Verständnis des ISE Stateful TLS Session Resume für EAP-PEAP

Inhalt

Einleitung

In diesem Dokument wird die TLS-Sitzungswiederaufnahme (Transport Layer Security) in der Cisco Identity Services Engine (ISE) beschrieben.

Voraussetzungen

Anforderungen

- Kenntnis des TLS-Handshake-Prozesses (Transport Layer Security)
- Kenntnis des PEAP-Datenflusses (Protected Extensible Authentication Protocol)
- Kenntnisse der Cisco Identity Services Engine

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen

- Cisco Identity Services Engine 3.2
- Virtuelles System der ISE (VM)
- Windows 10-PC

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die TLS-Sitzungswiederaufnahme ist eine Technik, die verwendet wird, um den Overhead des ursprünglichen TLS-Handshakes zu eliminieren. Sie ermöglicht es einem Client und Server, die zuvor eine TLS-Sitzung eingerichtet haben, diese Sitzung fortzusetzen, ohne den ressourcenintensiven Handshake-Prozess zu wiederholen.

Vorteile

- Es reduziert die Latenz, indem es die ressourcenintensiven Schritte des ersten Handshakes und die dafür erforderliche Zeit vermeidet.
- Außerdem wird die Rechenlast auf dem Server verringert, da die aufwändigen Prozesse für den Schlüsselaustausch und die Zertifikatsvalidierung übersprungen werden.

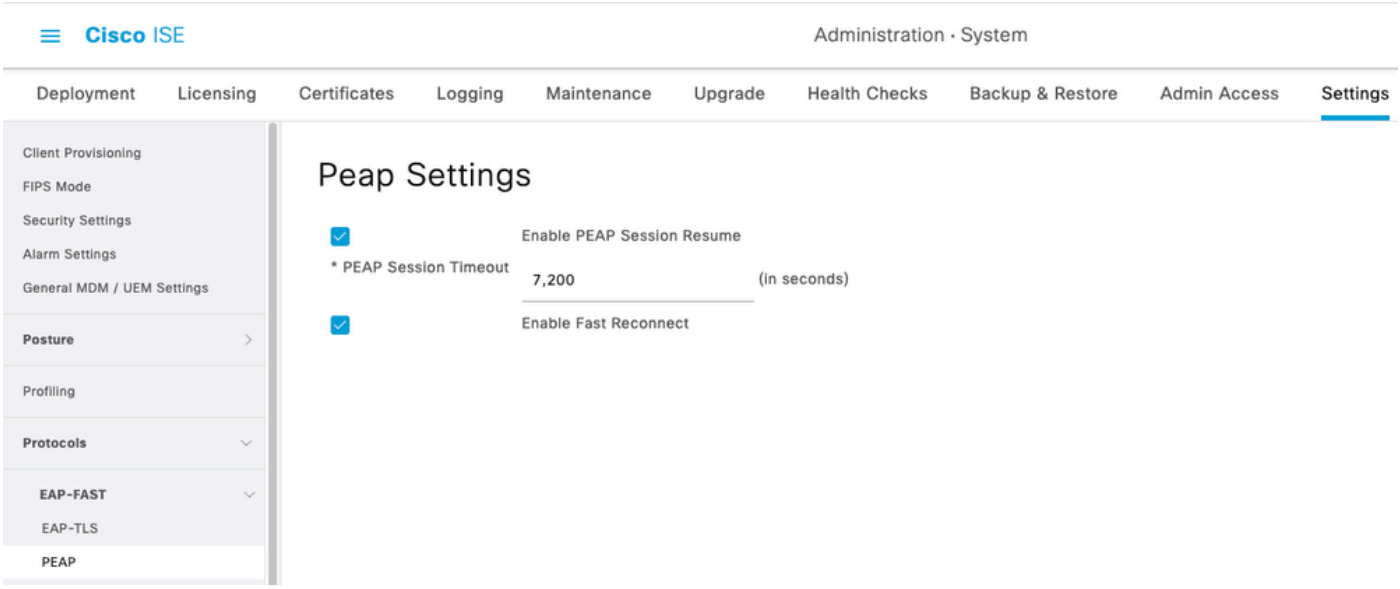
Konfigurieren

Setzen Sie die TLS-Sitzung auf der ISE für PEAP fort:

Administration > System > Einstellungen > Protokolle > PEAP > überprüfen Sie die Option PEAP-Sitzungswiederaufnahme aktivieren.

Standardmäßig wird die Sitzung von der ISE für 7.200 Sekunden gehalten.

Optional können Sie die Option Enable Fast Reconnect (Schnelle Wiederverbindung aktivieren) aktivieren, die wiederum die innere PEAP-Methode umgeht und eine noch schnellere Neuauthentifizierung ermöglicht. Dies ist bei Anwendungen wie Wireless-Roaming wünschenswert.

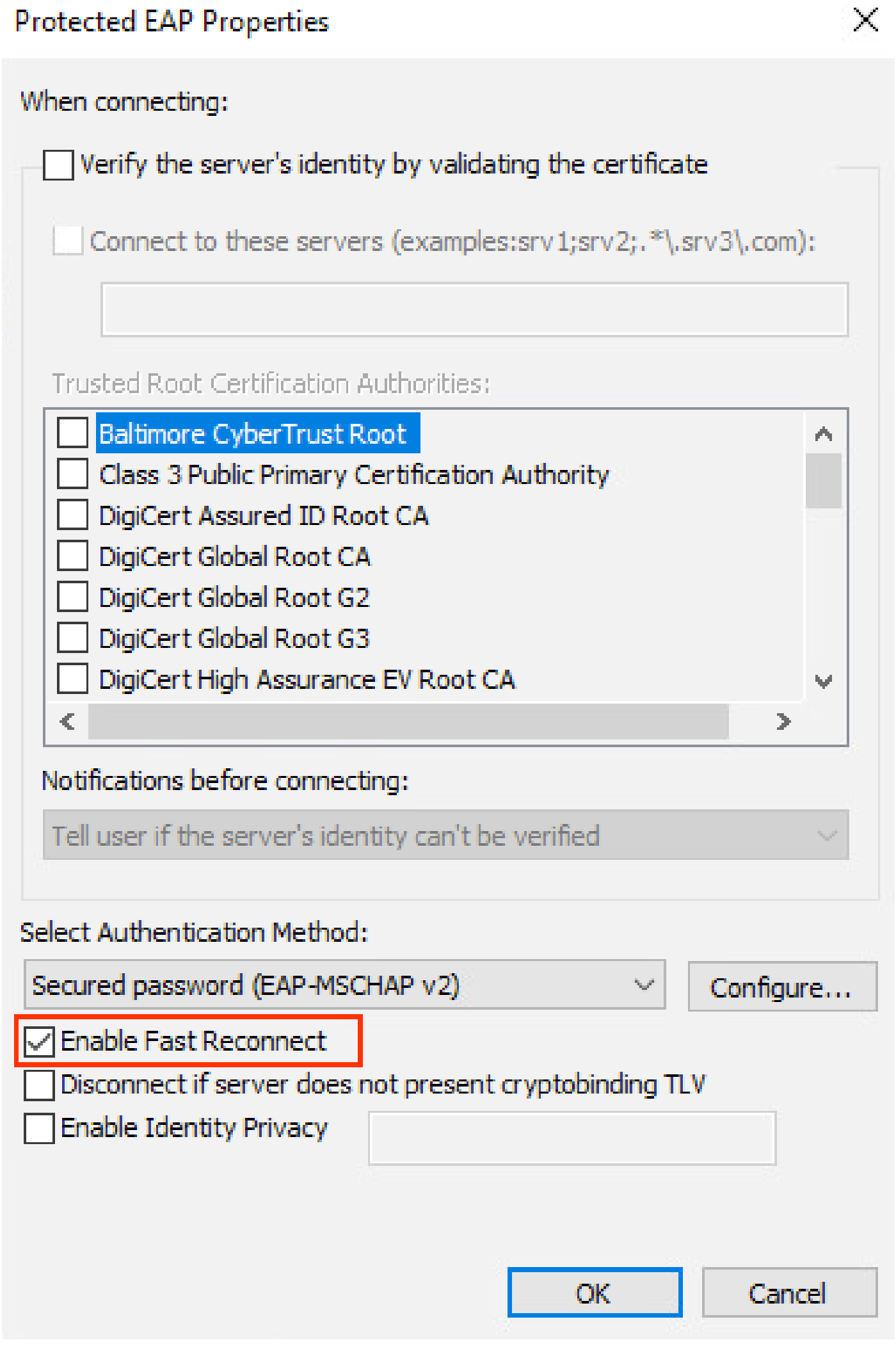


ISE PEAP-Sitzungswiederaufnahme - Konfiguration

Die Funktion für die schnelle Wiederverbindung muss ebenfalls in der Komponente aktiviert sein.

Diese Konfiguration ist für native Windows-Supplicants zur Aktivierung von Fast Reconnect

vorgesehen.


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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.