了解EAP-PEAP的ISE有状态TLS会话恢复

目录

简介

本文档介绍思科身份服务引擎(ISE)中的传输层安全(TLS)会话恢复。

先决条件

要求

- 传输层安全(TLS)握手流程知识。
- 受保护的可扩展身份验证协议(PEAP)流知识
- 思科身份服务引擎知识

使用的组件

本文档中的信息基于以下软件和硬件版本

- 思科身份服务引擎3.2
- ISE虚拟机(VM)
- Windows 10 PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

TLS会话恢复是一种用于消除初始TLS握手开销的技术。它允许以前建立TLS会话的客户端和服务器恢复该会话，而无需重复资源密集型握手过程。

优势

- 它通过避免初始握手的资源密集型步骤和所需的时间来减少延迟。
- 它还通过跳过密集的密钥交换和证书验证过程来减少服务器上的计算负载。

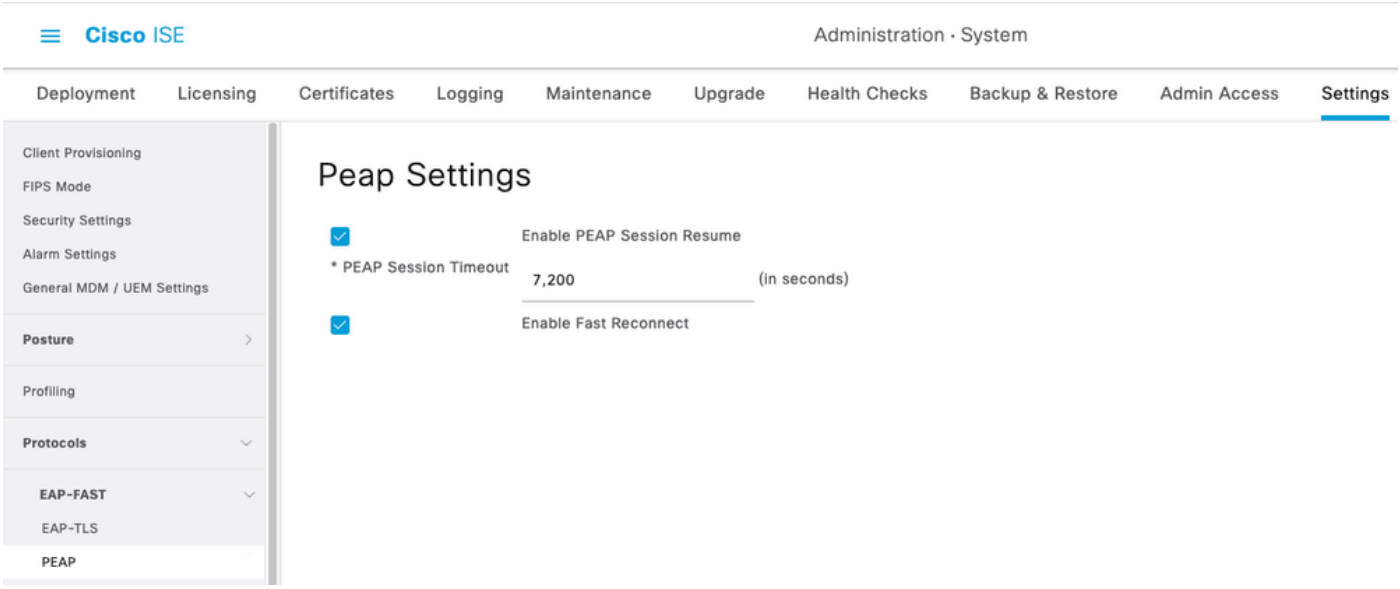
配置

在ISE上，要启用TLS会话，请恢复PEAP:

Administration > System > Settings > Protocols > PEAP >选中Enable PEAP Session Resume

默认情况下，ISE将会话保持7200秒。

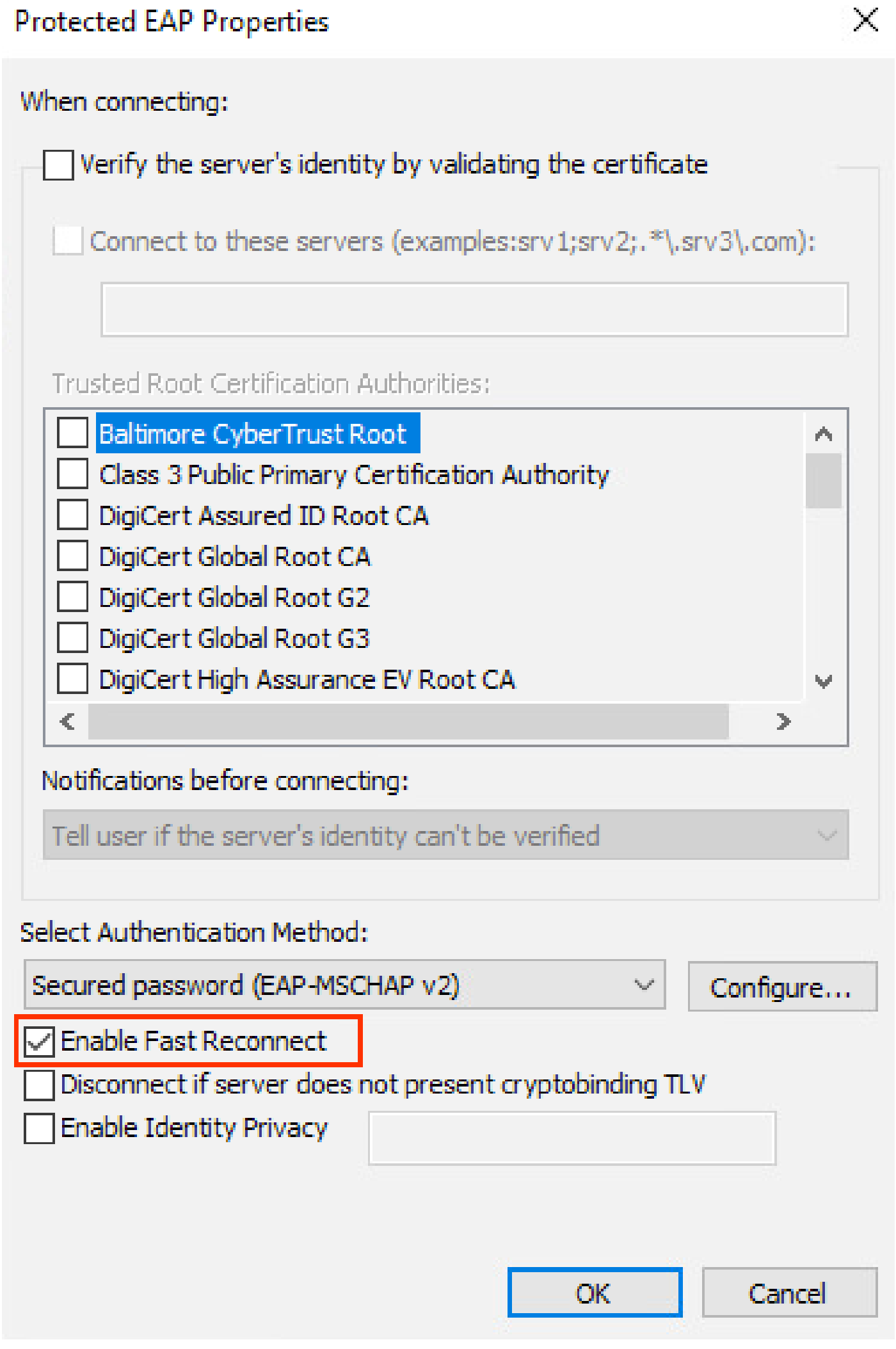
或者，您可以启用Enable Fast Reconnect，从而绕过PEAP的内部方法，并允许更快的重新身份验证。在无线漫游等应用中，这是理想选择。



ISE PEAP会话恢复配置

还必须在Supplicant客户端中启用快速重新连接。

此配置适用于Windows原生Supplicant客户端以启用快速重新连接。


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

来回复以重新建立相应的会话。这样可以快速建立安全连接，并且不会因重复使用之前协商的会话数据而丢失安全性。

3)TLS会话ID是否复制到其他节点？

否，TLS会话ID存储在PSN本身上。它不会复制到其他PSN。如果PSN重新启动或服务重新启动，所有会话ID都可能会从缓存中丢失，并且下次必须进行完全TLS握手。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。