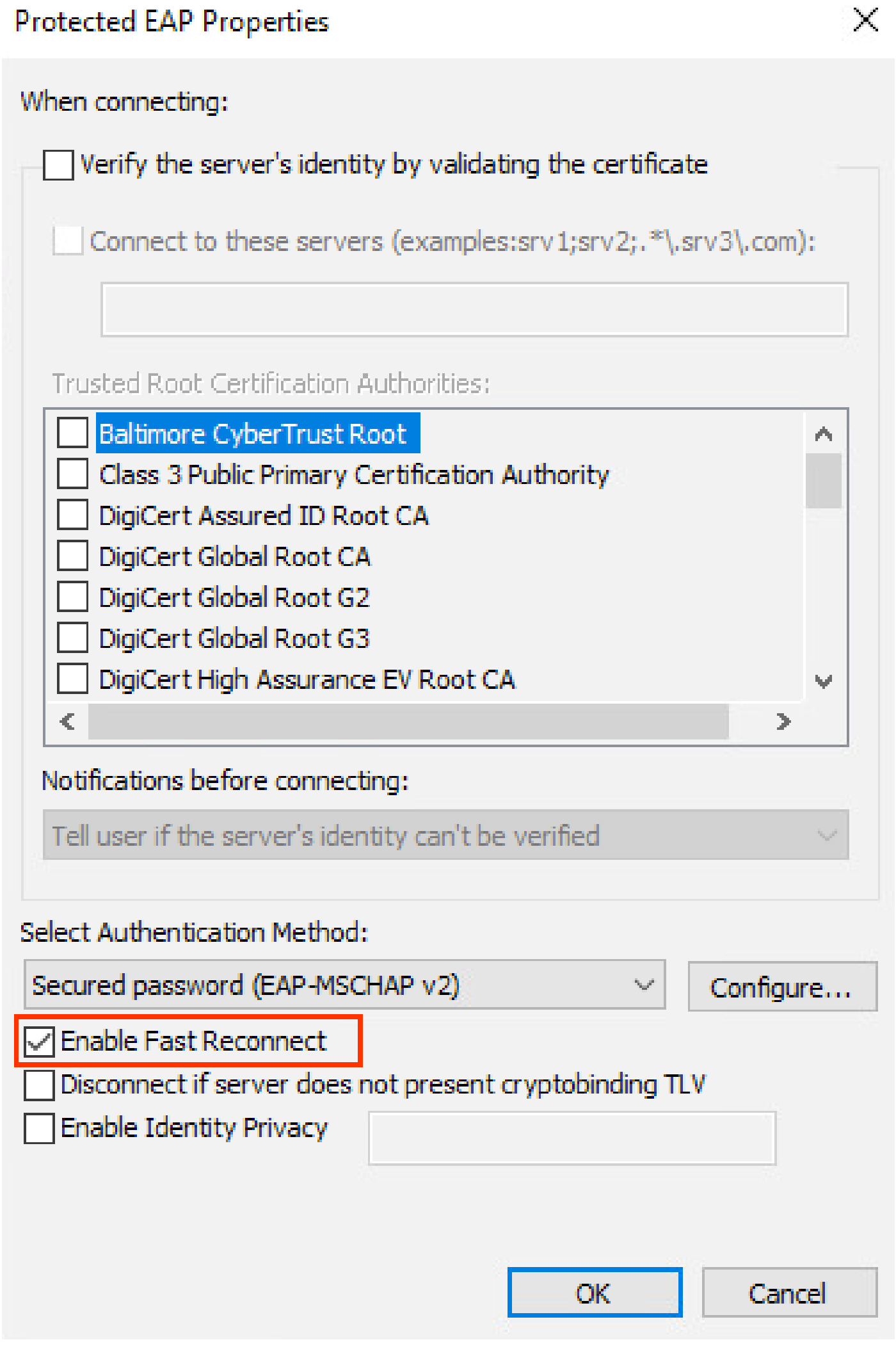
或者，您可以啟用Enable Fast Reconnect（啟用快速重新連線），這樣會繞過PEAP的內部方法，並允許更快的重新身份驗證。在諸如無線漫遊等應用中它是理想的。



ISE PEAP會話恢復配置

還必須啟用請求方中的快速重新連線。

此配置用於Windows本機請求方啟用Fast Reconnect。


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
DigiCert Global Root G3
DigiCert High Assurance EV Root CA
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

來回覆以重建相應的會話。這樣可快速建立安全連線，而且不會因重複使用先前協商的會話資料而失去安全性。

3)TLS會話ID是否複製到其他節點？

否，TLS會話ID儲存在PSN上。它不會複製到其他PSN。如果PSN重新啟動或服務重新啟動，所有會話ID都可能會從快取中丟失，並且下次必須執行完全TLS握手。

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）。