

Informazioni sulla ripresa della sessione ISE TLS stateful per EAP-PEAP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Autenticazione iniziale](#)

[Durante la riautenticazione](#)

[Domande frequenti](#)

Introduzione

Questo documento descrive la ripresa della sessione TLS (Transport Layer Security) in Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

- Processo di handshake TLS (Transport Layer Security).
- Conoscenza del flusso PEAP (Protected Extensible Authentication Protocol)
- Conoscenza di Cisco Identity Services Engine

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware

- Cisco Identity Services Engine 3.2
- Macchina virtuale ISE
- PC Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La ripresa della sessione TLS è una tecnica utilizzata per eliminare il sovraccarico dell'handshake TLS iniziale. Consente a un client e a un server che hanno precedentemente stabilito una sessione TLS di riprendere la sessione senza ripetere il processo di handshake con uso intensivo delle risorse.

Vantaggi

- Riduce la latenza evitando i passaggi dell'handshake iniziale che richiedono un uso intensivo delle risorse e il tempo necessario per farlo.
- Riduce inoltre il carico di calcolo sul server ignorando i processi intensivi di scambio di chiavi e convalida dei certificati.

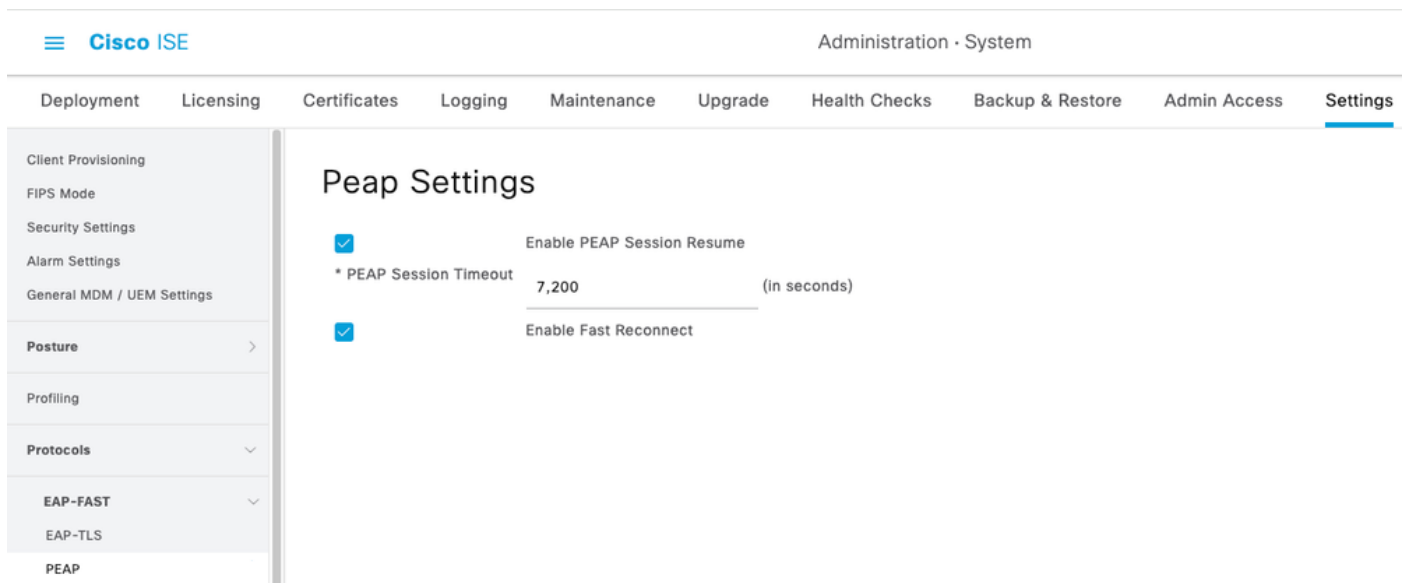
Configurazione

Su ISE, per abilitare la sessione TLS, riprendere per PEAP:

Amministrazione > Sistema > Impostazioni > Protocolli > PEAP > selezionare Abilita ripresa sessione PEAP

Per impostazione predefinita, ISE tiene la sessione per 7200 secondi.

Facoltativamente, è possibile abilitare l'opzione Abilita riconnessione rapida, che a sua volta ignora il metodo interno di PEAP e consente una riautenticazione ancora più veloce. È consigliabile in applicazioni quali il roaming wireless.



ISE PEAP Session Resume Config

La riconnessione rapida deve essere abilitata anche nel supplicant.

Questa configurazione consente al supplicant nativo di Windows di abilitare la riconnessione rapida.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).