

Configuration du VPN d'accès distant FTD avec MSCHAPv2 sur RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration du VPN RA avec authentification AAA/RADIUS via FMC](#)

[Configurer ISE pour prendre en charge MS-CHAPv2 en tant que protocole d'authentification](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment activer Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) en tant que méthode d'authentification via Firepower Management Center (FMC) pour les clients VPN d'accès distant avec authentification RADIUS (Remote Authentication Dial-In User Service).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Identity Services Engine (ISE)
- Client de mobilité sécurisée Cisco AnyConnect
- protocole RADIUS

Components Used

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

- FMCv - 7.0.0 (build 94)
- FTDv - 7.0.0 (build 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.02086
- Windows 10 Pro

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

Par défaut, FTD utilise le protocole PAP (Password Authentication Protocol) comme méthode d'authentification avec les serveurs RADIUS pour les connexions VPN AnyConnect.

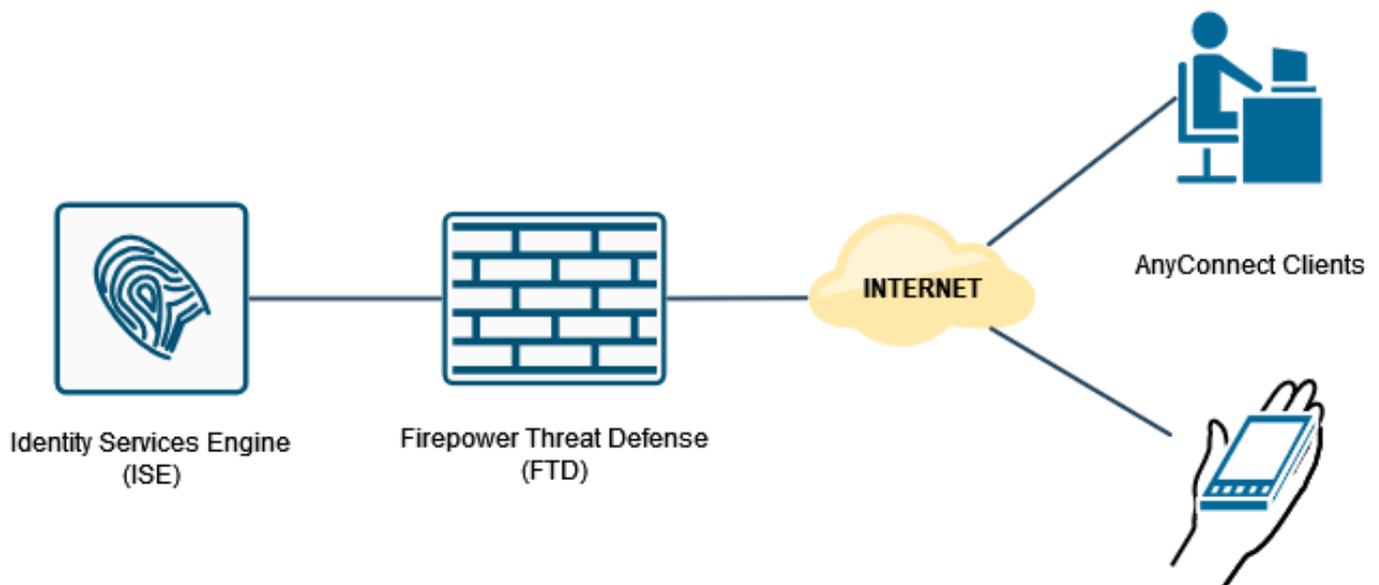
Le protocole PAP fournit une méthode simple permettant aux utilisateurs d'établir leur identité à l'aide d'un échange en deux étapes. Le mot de passe PAP est chiffré avec un secret partagé et est le protocole d'authentification le moins sophistiqué. Le protocole PAP n'est pas une méthode d'authentification puissante car il offre peu de protection contre les attaques répétées par essais et erreurs.

L'authentification MS-CHAPv2 introduit l'authentification mutuelle entre homologues et une fonction de modification du mot de passe.

Afin d'activer MS-CHAPv2 comme protocole utilisé entre l'ASA et le serveur RADIUS pour une connexion VPN, la gestion des mots de passe doit être activée dans le profil de connexion. L'activation de la gestion des mots de passe génère une demande d'authentification MS-CHAPv2 du FTD au serveur RADIUS.

Configuration

Diagramme du réseau

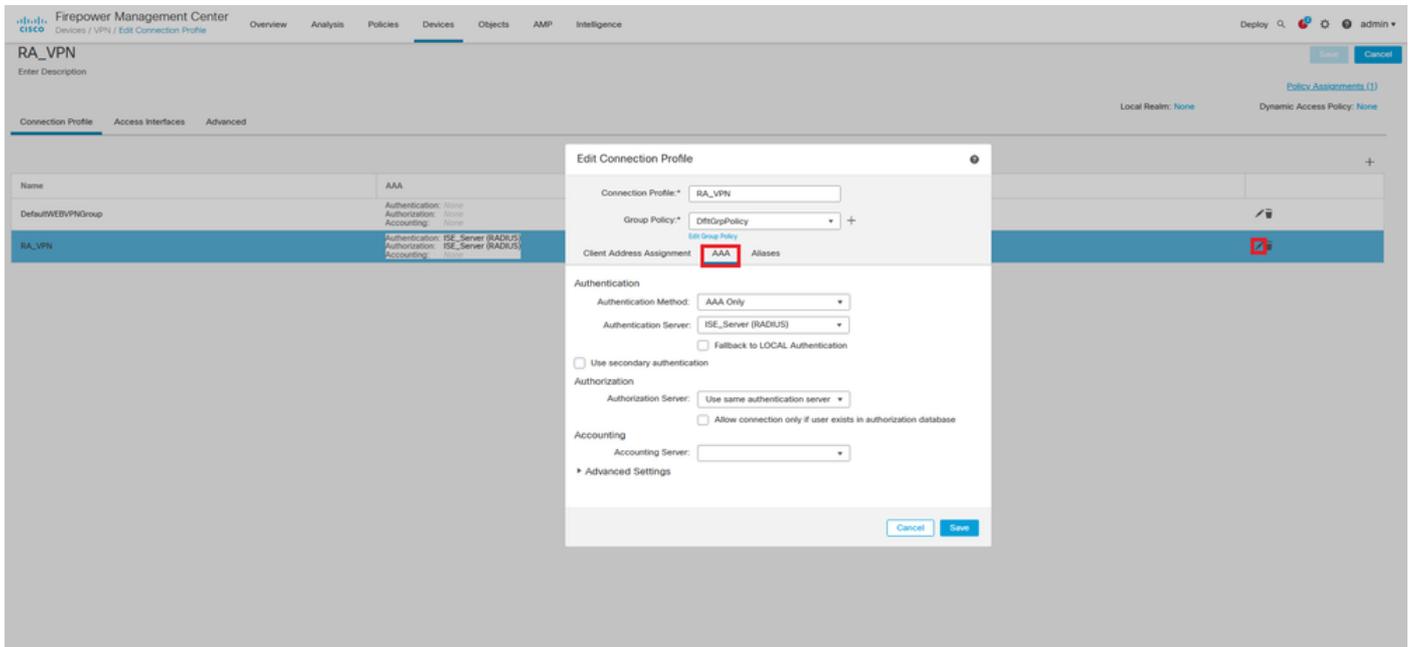


Configuration du VPN RA avec authentification AAA/RADIUS via FMC

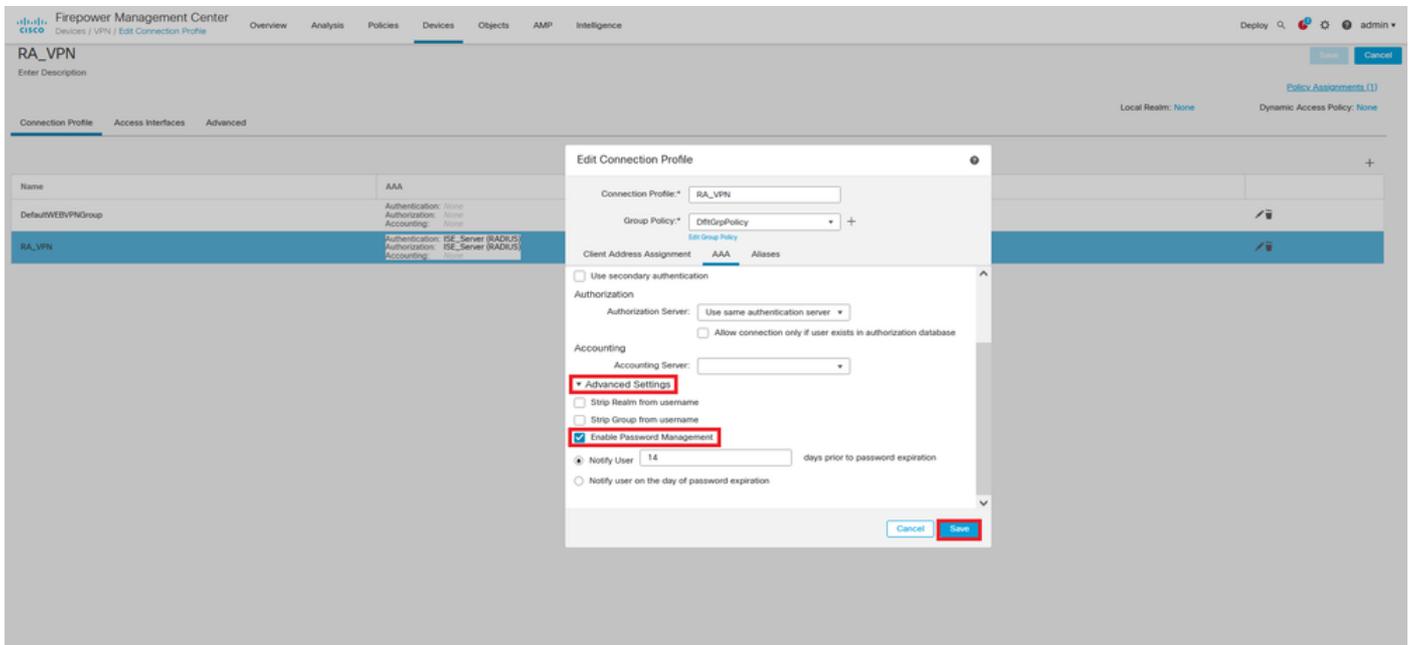
Pour une procédure pas à pas, reportez-vous à ce document et à cette vidéo :

- [Configuration VPN d'accès à distance AnyConnect sur FTD](#)
- [Configuration AnyConnect initiale pour FTD géré par FMC](#)

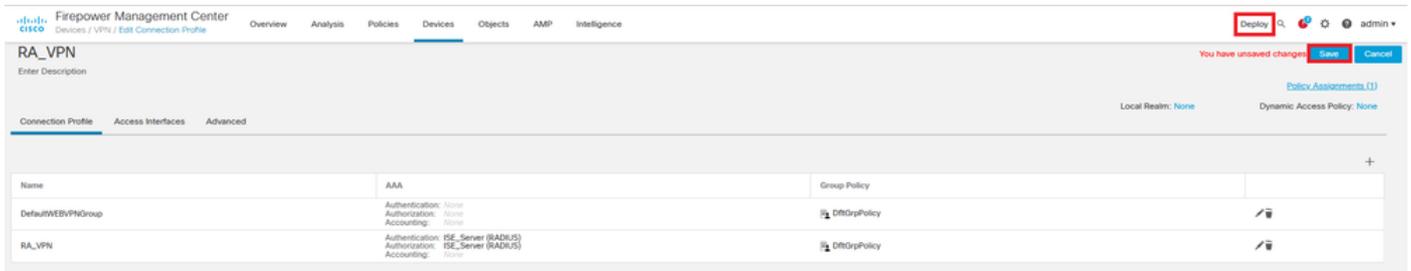
Étape 1. Une fois le VPN d'accès à distance configuré, accédez à **Périphériques > Accès à distance**, modifiez le profil de connexion nouvellement créé, puis accédez à l'onglet **AAA**.



Développez la section **Paramètres avancés** et activez la case à cocher **Activer la gestion des mots de passe**. Click **Save**.



Enregistrer et déployer.



La configuration VPN d'accès à distance sur l'interface de ligne de commande FTD est la suivante :

```
ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0
```

```
interface GigabitEthernet0/0
nameif Outside_Int
security-level 0
ip address 192.168.0.100 255.255.255.0
```

```
aaa-server ISE_Server protocol radius
aaa-server ISE_Server host 172.16.0.8
key *****
authentication-port 1812
accounting-port 1813
```

```
crypto ca trustpoint RAVPN_Self-Signed_Cert
enrollment self
fqdn none
subject-name CN=192.168.0.100
keypair <Default-RSA-Key>
crl configure
```

```
ssl trust-point RAVPN_Self-Signed_Cert
```

```
webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
no disable
error-recovery disable
```

```
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev2 ssl-client
user-authentication-idle-timeout none
webvpn
anyconnect keep-installer none
anyconnect modules value none
anyconnect ask none default anyconnect
```

```
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none
```

```
tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
```

password-management

```
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

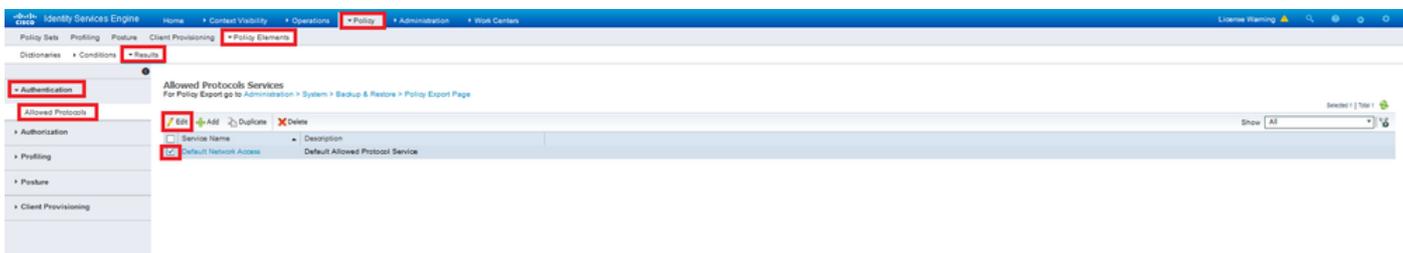
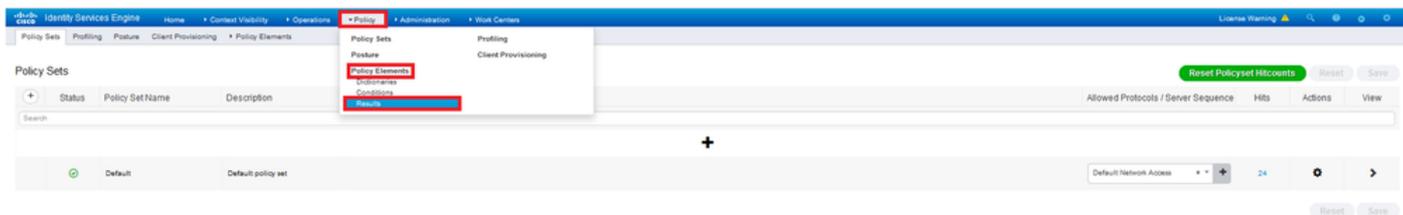
Configurer ISE pour prendre en charge MS-CHAPv2 en tant que protocole d'authentification

On suppose que :

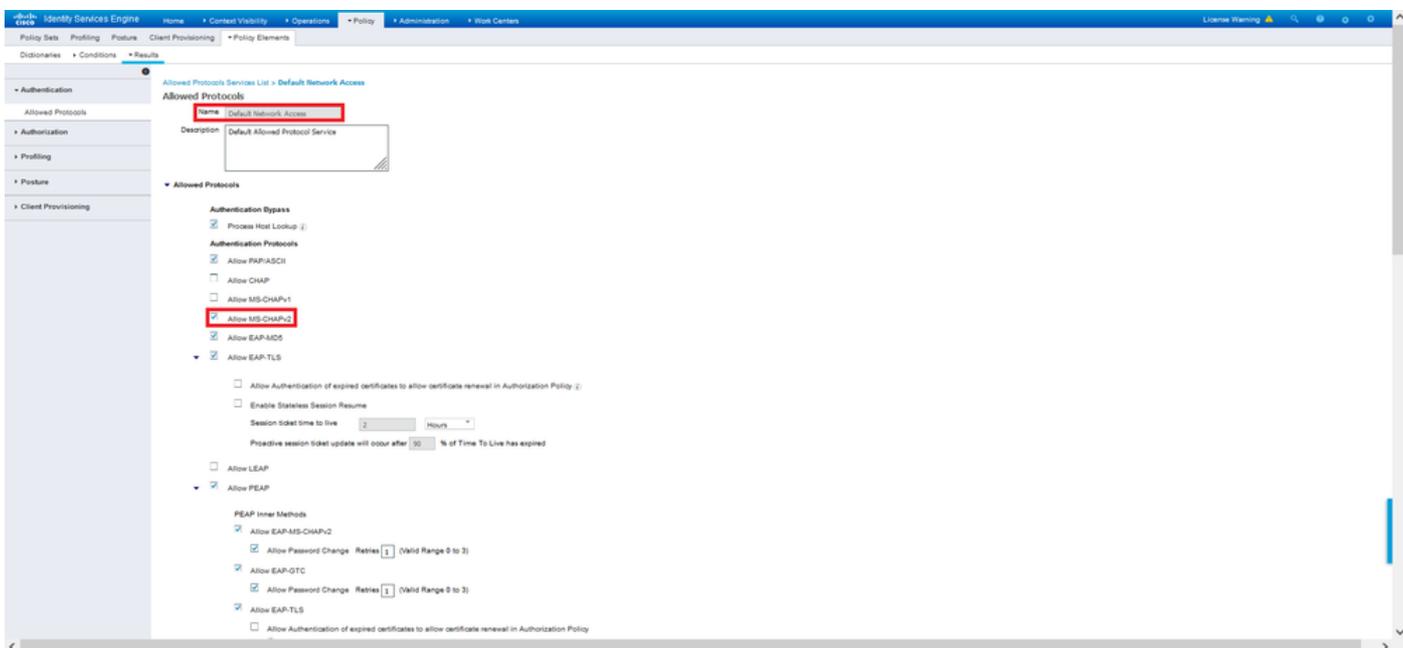
1. Le FTD est déjà ajouté en tant que périphérique réseau sur ISE afin de pouvoir traiter les demandes d'accès RADIUS à partir du FTD.
2. Au moins un utilisateur est disponible pour ISE pour authentifier le client AnyConnect.

Étape 2. Accédez à **Policy > Policy Sets** et recherchez la stratégie **Allowed Protocols** associée au Policy Set où vos utilisateurs AnyConnect sont authentifiés. Dans cet exemple, un seul ensemble de stratégies est présent, de sorte que la stratégie en question est *Accès réseau par défaut*.

Étape 3. Accédez à **Stratégie > Eléments de stratégie > Résultats**. Sous **Authentication > Allowed Protocols**, sélectionnez et modifiez **Default Network Access**.

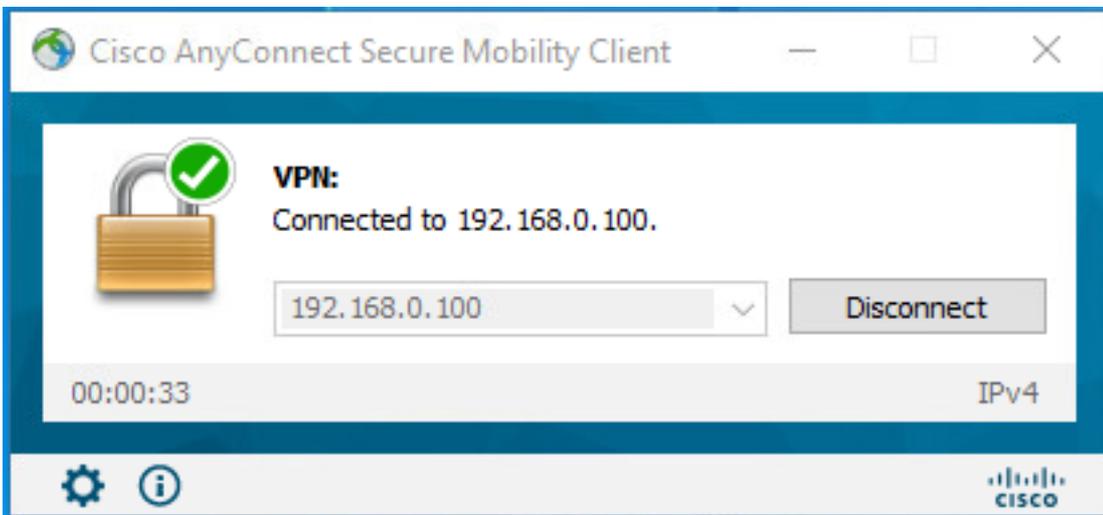


Assurez-vous que la case **Allow MS-CHAPv2** est cochée. Faites défiler jusqu'en bas et enregistrez-le.



Vérification

Accédez à la machine cliente sur laquelle le client Cisco AnyConnect Secure Mobility est installé. Connectez-vous à la tête de réseau FTD (un ordinateur Windows est utilisé dans cet exemple) et saisissez les informations d'identification de l'utilisateur.



Les journaux en direct RADIUS sur ISE montrent :

Identity Services Engine

Overview

| | |
|-----------------------|-------------------------------------|
| Event | 5200 Authentication succeeded |
| Username | user1 |
| Endpoint Id | 00:50:56:96:45:6F:0 |
| Endpoint Profile | Windows10-Workstation |
| Authentication Policy | Default >> Default |
| Authorization Policy | Default >> Static IP Address User 1 |
| Authorization Result | StaticIPAddressUser1 |

Authentication Details

| | |
|-------------------------------|-------------------------------|
| Source Timestamp | 2021-09-28 00:06:02.94 |
| Received Timestamp | 2021-09-28 00:06:02.94 |
| Policy Server | driverap-ISE-0-7 |
| Event | 5200 Authentication succeeded |
| Username | user1 |
| User Type | User |
| Endpoint Id | 00:50:56:96:45:6F:0 |
| Calling Station Id | 192.168.0.101 |
| Endpoint Profile | Windows10-Workstation |
| Authentication Identity Store | Internal Users |
| Identity Group | Workstation |
| Audit Session Id | c9a30054000a50061525049 |
| Authentication Method | MSCHAPV2 |
| Authentication Protocol | MSCHAPV2 |
| Network Device | DRIVERAP_FT12_7-0 |
| Device Type | All Device Types |
| Location | All Locations |
| NAS IPv4 Address | 0.0.0.0 |

Steps

```

11001 Received RADIUS AccessRequest
11017 RADIUS created a new session
15049 Evaluating Policy Group
15001 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15043 Queried PIP - Normalised Radius RadiusIofwType (4 times)
22072 Selected identity source sequence - All_User_ID_Stores
10010 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - user1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
24719 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15030 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user1
24211 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - Radius User-Name
15010 Selected Authorization Profile - StaticIPAddressUser1
22081 Max sessions policy passed
22080 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

```

Identity Services Engine

| | |
|-----------------------|----------------------|
| NAS Port Type | Virtual |
| Authorization Profile | StaticIPAddressUser1 |
| Response Time | 231 milliseconds |

Other Attributes

| | |
|--------------------------------------|--|
| ConfigVersionId | 147 |
| DestinationPort | 1812 |
| Protocol | Radius |
| NAS-Port | 57344 |
| Tunnel-Client-Endpoint | (tag=0) 192.168.0.101 |
| MS-CHAP-Challenge | 0F 4F 54 0E 45 0F 4F 55 AC 50 57 1C 57 56 A8 08 |
| MS-CHAP2-Response | 00 00 05 06 A0 20 A4 45 0 12 FF 6A 20 6C A1 19 45 A9 00 00 00 00 00 00 00 05 41 29 52 30 5A 20 A1 09 A7 50 3C 0E 8A 73 32 A9 50 54 27 5C 54 99 |
| CVPR3000ASAPOD7x-Tunnel-Group-Name | RA_VPN |
| NetworkDeviceProfileId | 9009905-3150-4215-a80e-6753645a056c |
| IsThirdPartyDeviceFlow | false |
| CVPR3000ASAPOD7x-Client-Type | 2 |
| Acx-Session-Id | driverap-ISE-0-71417494978-25 |
| SelectedAuthenticationIdentityStores | Internal Users |
| SelectedAuthenticationIdentityStores | All_AD_join_Points |
| SelectedAuthenticationIdentityStores | Guest Users |
| Authentication Status | AuthenticationPassed |
| IdentityPolicyMatchedRule | Default |
| AuthorizationPolicyMatchedRule | Static IP Address User 1 |
| ISE Policy Set Name | Default |
| Identity Selection Matched Rule | Default |
| DTLS Support | Unknown |
| Host Identity Group | Endpoint Identity Groups Profiled Workstation |
| Network Device Profile | Cisco |

| | |
|-------------------|--|
| Location | Location#All Locations |
| Device Type | Device Type#All Device Types |
| IPSEC | IPSEC#All IPSEC Device#No |
| EnableFlag | Enabled |
| RADIUS Username | user1 |
| Device IP Address | 192.168.0.100 |
| CPMSessionID | ida80064000a0001525a9 |
| Called Station ID | 192.168.0.100 |
| CiscoAVPair | mgn-du#device:platformmin mgn-du#device:macr-00-50-50-45-01 mgn-du#device:platform:version10.0.18202 mgn-du#device:publicmacr-00-50-50-45-01 mgn-du#device:agent#anyConnect:Windows 4.10.2208 mgn-du#device:type#VMware, Inc. VMware Virtual Platform mgn-du#device:uid gidbn158f885ccf52f3f2c0e2431455f4baa2ae2c0b3 mgn-du#device user#058437071f98782f816f124621184408986c717e37d188cc00f 84A3CB82344 a:0:session-cpm#ida80064000a0001525a9 ip source-ip#192.168.0.101 008-push#ave |

| | |
|-------------------|--|
| Result | |
| Framed IP Address | 10.0.50.101 |
| Class | CACS ida80064000a0001525a9 avirap-ISE-2.741749497825 |
| cisco-av-pair | profile-name#Windows10-Rotation |
| MS-CHAP2-Success | 00 53 30 33 30 33 40 33 30 37 30 34 42 43 40 32 33 40 41 31 39 37 37 32 44 45 39 30 39 44 41 35 37 31 36 44 35 41 43 45 43 41 |
| LicenseType | Base license consumed |

| | |
|-----------------------|--|
| Session Events | |
|-----------------------|--|

Remarque : la commande **test aaa-server authentication** utilise toujours PAP pour envoyer des requêtes d'authentification au serveur RADIUS, il n'y a aucun moyen de forcer le pare-feu à utiliser MS-CHAPv2 avec cette commande.

firepower# test aaa-server authentication ISE_Server host 172.16.0.8 username user1 password XXXXXX

INFORMATIONS : Tentative de test d'authentification sur l'adresse IP (172.16.0.8) (délai d'attente : 12 secondes)

INFORMATIONS : Authentification réussie

Note: Ne modifiez pas les attributs **ppp-group tunnel** via Flex-config, car cela n'a aucun effet sur les protocoles d'authentification négociés sur RADIUS pour les connexions VPN AnyConnect (SSL et IPsec).

tunnel-group RA_VPN ppp-attribute

- no authentication pap
- authentication chap
- authentication ms-chap-v1
- no authentication ms-chap-v2
- no authentication eap-proxy

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Sur FTD :

- **debug radius all**

Sur ISE :

- Journaux en direct RADIUS