

EAP-Verkettung mit TEAP

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfiguration der Cisco ISE](#)

[Konfiguration der nativen Windows-Komponente](#)

[Überprüfung](#)

[Detaillierter Authentifizierungsbericht](#)

[Authentifizierung des Systems](#)

[Benutzer- und Geräteauthentifizierung](#)

[Fehlerbehebung](#)

[Live-Protokollanalyse](#)

[Authentifizierung des Systems](#)

[Benutzer- und Geräteauthentifizierung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie ISE und Windows-Supplikat für die EAP-Verkettung (Extensible Authentication Protocol) mit dem tunnelbasierten TEAP (Extensible Authentication Protocol) konfiguriert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE
- Konfiguration von Windows Supplikat

Verwendete Komponenten

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

- Cisco ISE Version 3.0
- Windows 10, Build 2004
- Kenntnisse des Protokolls TEAP

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 verstehen.

Hintergrundinformationen

TEAP ist ein tunnelbasiertes Extensible Authentication Protocol-Verfahren, das einen sicheren Tunnel erstellt und andere EAP-Verfahren unter dem Schutz dieses geschützten Tunnels ausführt.

Die TEAP-Authentifizierung erfolgt in zwei Phasen nach dem anfänglichen EAP-Identitätsanforderungs-/Antwortaustausch.

In der ersten Phase verwendet TEAP den TLS-Handshake, um einen authentifizierten Schlüsselaustausch bereitzustellen und einen geschützten Tunnel einzurichten. Sobald der Tunnel eingerichtet ist, beginnt die zweite Phase mit dem Peer, und der Server führt eine weitere Konversation durch, um die erforderlichen Authentifizierungs- und Autorisierungsrichtlinien festzulegen.

Cisco ISE 2.7 und höher unterstützt das TEAP-Protokoll. Die TLV-Objekte (Type-Length-Value) werden im Tunnel verwendet, um authentifizierungsbezogene Daten zwischen dem EAP-Peer und dem EAP-Server zu übertragen.

Microsoft hat die Unterstützung für TEAP in der Version Windows 10 2004 eingeführt, die im Mai 2020 veröffentlicht wurde.

Die EAP-Verkettung ermöglicht die Benutzer- und Geräteauthentifizierung innerhalb einer EAP/Radius-Sitzung anstelle von zwei separaten Sitzungen.

Bisher war hierzu das Cisco AnyConnect NAM-Modul erforderlich, und EAP-FAST wurde auf der Windows-Komponente verwendet, da diese von der nativen Windows-Komponente nicht unterstützt wird. Jetzt können Sie die Windows Native Suppllicant verwenden, um die EAP-Verkettung mit ISE 2.7 mithilfe von TEAP durchzuführen.

Konfigurieren

Konfiguration der Cisco ISE

Schritt 1: Sie müssen die zulässigen Protokolle bearbeiten, um die TEAP- und EAP-Verkettung zu aktivieren.

Navigieren Sie zu **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** . Aktivieren Sie die Kontrollkästchen TEAP- und EAP-Verkettung.

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 ⓘ

Schritt 2: Erstellen Sie ein Zertifikatprofil, und fügen Sie es der Identitätsquellensequenz hinzu.

Navigieren Sie zu ISE > Administration > Identities > identity Source Sequence und wählen Sie das Zertifikatprofil aus.

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

Schritt 3: Sie müssen diese Sequenz in der Authentifizierungsrichtlinie aufrufen.

Navigieren Sie zu ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy und wählen Sie die in Schritt 2 erstellte Identitätsquellensequenz aus.

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

Schritt 4: Nun müssen Sie die Autorisierungsrichtlinie unter dem Punkt1x-Richtliniensatz ändern.

Navigieren Sie zu ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .

Sie müssen zwei Regeln erstellen. Die erste Regel überprüft, ob der Computer authentifiziert ist, der Benutzer jedoch nicht. Mit der zweiten Regel wird überprüft, ob Benutzer und Computer authentifiziert sind.

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	

Damit ist die ISE-Serverkonfiguration abgeschlossen.

Konfiguration der nativen Windows-Komponente

Konfigurieren Sie die Einstellungen für die kabelgebundene Authentifizierung in diesem Dokument.

Navigieren Sie zu Control Panel > Network and Sharing Center > Change Adapter Settings und mit der rechten Maustaste auf LAN Connection > Properties. Klicken Sie auf Authentication aus.

Schritt 1: Klicken Sie Authentication Dropdown-Liste und wählen 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

Schritt 2: Klicken Sie auf settings -Taste neben TEAP.

1. Beibehalten `Enable Identity Privacy` **aktiviert** mit `anonymous` als Identität.
2. Setzen Sie ein Häkchen neben den Stammzertifizierungsstellenservern unter `Vertrauenswürdige Stammzertifizierungsstellen`, die verwendet werden, um das Zertifikat für die EAP-Authentifizierung auf dem ISE PSN zu signieren.

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.