

Chaînage EAP avec TEAP

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configuration de Cisco ISE](#)

[Configuration du demandeur natif Windows](#)

[Vérifier](#)

[Rapport d'authentification détaillé](#)

[Authentification machine](#)

[Authentification des utilisateurs et des machines](#)

[Dépannage](#)

[Analyse du journal en direct](#)

[Authentification machine](#)

[Authentification des utilisateurs et des machines](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer ISE et le demandeur Windows pour le chaînage EAP (Extensible Authentication Protocol) avec le protocole TEAP (Extensible Authentication Protocol) basé sur un tunnel.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- Configuration du demandeur Windows

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.0
- Windows 10 version 2004
- Connaissance du protocole TEAP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

TEAP est une méthode de protocole d'authentification extensible basée sur un tunnel qui établit un tunnel sécurisé et exécute d'autres méthodes EAP sous la protection de ce tunnel sécurisé.

L'authentification TEAP se produit en deux phases après l'échange initial de requête/réponse d'identité EAP.

Dans la première phase, le protocole TEAP utilise la connexion TLS pour fournir un échange de clés authentifié et pour établir un tunnel protégé. Une fois le tunnel établi, la deuxième phase commence avec l'homologue et le serveur engage une conversation supplémentaire pour établir les politiques d'authentification et d'autorisation requises.

Cisco ISE 2.7 et versions ultérieures prennent en charge le protocole TEAP. Les objets TLV (type-length-value) sont utilisés dans le tunnel pour transporter des données liées à l'authentification entre l'homologue EAP et le serveur EAP.

Microsoft a introduit la prise en charge de TEAP dans la version Windows 10 2004 publiée en MAI 2020.

Le chaînage EAP permet l'authentification de l'utilisateur et de la machine dans une session EAP/Radius au lieu de deux sessions distinctes.

Auparavant, pour ce faire, vous aviez besoin du module NAM Cisco AnyConnect et utilisiez EAP-FAST sur le demandeur Windows, car le demandeur Windows natif ne le prenait pas en charge. Vous pouvez désormais utiliser le demandeur natif Windows pour effectuer le chaînage EAP avec ISE 2.7 à l'aide de TEAP.

Configurer

Configuration de Cisco ISE

Étape 1. Vous devez modifier les protocoles autorisés pour activer le chaînage TEAP et EAP.

Naviguez jusqu'à **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Cochez les cases de chaînage TEAP et EAP.

Dictionaryes
Conditions
Results

- Allow MS-CHAPV2
- Allow EAP-MD5
- Allow EAP-MS-CHAPv2
- Allow Password Change Retries 1 (Valid Range 0 to 3)
- Allow TEAP**
- TEAP Inner Methods
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries 3 (Valid Range 0 to 3) ⓘ
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ
 - Allow downgrade to MSK ⓘ
 - Accept client certificate during tunnel establishment ⓘ
 - Enable EAP Chaining** ⓘ
- Preferred EAP Protocol LEAP ⓘ
- EAP-TLS L-bit ⓘ
- Allow weak ciphers for EAP ⓘ
- Require Message-Authenticator for all RADIUS Requests ⓘ

Étape 2. Créez un profil de certificat et ajoutez-le à la séquence source d'identité.

Naviguez jusqu'à ISE > Administration > Identities > identity Source Sequence et sélectionnez le profil de certificat.

Identities
Groups
External Identity Sources
Identity Source Sequences
Settings

Identity Source Sequence

- * Name
- Description

Certificate Based Authentication

- Select Certificate Authentication Profile**

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
Guest Users	ADJooint

Étape 3. Vous devez appeler cette séquence dans la stratégie d'authentification.

Naviguez jusqu'à ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy et choisissez la séquence source Identity créée à l'étape 2.

Status	Rule Name	Conditions	Use	Hits
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	For_Teap > Options	0

Étape 4. Vous devez maintenant modifier la stratégie d'autorisation sous l'ensemble de stratégies Dot1x.

Naviguez jusqu'à ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .

Vous devez créer deux règles. La première règle vérifie que la machine est authentifiée, mais pas l'utilisateur. La deuxième règle vérifie que l'utilisateur et la machine sont authentifiés.

Status	Rule Name	Conditions	Profiles	Results
✓	User authentication	Network Access:EapChainingResult EQUALS User and machine both succeeded	PermitAccess	
✓	Machine authentication	Network Access:EapChainingResult EQUALS User failed and machine succeeded	PermitAccess	

La configuration est ainsi terminée du côté du serveur ISE.

Configuration du demandeur natif Windows

Configurez le paramètre d'authentification câblée dans ce document.

Naviguez jusqu'à Control Panel > Network and Sharing Center > Change Adapter Settings et cliquez avec le bouton droit sur LAN Connection > Properties. Cliquez sur le bouton Authentication s'affiche.

Étape 1. Cliquez sur Authentication et choisissez Microsoft EAP-TEAP.

Networking

Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: EAP-TEAP

Settings

Remember my credentials for this connection each time I'm logged on

Fall-back to unauthorised network access

Additional Settings...

OK

Cancel

Étape 2. Cliquez sur le bouton `Settings` en regard de TEAP.

1. Conserver `Enable Identity Privacy` activé avec `anonymous` en tant qu'identité.
2. Cochez la case en regard du ou des serveurs CA racine sous `Autorités de certification racine de confiance` qui sont utilisées pour signer le certificat pour l'authentification EAP sur le PSN ISE.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.