

Begrijpen stateful TLS-sessie hervatten voor EAP-PEAP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

[Eerste verificatie](#)

[Tijdens opnieuw authenticeren](#)

[Veelgestelde vragen](#)

Inleiding

Dit document beschrijft de sessie voor Transport Layer Security (TLS) in Cisco Identity Services Engine (ISE).

Voorwaarden

Vereisten

- Kennis van TLS-handshake (Transport Layer Security).
- Kennis van Protected Extensible Verification Protocol (PEAP)-stroom
- Kennis van Cisco Identity Services Engine

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies

- Cisco Identity Services Engine 3.2
- ISE virtuele machine (VM)
- Windows 10 PC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

TLS-sessiehervatting is een techniek die wordt gebruikt om de overheadkosten van de eerste TLS-handshake te elimineren. Hiermee kunnen een client en server die eerder een TLS-sessie hebben ingesteld, die sessie hervatten zonder het resourcegerichte handshake-proces te herhalen.

Voordelen

- Het vermindert de latentie door de middel-intensieve stappen van de aanvankelijke handdruk en de tijd te vermijden die wordt vereist om dat te doen.
- Het vermindert ook de computerbelasting op de server door de intensieve sleuteluitwisseling en certificatsvalidatieprocessen over te slaan.

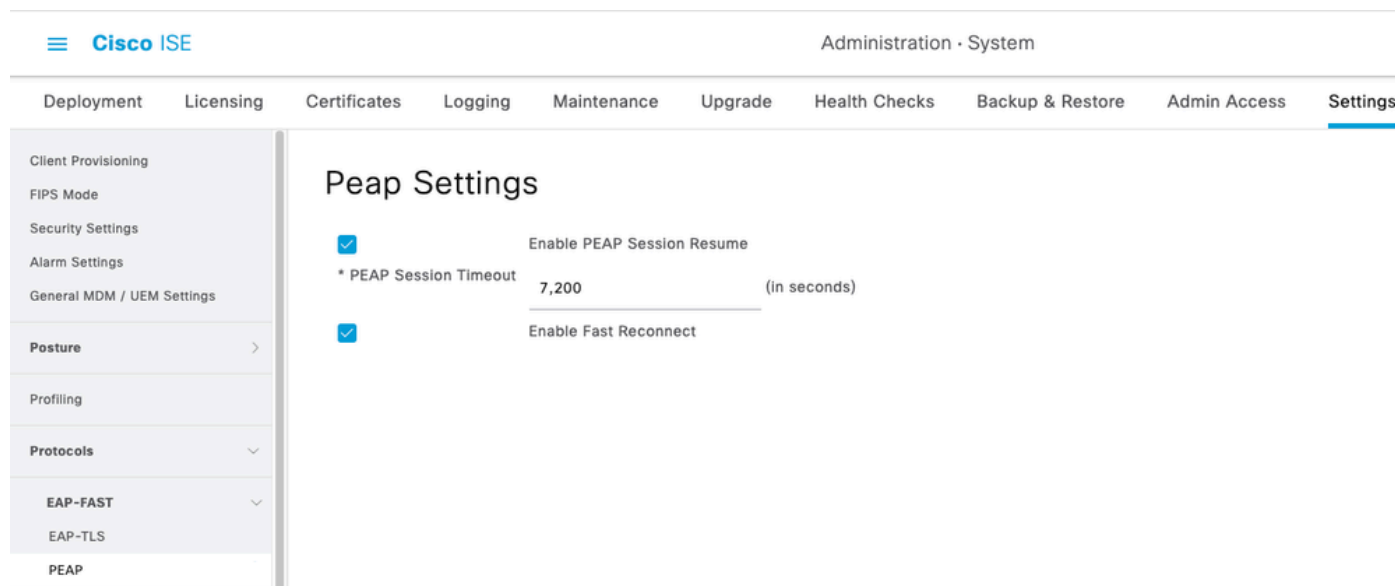
Configureren

Ga op ISE als volgt te werk om de TLS-sessie in te schakelen:

Beheer > Systeem > Instellingen > Protocollen > PEAP > controleren of PEAP-sessie inschakelen

Standaard houdt ISE de sessie 7200 seconden.

Optioneel kunt u de optie Snelle herverbinding inschakelen inschakelen, waardoor de binnenmethode van PEAP wordt omzeild en de verificatie nog sneller kan worden uitgevoerd. Het is wenselijk in toepassingen zoals draadloze roaming.



Config. van ISE-PEAP-sessie

Fast Reconconnect moet ook zijn ingeschakeld in de aanvrager.

Deze configuratie is bedoeld voor Windows-native applicatie om Fast Reconconnect in te schakelen.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.