

# Configurer le mappage d'attributs RADIUS pour les utilisateurs distants FlexVPN

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du routeur](#)

[Configuration d'Identity Services Engine \(ISE\)](#)

[Configuration du client](#)

[Vérifier](#)

[Dépannage](#)

[Débogages et journaux](#)

[Scénario de travail](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment configurer FlexVPN à l'aide de Cisco Identity Services Engine (ISE) pour vérifier les identités et effectuer le mappage des groupes d'attributs.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau privé virtuel d'accès à distance (RAVPN) avec configuration IKEV2/IPsec sur un routeur Cisco IOS® XE via CLI
- Configuration de Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocole RADIUS

### Composants utilisés

Ce document est basé sur les versions logicielles et matérielles suivantes :

- Cisco CSR1000V (VXE) - Version 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1
- Cisco Secure Client (CSC) - Version 5.0.05040
- Windows 11

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.

## Configurer

### Diagramme du réseau

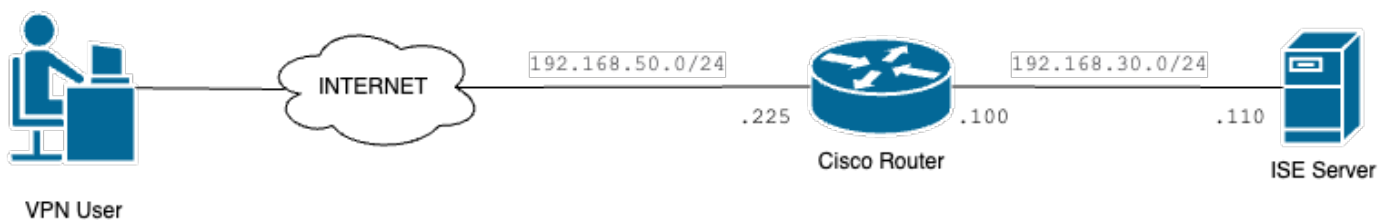


Schéma de réseau de base

## Configurations

### Configuration du routeur

Étape 1. Configurez un serveur RADIUS pour l'authentification et l'autorisation locale sur le périphérique :

```
aaa new-model
aaa group server radius FlexVPN-Authentication-Server
server-private 192.168.30.110 key Cisco123
aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server
aaa authorization network FlexVPN-Authorization-List local
```

La commande `aaa authentication login <list_name>` fait référence au groupe AAA (authentification, autorisation, and accounting) (qui définit le serveur RADIUS).

La commande `aaa authorization network <list_name> local` indique que des utilisateurs/groupes définis localement doivent être utilisés.

Étape 2 : configuration d'un point de confiance pour stocker le certificat du routeur Comme l'authentification locale du routeur est de type RSA, le périphérique nécessite que le serveur s'authentifie à l'aide d'un certificat :

```
crypto pki trustpoint FlexVPN-TP
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
revocation-check none
rsa-keypair FlexVPN_KEY
```

Étape 3. Définissez un pool d'adresses IP locales pour chaque groupe d'utilisateurs :

```
ip local pool group1 172.16.10.1 172.16.10.50
ip local pool group2 172.16.20.1 172.16.20.50
```

Étape 4. Configurez la stratégie d'autorisation locale :

```
crypto ikev2 authorization policy FlexVPN-Local-Policy
```

Aucune configuration n'est requise sur la stratégie d'autorisation, car le serveur d'authentification est responsable de l'envoi des valeurs appropriées (DNS, pool, routes protégées, etc.) en fonction du groupe auquel appartient l'utilisateur. Cependant, il doit être configuré pour définir le nom d'utilisateur dans notre base de données d'autorisation locale.

Étape 5 (facultatif). Créez une proposition et une stratégie IKEv2 (si elles ne sont pas configurées, les valeurs par défaut intelligentes sont utilisées) :

```
crypto ikev2 proposal IKEv2-prop
  encryption aes-cbc-256
  integrity sha256
  group 14
```

```
crypto ikev2 policy IKEv2-pol
  proposal IKEv2-prop
```

Étape 6 (facultatif). Configurez le transform-set (s'il n'est pas configuré, les valeurs Smart par défaut sont utilisées) :

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
  mode tunnel
```

Étape 7. Configurez un profil IKEv2 avec les identités locales et distantes appropriées, les

méthodes d'authentification (locales et distantes), le point de confiance, AAA et l'interface de modèle virtuelle utilisée pour les connexions :

```
crypto ikev2 profile FlexVPN-IKEv2-Profile
match identity remote key-id cisco.example
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FlexVPN-TP
aaa authentication eap FlexVPN-Authentication-List
aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy
aaa authorization user eap cached
virtual-template 100
```

La commande `aaa authorization user eap cached` spécifie que les attributs reçus pendant l'authentification EAP doivent être mis en cache. Cette commande est essentielle pour la configuration car sans elle, les données envoyées par le serveur d'authentification ne sont pas utilisées, ce qui entraîne l'échec de la connexion.



Remarque : l'ID de clé distante doit correspondre à la valeur de l'ID de clé dans le fichier XML. S'il n'est pas modifié dans le fichier XML, la valeur par défaut (\*\$AnyConnectClient\$\*) est utilisée et doit être configurée sur le profil IKEv2.

---

Étape 8. Configurez un profil IPsec et attribuez le transform-set et le profil IKEv2 :

```
crypto ipsec profile FlexVPN-IPsec-Profile
set transform-set TS
set ikev2-profile FlexVPN-IKEv2-Profile
```

Étape 9. Configurer une interface de bouclage Les interfaces d'accès virtuel lui empruntent l'adresse IP :

```
interface Loopback100
```

```
ip address 10.0.0.1 255.255.255.255
```

Étape 10. Créez le modèle virtuel qui sera utilisé pour créer les différentes interfaces d'accès virtuel et liez le profil IPsec créé à l'étape 8 :

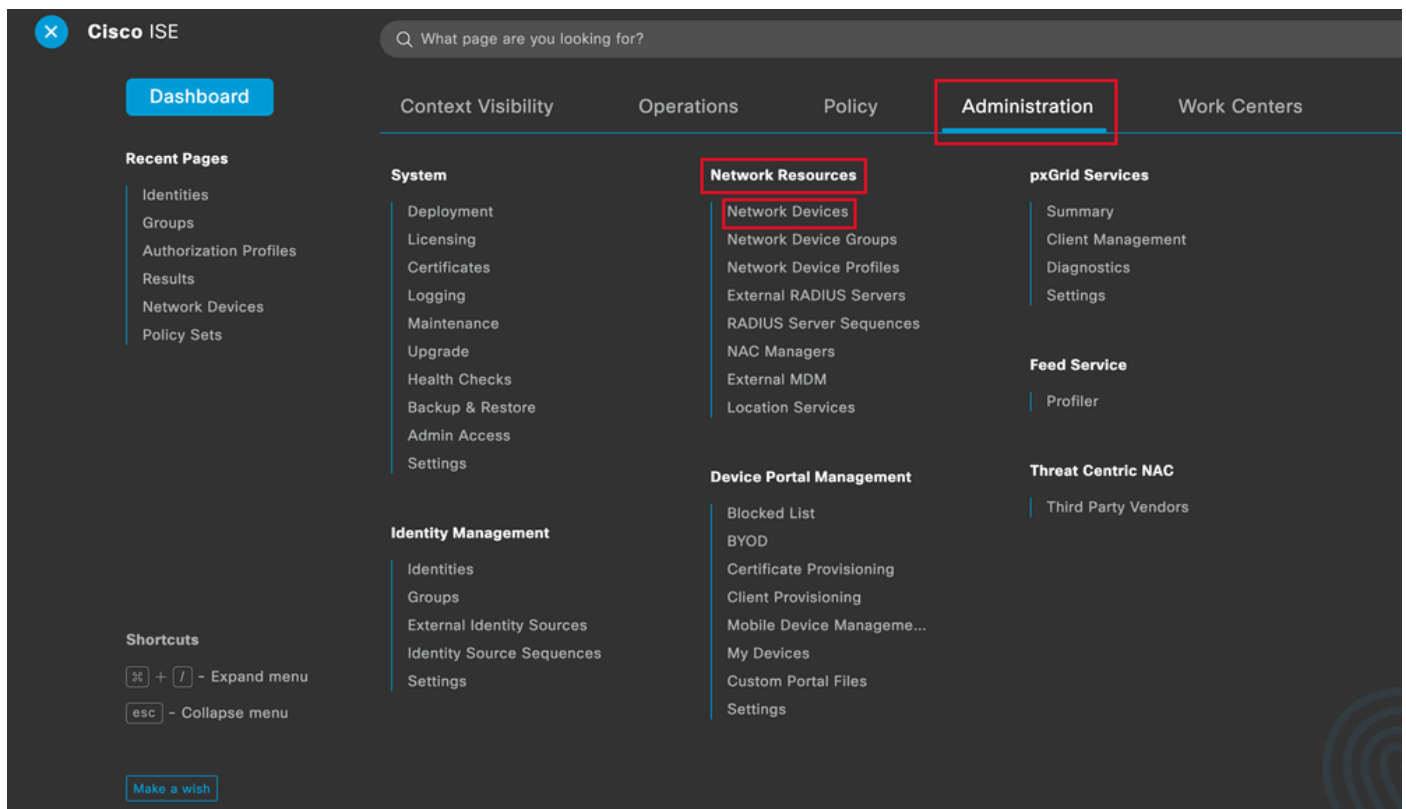
```
interface Virtual-Template100 type tunnel
ip unnumbered Loopback100
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

Étape 11. Désactivez la recherche de certificat basée sur HTTP-URL et le serveur HTTP sur le routeur :

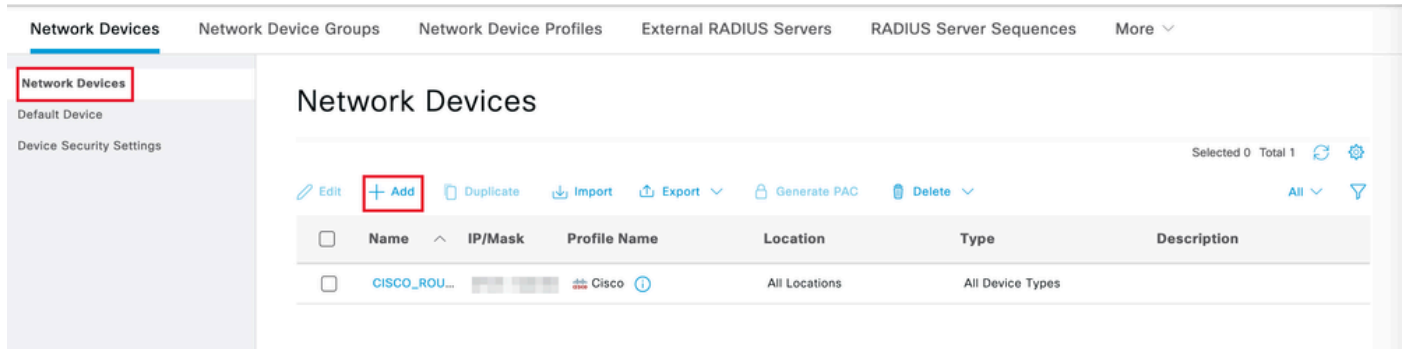
```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

## Configuration ISE (Identity Services Engine)

Étape 1. Connectez-vous au serveur ISE et accédez à Administration > Network Resources > Network Devices:



Étape 2. Cliquez sur Add pour configurer le routeur en tant que client AAA :



Ajout d'un nouveau périphérique réseau

Entrez les champs Nom du périphérique réseau et Adresse IP, puis cochez la case Paramètres d'authentification RADIUS et ajoutez le secret partagé, cette valeur doit être la même que celle qui a été utilisée lors de la création de l'objet Serveur RADIUS sur le routeur.

## Network Devices

Name

Description

IP Address

Nom et adresse IP

## ✓ RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol

RADIUS

Shared Secret

\*\*\*\*\*

Show

Use Second Shared Secret ⓘ

networkDevices.secondSharedSecret

Show

Mot de passe Radius

Cliquez sur Save.

Étape 3. Accédez à Administration > Identity Management > Groups :

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted with a red box), and 'Work Centers'. The left sidebar lists 'Recent Pages' (Identities, Groups, Authorization Profiles, Results, Policy Sets) and 'Shortcuts'. The main content area is divided into several sections: 'System' (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), 'Network Resources' (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), 'Device Portal Management' (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Manageme..., My Devices, Custom Portal Files, Settings), 'pxGrid Services' (Summary, Client Management, Diagnostics, Settings), 'Feed Service' (Profiler), and 'Threat Centric NAC' (Third Party Vendors). The 'Identity Management' section is highlighted with a red box, and the 'Groups' link within it is also highlighted with a red box.

Menu général ISE

Étape 4. Cliquez sur User Identity Groups, puis sur Add :



## Identity Groups

EQ



> Endpoint Identity Groups

> User Identity Groups

## User Identity Groups

Selected 0 Total 10

Edit **+ Add** Delete Import Export

All Filter

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group

Ajouter un nouveau groupe

Saisissez le nom du groupe et cliquez sur Submit.

### Identity Group

\* Name Group1

Description

Submit

Cancel

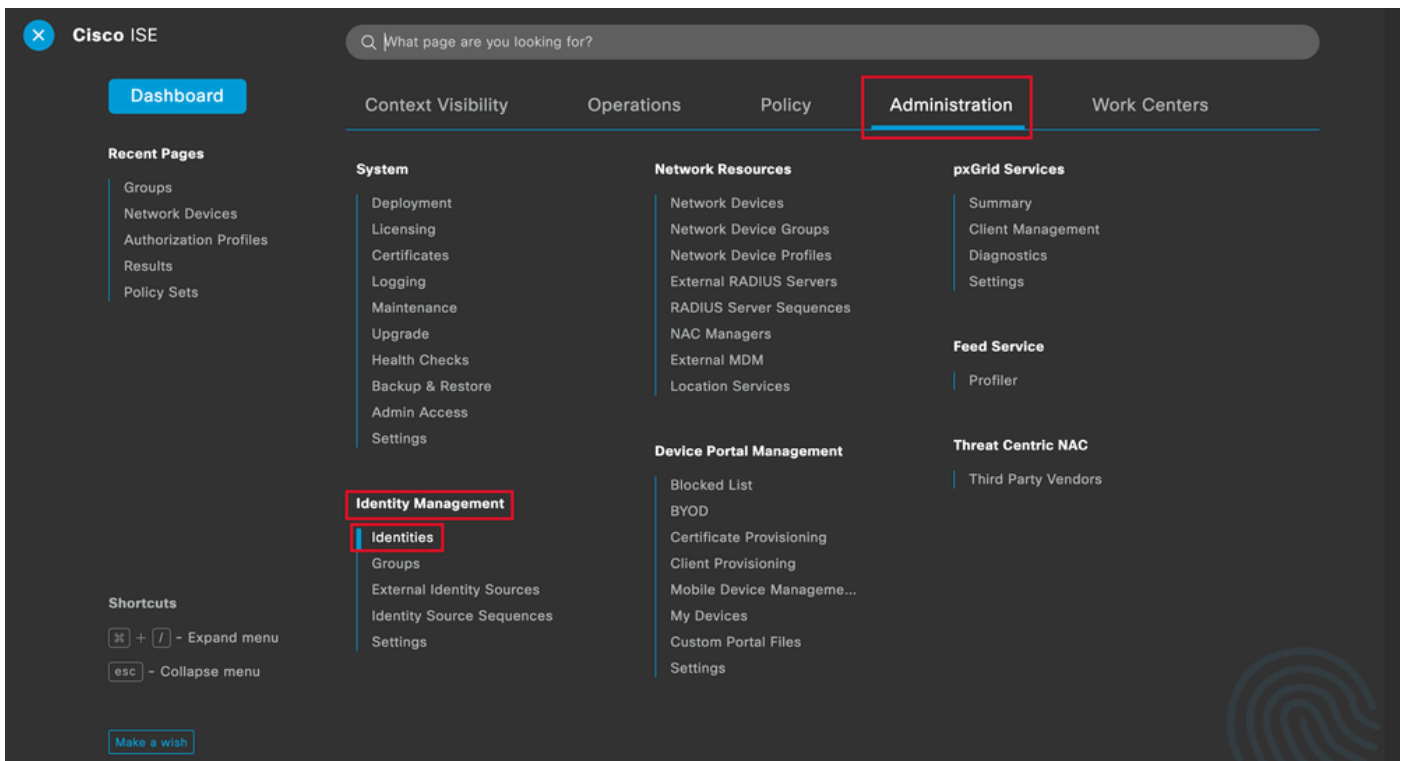
Informations de groupe



Remarque : répétez les étapes 3 et 4 pour créer autant de groupes que nécessaire.

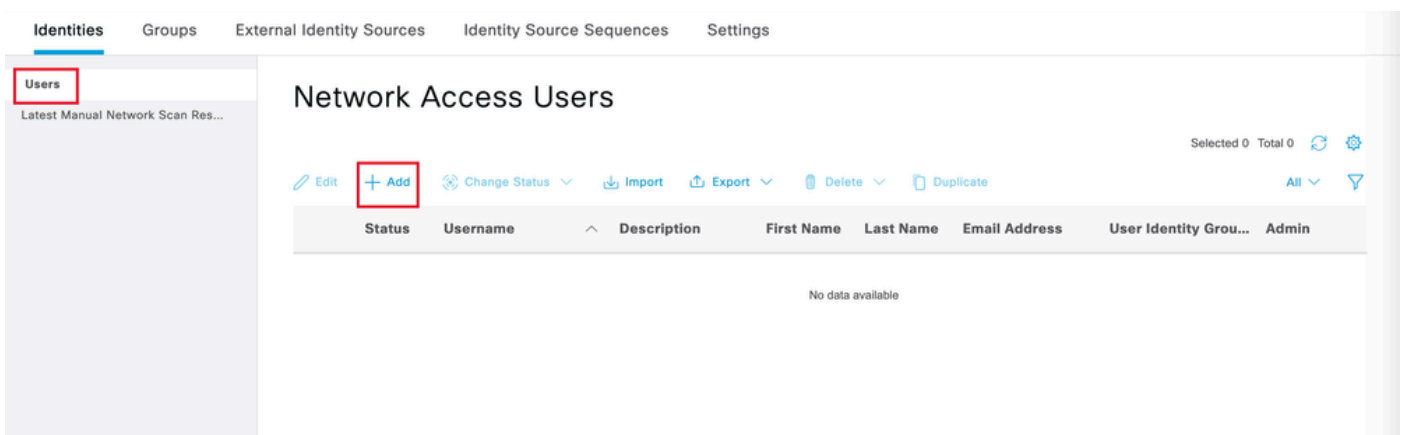
---

Étape 5. Accédez à Administration > Identity Management > Identities :



Menu général ISE

Étape 6. Cliquez sur Add afin de créer un nouvel utilisateur dans la base de données locale du serveur :



Ajouter un utilisateur

Saisissez le nom d'utilisateur et le mot de passe de connexion. Accédez ensuite à la fin de cette page et sélectionnez le groupe d'utilisateurs :

Network Access User

\* Username user1

Status  Enabled

Email

Passwords

Password Type: Internal Users

Password \* Login Password ..... Re-Enter Password .....

Generate Password ⓘ

Generate Password ⓘ

Enable Password

Nom d'utilisateur et mot de passe

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 20

User Groups

User Groups

ALL\_ACCOUNTS (default)

Employee

Group1

Group2

GROUP\_ACCOUNTS (default)

Select an item

Affecter le groupe approprié à l'utilisateur

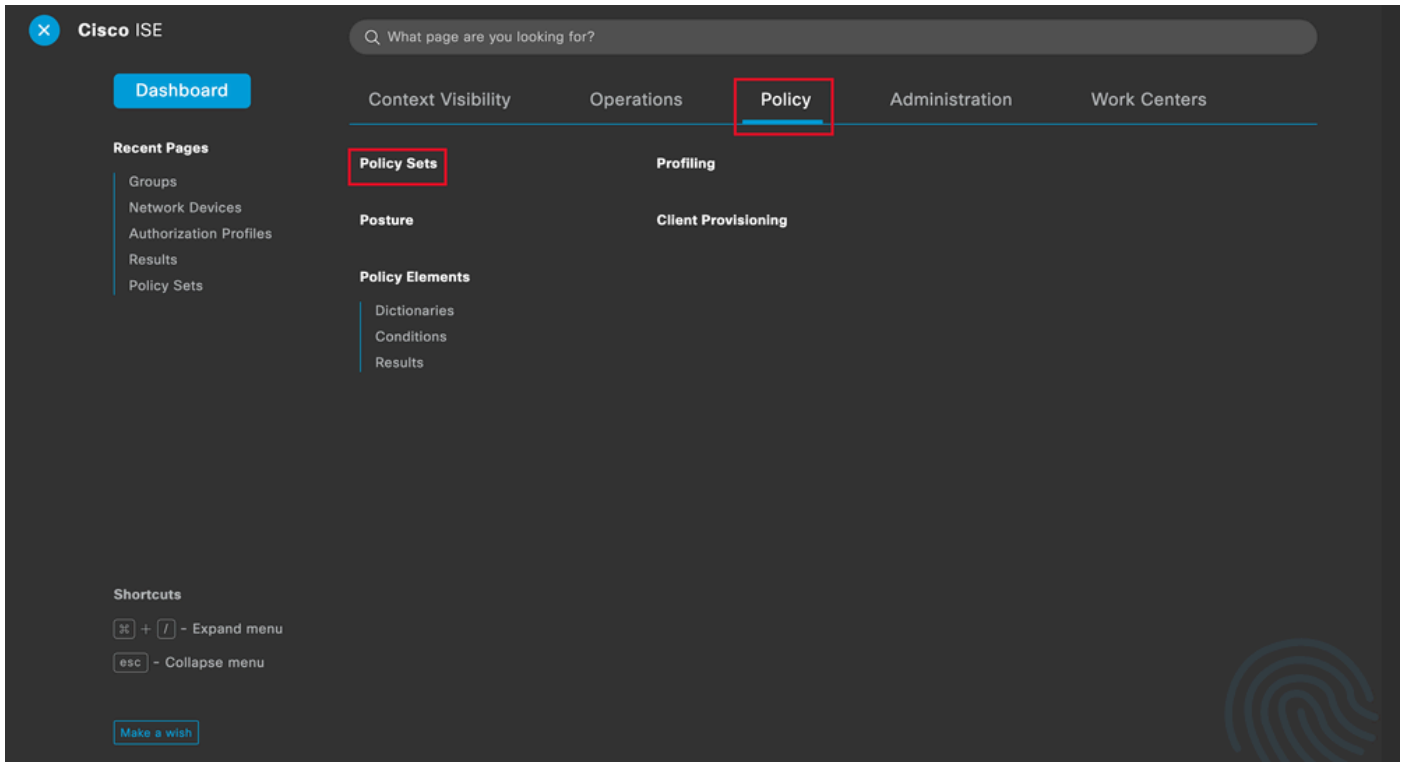
Cliquez sur Save.



Remarque : répétez les étapes 5 et 6 pour créer les utilisateurs dont vous avez besoin et les affecter au groupe correspondant.

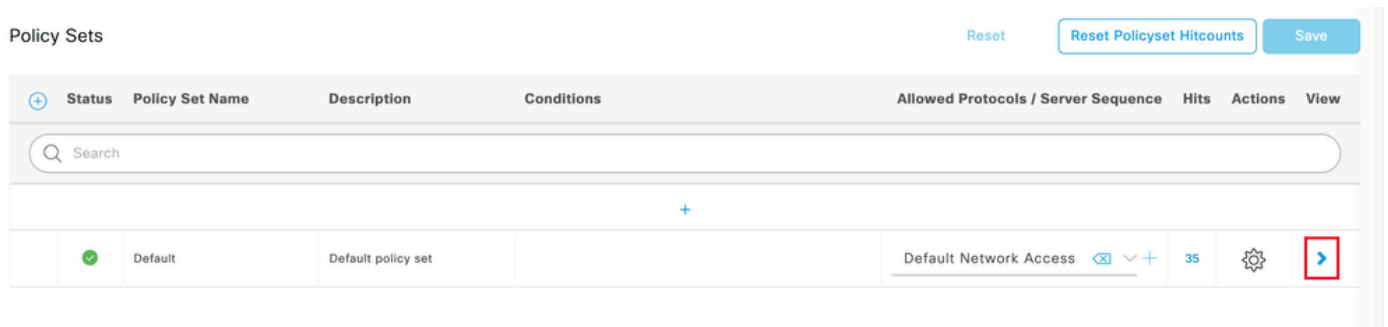
---

Étape 7. Accédez à Policy > Policy Sets :



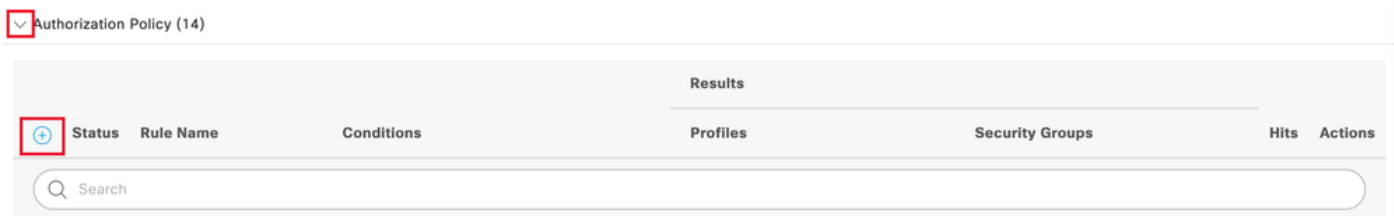
Menu général ISE

Sélectionnez la stratégie d'autorisation par défaut en cliquant sur la flèche située à droite de l'écran :



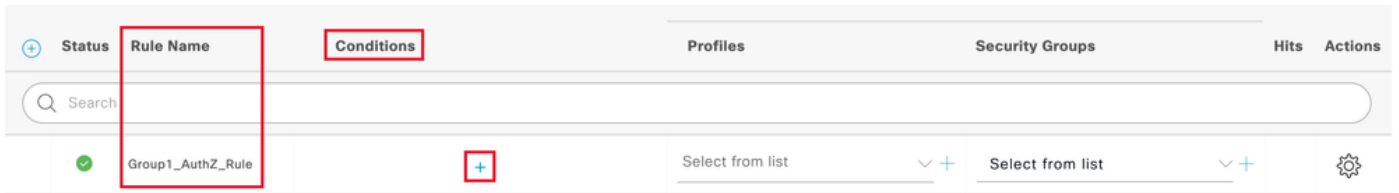
Sélectionnez la stratégie d'autorisation

Étape 8. Cliquez sur la flèche du menu déroulant en regard de Politique d'autorisation pour la développer. Ensuite, cliquez sur l'icône add (+) afin d'ajouter une nouvelle règle :



Ajouter une nouvelle règle d'autorisation

Entrez le nom de la règle et sélectionnez l'icône d'ajout (+) dans la colonne Conditions :



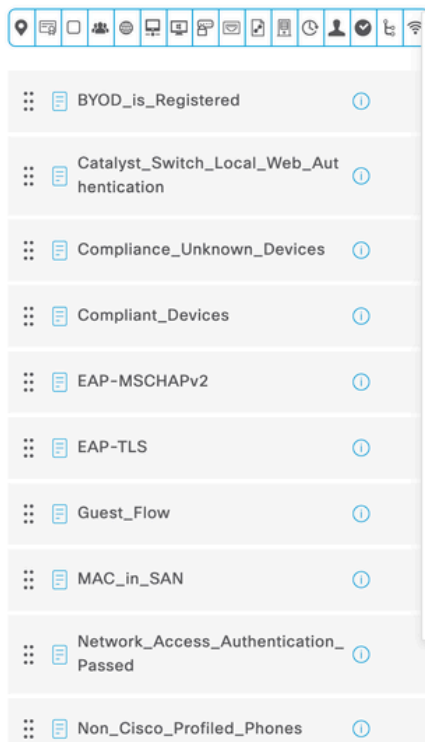
Ajouter une condition

Étape 9. Cliquez dans la zone de texte Éditeur d'attributs et cliquez sur le groupe Identité. Sélectionnez l'attribut Groupe d'identités - Nom :

## Conditions Studio

### Library

Search by Name



### Editor

Click to add an attribute

#### Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		
IdentityGroup	Description		
IdentityGroup	Name		
InternalUser	IdentityGroup		
PassiveID	PassiveID_Groups		

Sélectionnez la condition

Sélectionnez Égal à en tant qu'opérateur, puis cliquez sur la flèche du menu déroulant pour afficher les options disponibles et sélectionnez Groupes d'identités d'utilisateurs : <GROUP\_NAME>.

## Editor

IdentityGroup-Name

Equals

Choose from list or type

Set to 'Is not'

User Identity Groups:GROUP\_ACCOUNTS (default)

**User Identity Groups:Group1**

User Identity Groups:Group2

User Identity Groups:GuestType\_Contractor (default)

User Identity Groups:GuestType\_Daily (default)

Save

Sélectionnez le groupe

Cliquez sur Save.

Étape 10. Dans la colonne Profiles, cliquez sur l'icône add (+) et choisissez Create a New Authorization Profile :

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Group1_AuthZ_Rule	IdentityGroup-Name EQUALS User Identity Groups:Group1	Select from list <b>+</b>	Select from list	10	⚙️
✓	Wireless Black List Default	Wireless_Access AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	<b>Create a New Authorization Profile</b>	Select from list	0	⚙️

Créer le profil d'autorisation

Saisissez le nom du profil




# Add New Standard Profile

## Authorization Profile


\* Name Profile\_group1


Description


\* Access Type ACCESS\_ACCEPT

Network Device Profile  Cisco

Service Template

Track Movement  

Agentless Posture  

Passive Identity Tracking  

### Informations de profil

Accédez à la fin de cette page jusqu'à Advanced Attribute Settings, puis cliquez sur la flèche du menu déroulant. Cliquez ensuite sur Cisco et sélectionnez cisco-av-pair--[1] :

Advanced Attributes Settings

Select an item  =

**Cisco**

Search:

- 
- cisco-account-info--[250]
- cisco-assign-ip-pool--[218]
- 
- cisco-call-filter--[243]
- cisco-call-id--[141]

Attributes Details

Access Type = ACCESS\_ACCEPT

Sélectionnez le type d'attribut

Ajoutez l'attribut cisco-av-pair que vous souhaitez configurer et cliquez sur l'icône add (+) pour ajouter un autre attribut :

### Advanced Attributes Settings

⋮ Cisco:cisco-av-pair = ipsec:dns-servers=10.0.50.10 +

Configuration de l'attribut

Remarque : pour connaître les spécifications d'attribut (nom, syntaxe, description, exemple, etc.), consultez le guide de configuration des attributs RADIUS FlexVPN :

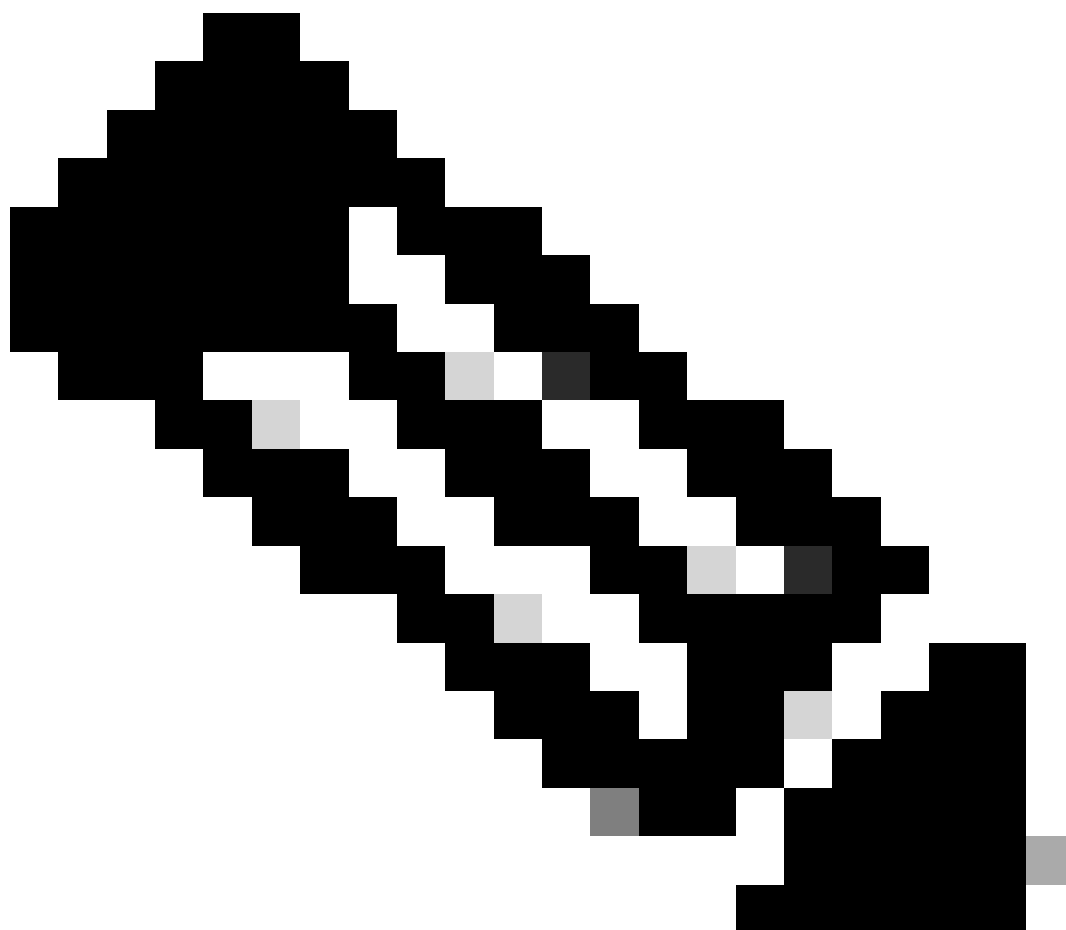
[Guide de configuration FlexVPN et Internet Key Exchange version 2, Cisco IOS XE Fuji](#)

---

## [16.9.x - Attributs RADIUS pris en charge](#)

---

---



Remarque : répétez l'étape précédente pour créer les attributs nécessaires.

---

Cliquez sur Save.

Les attributs suivants ont été attribués à chaque groupe :

- Attributs du groupe 1 :

Advanced Attributes Settings

⋮	Cisco:cisco-av-pair	=	ipsec:dns-servers=10.0.50.10	-
⋮	Cisco:cisco-av-pair	=	ipsec:route-set=prefix 192.168.100.0/24	-
⋮	Cisco:cisco-av-pair	=	ipsec:addr-pool=group1	+ -

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = ipsec:dns-servers=10.0.50.101  
cisco-av-pair = ipsec:route-set=prefix 192.168.100.0/24  
cisco-av-pair = ipsec:addr-pool=group1

Attribut Group1

- Attributs du groupe 2 :

Advanced Attributes Settings

⋮	Cisco:cisco-av-pair	=	ipsec:dns-servers=10.0.50.20	-
⋮	Cisco:cisco-av-pair	=	ipsec:route-set=prefix 192.168.200.0/24	-
⋮	Cisco:cisco-av-pair	=	ipsec:addr-pool=group2	+ -

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = ipsec:dns-servers=10.0.50.202  
cisco-av-pair = ipsec:route-set=prefix 192.168.200.0/24  
cisco-av-pair = ipsec:addr-pool=group2

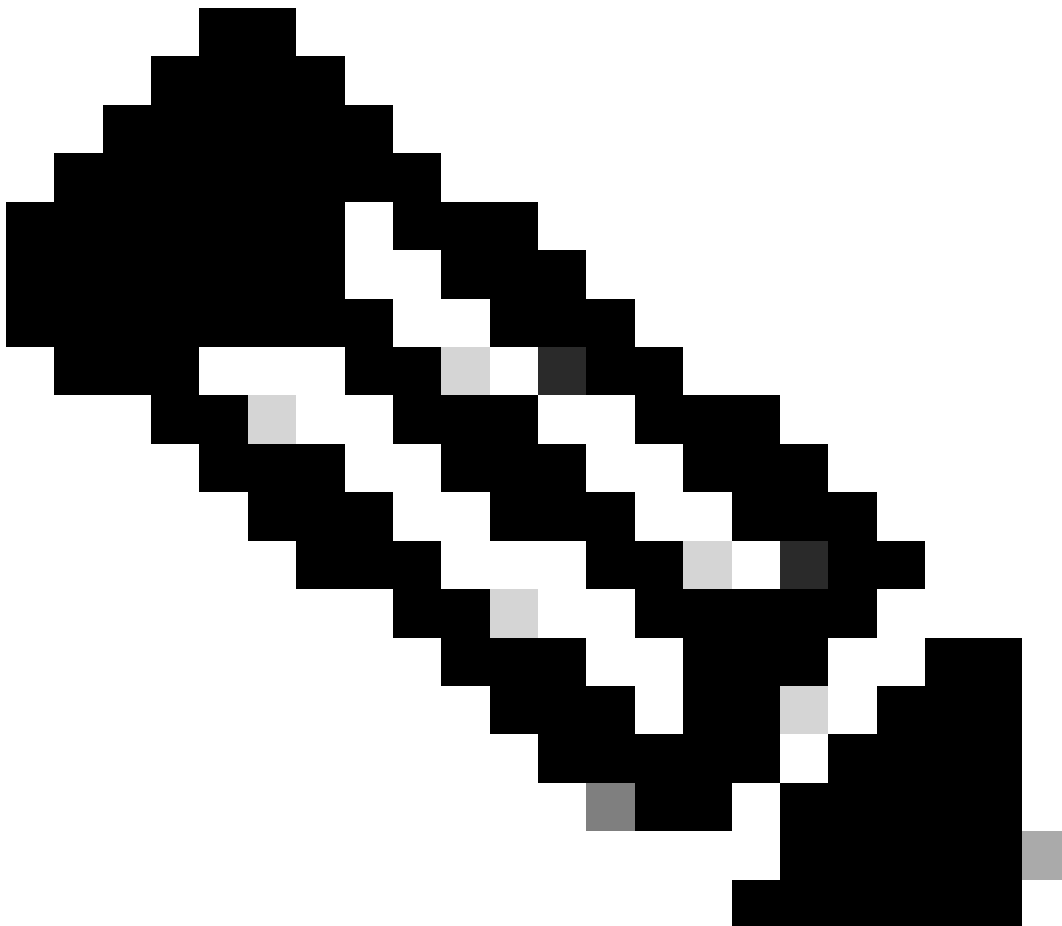
Attributs du groupe 2

Étape 11. Cliquez sur la flèche du menu déroulant et sélectionnez le profil d'autorisation créé à l'étape 10 :

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Group1_AuthZ_Rule	IdentityGroup-Name EQUALS User Identity Groups:Group1	Select from list	Select from list	10	⚙️
✓	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	DenyAccess NSP_Onboard Non_Cisco_IP_Phones PermitAccess Profile_group1	Select from list	0	⚙️
✓	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Non_Cisco_IP_Phones	Select from list	0	⚙️
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0	⚙️

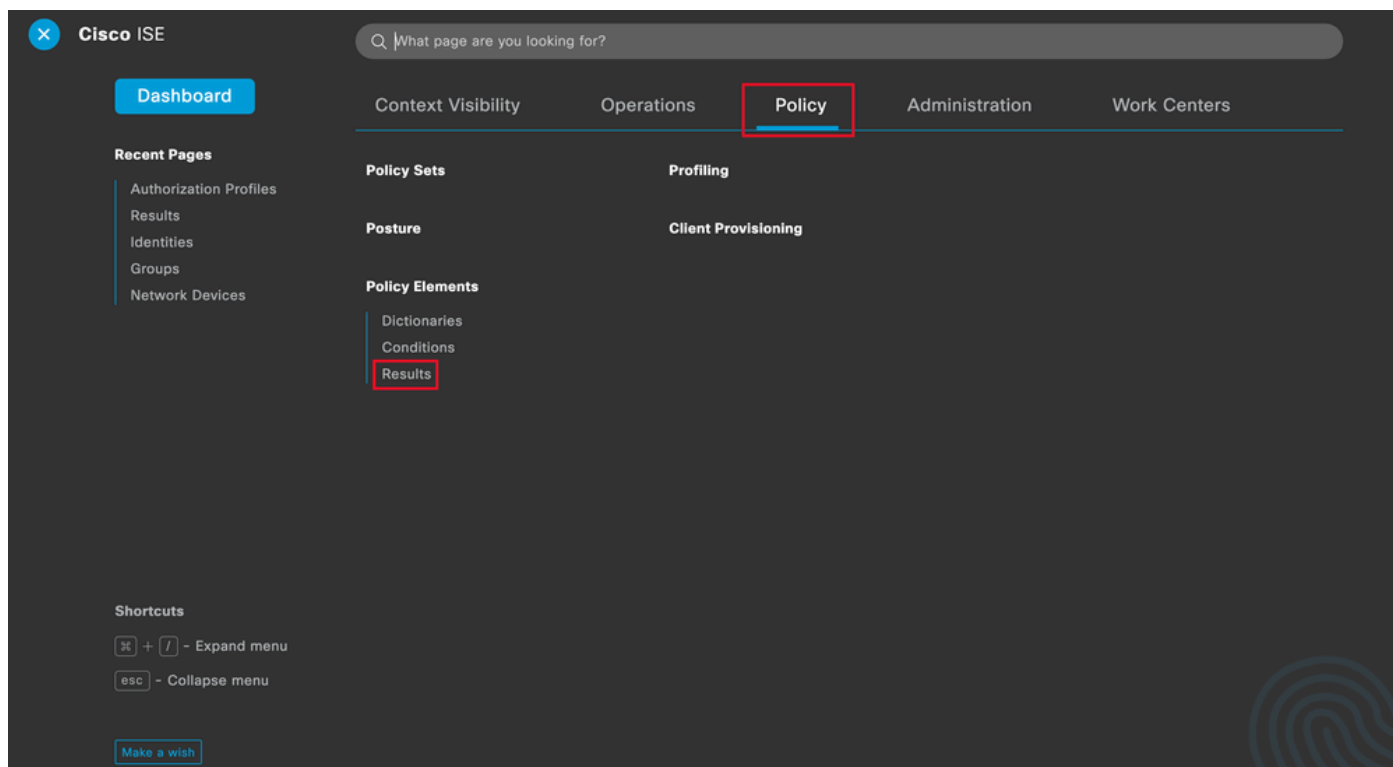
Attribuer un profil d'autorisation

Cliquez sur Save.



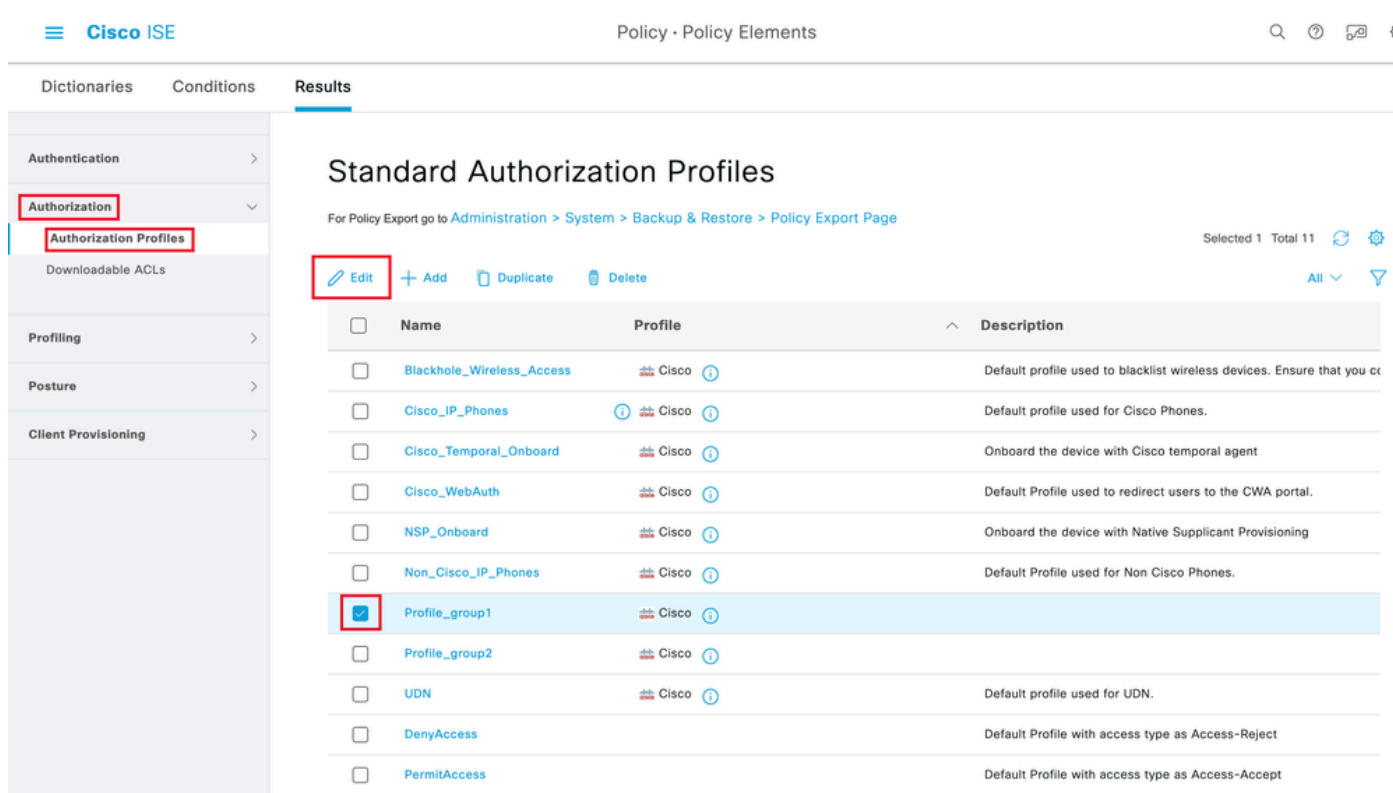
Remarque : répétez les étapes 8 à 11 pour créer les règles d'autorisation nécessaires pour chaque groupe.

Étape 12 (facultative). Si vous devez modifier le profil d'autorisation, accédez à Policy > Results :



Menu général ISE

Accédez à Autorisation > Profils d'autorisation. Cochez la case du profil que vous souhaitez modifier, puis cliquez sur Modifier :



Modifier le profil d'autorisation

## Configuration du client

Étape 1. Créez un profil XML à l'aide de l'éditeur de profil XML. Cet exemple est celui utilisé pour la création de ce document :

```
<#root>
```

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
    <ShowPreConnectMessage>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreLinux>All</CertificateStoreLinux>
    <CertificateStoreOverride>true</CertificateStoreOverride>
    <ProxySettings>Native</ProxySettings>
    <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
    <AuthenticationTimeout>30</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4, IPv6</IPProtocolSupport>
    <AutoReconnect UserControllable="false">
      true
    </AutoReconnect>
    <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
    <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">true</AutoUpdate>
    <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
    <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
    <PPPEExclusion UserControllable="false">
      Disable
    </PPPEExclusion>
    <PPPEExclusionServerIP UserControllable="false"/>
    <EnableScripting UserControllable="false">false</EnableScripting>
    <EnableAutomaticServerSelection UserControllable="false">
      false
    </EnableAutomaticServerSelection>
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
    <RetainVpnOnLogoff>false </RetainVpnOnLogoff>
    <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
    <AllowManualHostInput>true</AllowManualHostInput>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>
FlexVPN HUB
      </HostName>
      <HostAddress>
```

192.168.50.225

```
</HostAddress>  
<PrimaryProtocol>
```

**IPsec**

```
<StandardAuthenticationOnly>  
true  
<AuthMethodDuringIKENegotiation>
```

**EAP-MD5**

```
</AuthMethodDuringIKENegotiation>  
<IKEIdentity>
```

**cisco.example**

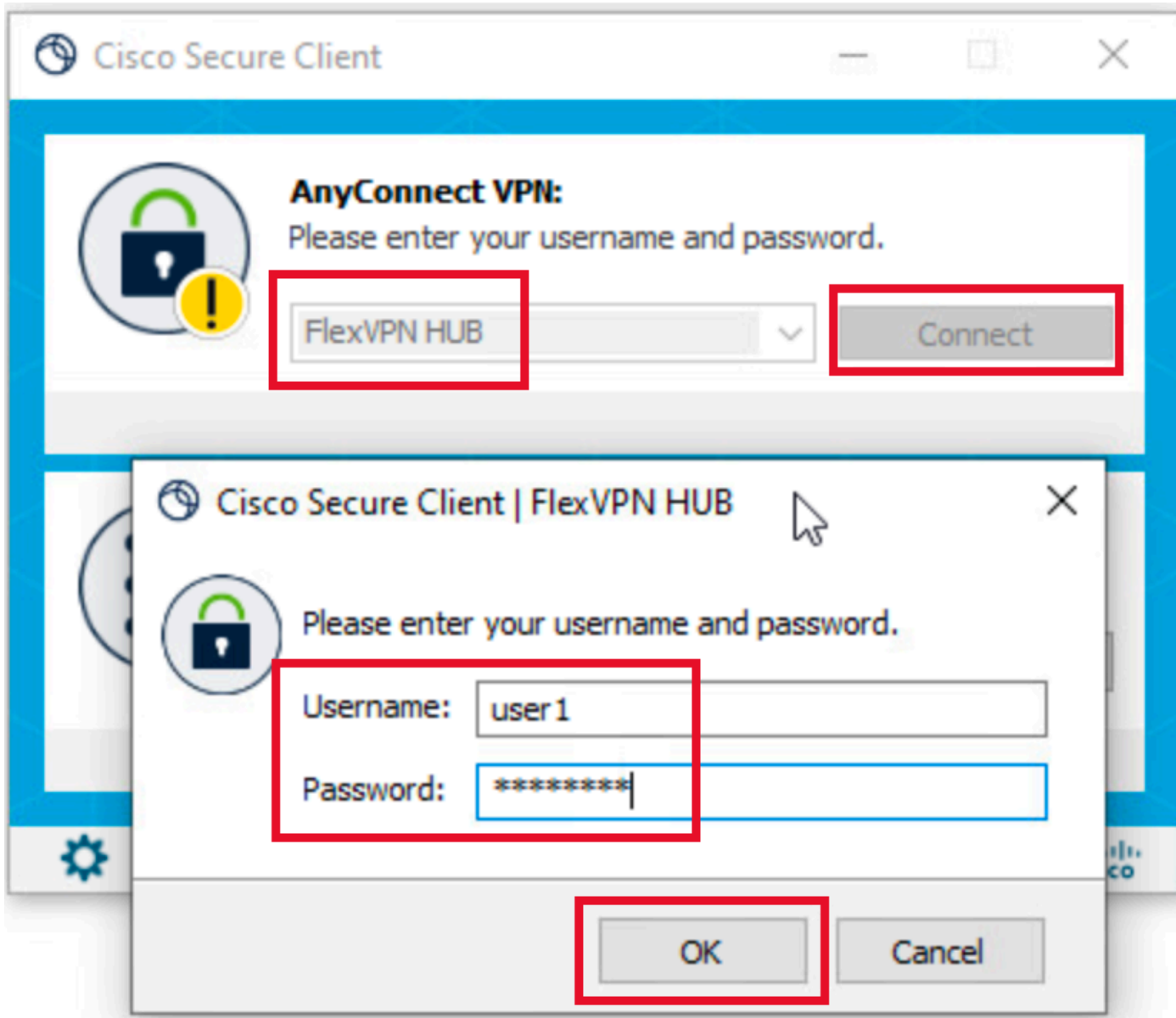
```
</IKEIdentity>  
</StandardAuthenticationOnly>  
</PrimaryProtocol>  
</HostEntry>  
</ServerList>  
</AnyConnectProfile>
```

- **<HostName>** : alias utilisé pour faire référence à l'hôte, à l'adresse IP ou au nom de domaine complet (FQDN). Ce message s'affiche dans la zone CSC.
- **<HostAddress>** : adresse IP ou nom de domaine complet du concentrateur FlexVPN.
- **<PrimaryProtocol>** - Doit être défini sur IPsec pour forcer le client à utiliser IKEv2/IPsec au lieu de SSL.
- **<AuthMethodDuringIKENegotiation>** - Doit être défini pour utiliser EAP-MD5 dans EAP. Ceci est requis pour l'authentification sur le serveur ISE.
- **<IKEIdentity>** - Cette chaîne est envoyée par le client comme charge utile ID\_GROUP type ID. Cela peut être utilisé pour faire correspondre le client à un profil IKEv2 spécifique sur le concentrateur.

## Vérifier

Étape 1. Accédez à l'ordinateur client sur lequel CSC est installé. Connectez-vous au concentrateur FlexVPN et saisissez les informations d'identification user1 :





Identifiants utilisateur1

Étape 2. Une fois la connexion établie, cliquez sur l'icône d'engrenage (coin inférieur gauche) et naviguez jusqu'à AnyConnectVPN > Statistics. Dans la section Address Information, vérifiez que l'adresse IP attribuée appartient au pool configuré pour le groupe 1 :

The screenshot shows the Cisco Secure Client interface. On the left, a navigation pane includes 'Status Overview', 'AnyConnect VPN' (highlighted with a red box), and 'Secure Endpoint'. The main area is titled 'Virtual Private Network (VPN)' and contains tabs for 'Preferences', 'Statistics' (highlighted with a red box), 'Route Details', 'Firewall', and 'Message History'. The 'Statistics' tab is active, displaying two sections: 'Connection Information' and 'Address Information' (both highlighted with red boxes). The 'Connection Information' section lists: State: Connected, Tunnel Mode (IPv4): Split Include, Tunnel Mode (IPv6): Drop All Traffic, Dynamic Tunnel Exclusion: None, Dynamic Tunnel Inclusion: None, Duration: 00:00:22, Session Disconnect: None, and Management Connection State: Disconnected (user tunnel active). The 'Address Information' section lists: Client (IPv4): 172.16.10.5, Client (IPv6): Not Available, and Server: [redacted]. At the bottom right of the statistics window are 'Reset' and 'Export Stats' buttons.

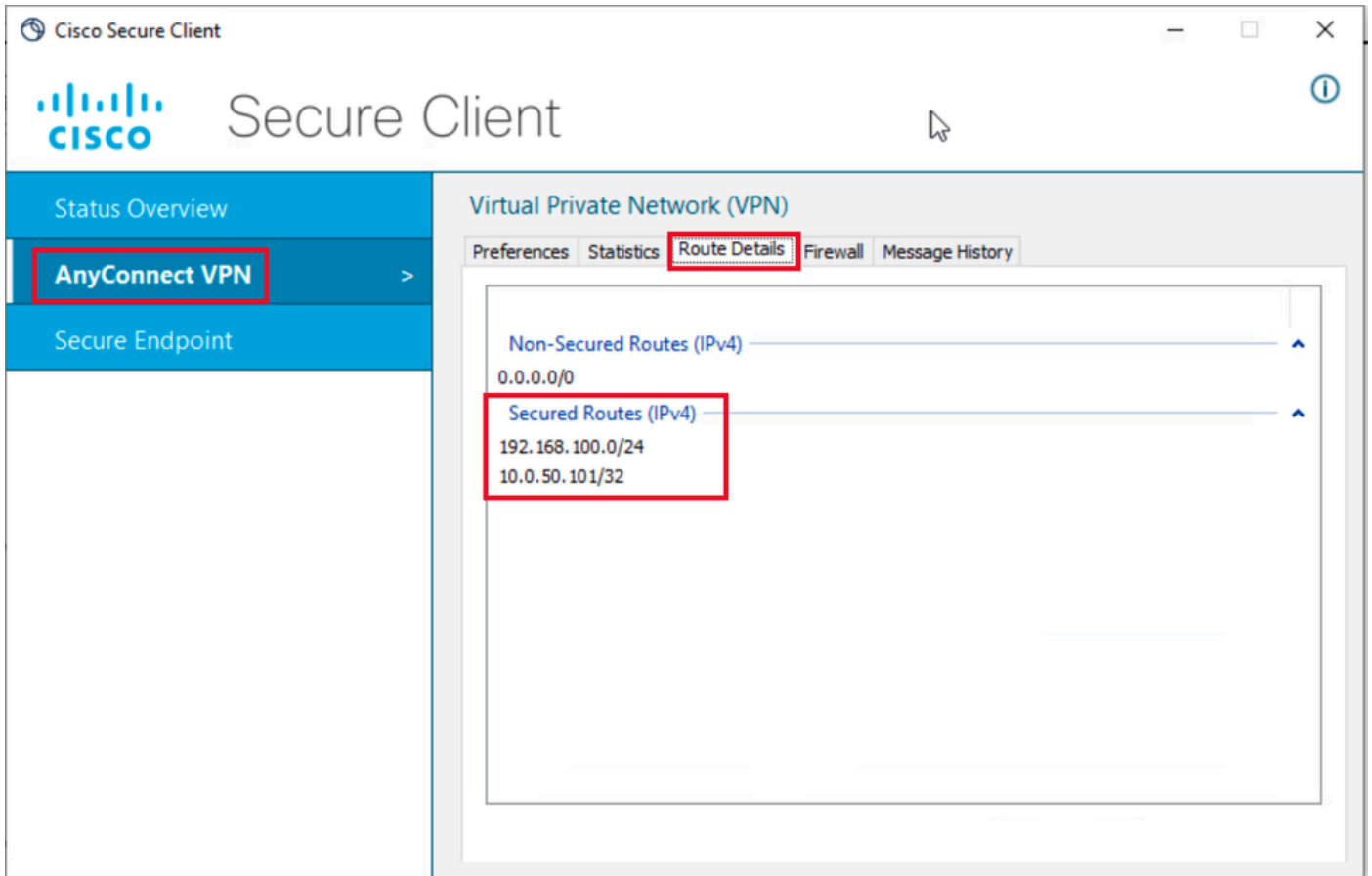
Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:22
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information	
Client (IPv4):	172.16.10.5
Client (IPv6):	Not Available
Server:	[redacted]

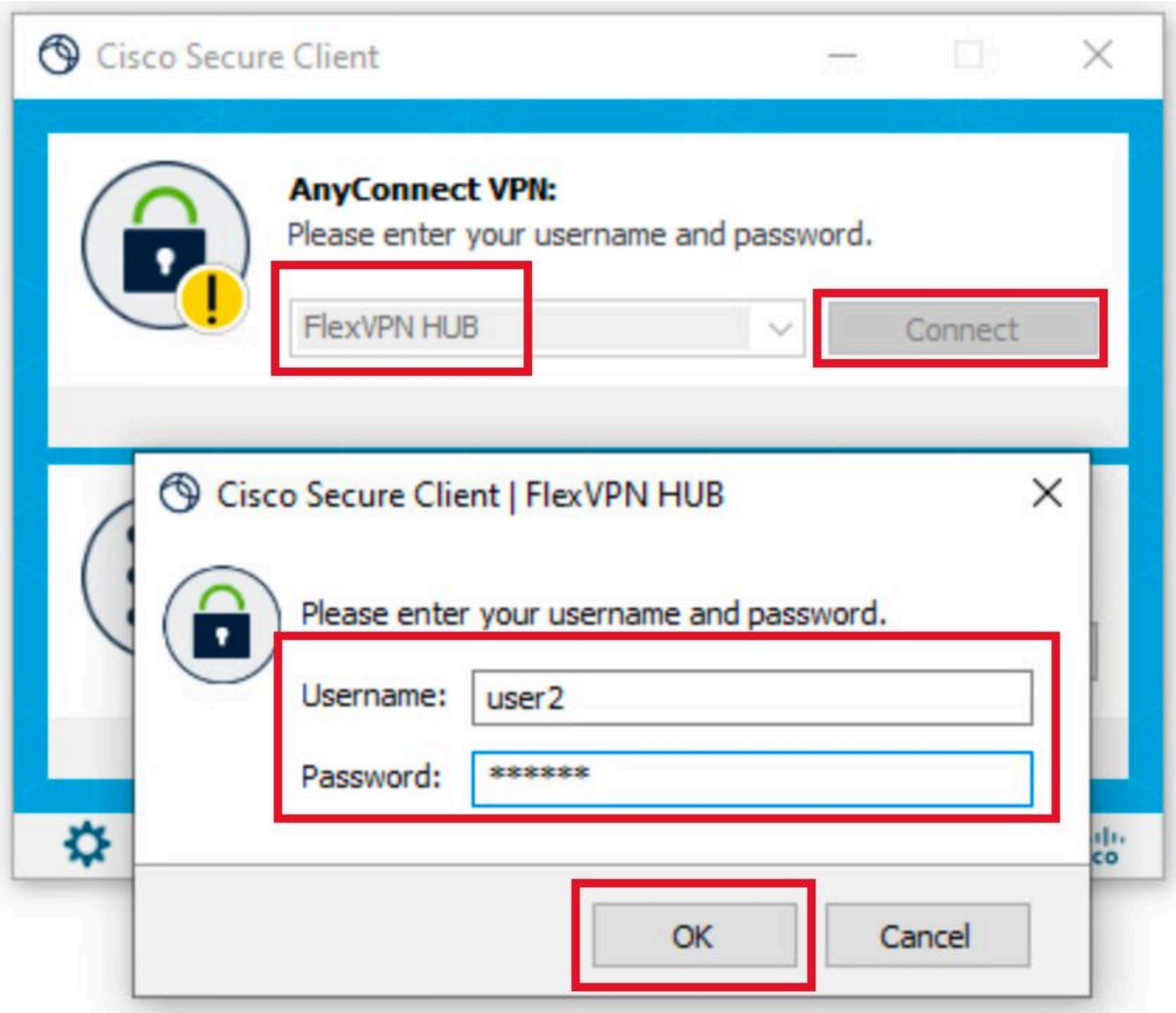
Statistiques utilisateur1

Accédez à AnyConnectVPN > Route details et vérifiez que les informations affichées correspondent aux routes sécurisées et au DNS configuré pour le groupe 1 :

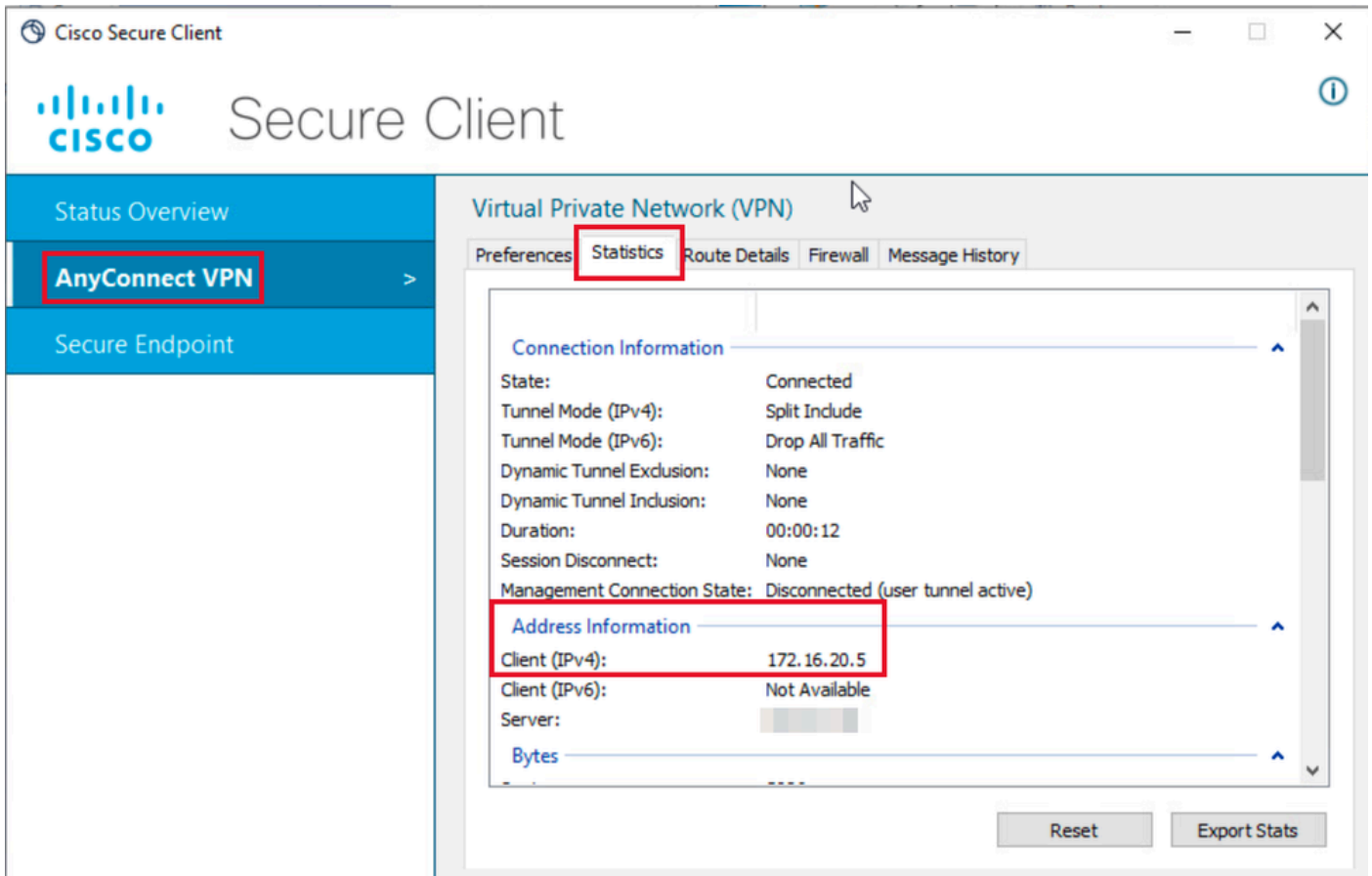


Détails de la route User1

Étape 3. Répétez les étapes 1 et 2 avec les informations d'identification de l'utilisateur 2 pour vérifier que les informations correspondent aux valeurs configurées sur la stratégie d'autorisation ISE pour ce groupe :



Informations d'identification utilisateur2



The screenshot shows the Cisco Secure Client interface with the 'AnyConnect VPN' section selected in the left sidebar. The main window displays the 'Virtual Private Network (VPN)' settings, with the 'Statistics' tab active. The 'Statistics' tab is highlighted with a red box. Below it, the 'Connection Information' section is expanded, showing the following details:

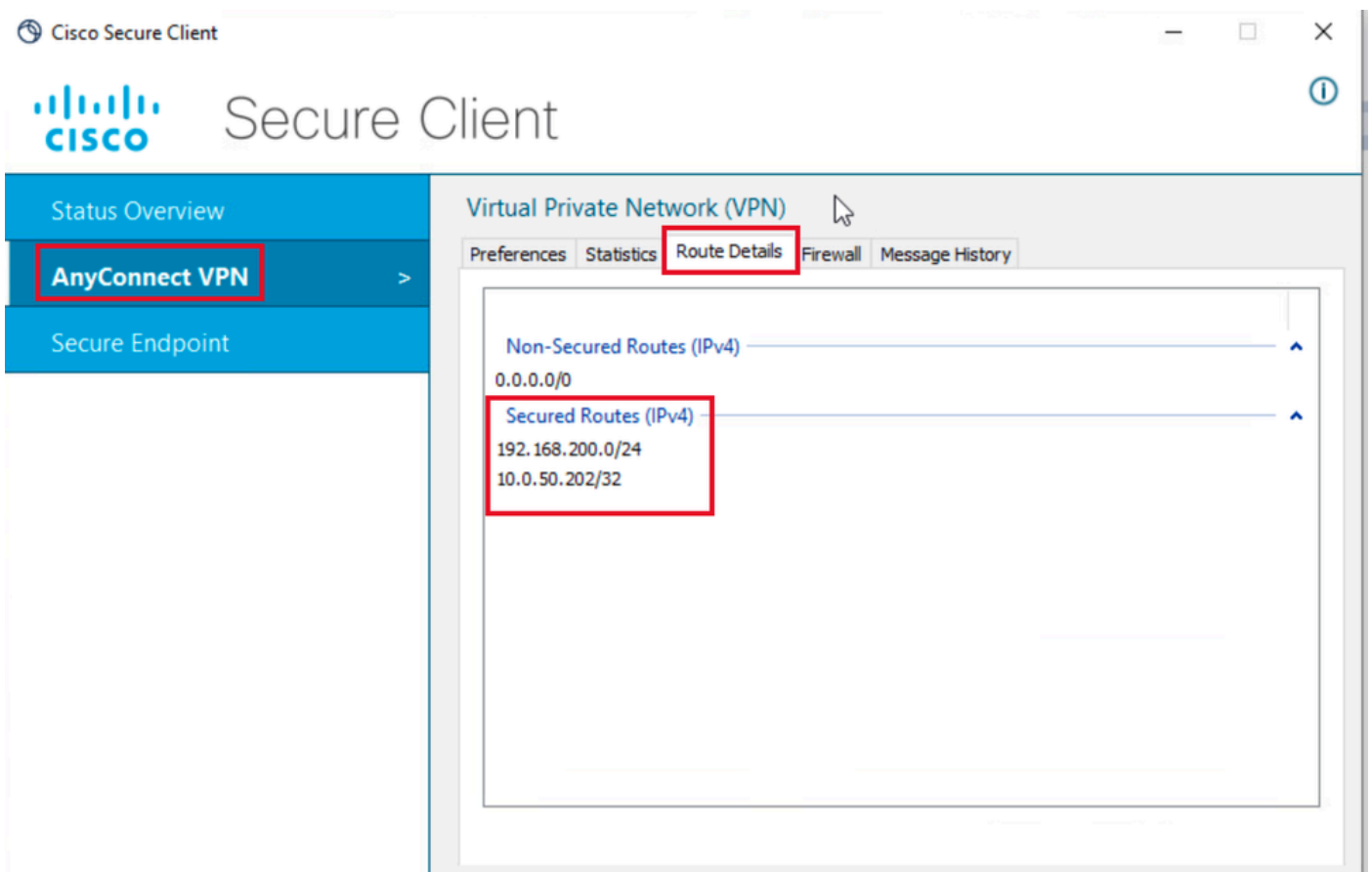
State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:12
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

The 'Address Information' section is also expanded and highlighted with a red box, showing:

Client (IPv4):	172.16.20.5
Client (IPv6):	Not Available
Server:	[Redacted]

At the bottom of the statistics window, there are 'Reset' and 'Export Stats' buttons.

Statistiques utilisateur2



The screenshot shows the Cisco Secure Client interface with the 'AnyConnect VPN' section selected in the left sidebar. The main window displays the 'Virtual Private Network (VPN)' settings, with the 'Route Details' tab active. The 'Route Details' tab is highlighted with a red box. Below it, the 'Secured Routes (IPv4)' section is expanded and highlighted with a red box, showing the following routes:

192.168.200.0/24
10.0.50.202/32

The 'Non-Secured Routes (IPv4)' section is also visible, showing the route 0.0.0.0/0.

Détails de la route User2

# Dépannage

## Débogages et journaux

Sur le routeur Cisco :

1. Utilisez les débogages IKEv2 et IPSec pour vérifier la négociation entre la tête de réseau et le client :

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. Utilisez les débogages AAA pour vérifier l'attribution des attributs locaux et/ou distants :

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

Sur ISE :

- Journaux RADIUS en direct

## Scénario de travail

Les résultats suivants sont des exemples de connexions réussies :

- Sortie du débogage User1 :

<#root>

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
```

```
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
```

```
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
```

```
Jan 30 02:57:21.088: vrfid: [65535] ipv6 tableid : [0]
```

```
Jan 30 02:57:21.088: idb is NULL
```

```
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IPv6: ::
```

Jan 30 02:57:21.089: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.089: RADIUS(000000FF): sending  
Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.089: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229

RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34  
Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.089: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12  
RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1]  
Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18  
RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II\*?0"  
Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.089: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.090: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.094: RADIUS:

Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5  
Jan 30 02:57:21.094: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8  
RADIUS: 01 52 00 06 0D 20 [ R ]  
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18  
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@0XH6]  
Jan 30 02:57:21.094: RADIUS(000000FF): Received from id 1645/85  
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes  
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (000000FF):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC  
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0  
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 02:57:21.097: idb is NULL

Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::  
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.097: RADIUS(000000FF): sending  
Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.097: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC

Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.098: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8  
RADIUS: 02 52 00 06 03 04 [ R]  
Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18  
RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g\$D&d]  
Jan 30 02:57:21.098: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.101: RADIUS:

Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1

Jan 30 02:57:21.101: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32  
RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC 0F B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai  
Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18  
RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL!]  
Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86  
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes  
Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):



Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC  
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-  
Jan 30 02:57:21.103: RADIUS(000000FF): Config NAS IP: 0.0.0.0  
Jan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]  
Jan 30 02:57:21.104: idb is NULL  
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::  
Jan 30 02:57:21.104: RADIUS/ENCODE(000000FF): acct\_session\_id: 4245  
Jan 30 02:57:21.104: RADIUS(000000FF): sending  
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded  
Jan 30 02:57:21.104: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332

RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46  
Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z  
Jan 30 02:57:21.104: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21  
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24  
RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/]  
Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18  
RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>Tv]  
Jan 30 02:57:21.104: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]  
Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet  
Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout  
Jan 30 02:57:21.170: RADIUS:

Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233

RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6  
Jan 30 02:57:21.170: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.170: RADIUS: Class [25] 68  
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]

```
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]
RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams()]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31
```

```
"ipsec:dns-servers=10.0.50.101"
```

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41
```

```
"ipsec:route-set=prefix 192.168.100.0/24"
```

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24
```

```
"ipsec:addr-pool=group1"
```

```
Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f
Jan 30 02:57:21.175: AAA/AUTHOR (0x100):
```

```
Pick method list 'FlexVPN-Authorization-List'
```

```
Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
Jan 30 02:57:21.192: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:
```

```
Line protocol on Interface Virtual-Access1, changed state to up
```

- Sortie du débogage User2 :

```
<#root>
```

```
Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f
Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.103: RADIUS(00000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229

RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64

Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]

Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26

Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"

Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36

Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phrase1-id=cisco.example"

Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"

Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64

Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"

Jan 30 03:28:58.104: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21

Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"

Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12

RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]

Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18

RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]

Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100

Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet

Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout

Jan 30 03:28:58.109: RADIUS:

Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43

Jan 30 03:28:58.109: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8

RADIUS: 01 35 00 06 0D 20 [ 5 ]

Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18

RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]

Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88

RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes

Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC

Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-

Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0

Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]

Jan 30 03:28:58.113: idb is NULL

Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: ::

Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct\_session\_id: 4249

Jan 30 03:28:58.113: RADIUS(00000103): sending

Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1

Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded

Jan 30 03:28:58.113: RADIUS(00000103):

Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316

RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C

Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30

"isakmp-phrase1-id=cisco.example"

Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"

Jan 30 03:28:58.113: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21

Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"

Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8

RADIUS: 02 35 00 06 03 04 [ 5]

Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18

RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]

Jan 30 03:28:58.113: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100

Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet

Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout

Jan 30 03:28:58.116: RADIUS:

Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02

Jan 30 03:28:58.116: RADIUS: State [24] 91

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]

RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]

RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]

Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32

RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM]

Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18

RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]

Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89

RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes

Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-

Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0

Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0]

Jan 30 03:28:58.118: idb is NULL  
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: ::  
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct\_session\_id: 4249  
Jan 30 03:28:58.118: RADIUS(00000103): sending  
Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1  
Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded  
Jan 30 03:28:58.119: RADIUS(00000103):

Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332

RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE  
Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1]  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"  
Jan 30 03:28:58.119: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21  
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  
Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24  
RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w]  
Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18  
RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo]  
Jan 30 03:28:58.119: RADIUS: State [24] 91  
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]  
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]  
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]  
Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  
Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet  
Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout  
Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233  
RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD  
Jan 30 03:28:58.186: RADIUS: User-Name [1] 7

"user2"

Jan 30 03:28:58.186: RADIUS: Class [25] 68  
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]  
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]  
RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE]  
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]  
RADIUS: 33 30 [ 30]  
Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6  
RADIUS: 03 36 00 04 [ 6]  
Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18  
RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S]  
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37  
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31

"ipsec:dns-servers=10.0.50.202"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47

Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.200.0/24"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30

Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group2"

Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90

RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes

Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f

Jan 30 03:28:58.190: AAA/AUTHOR (0x104):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to

Jan 30 03:28:58.209: %SYS-5-CONFIG\_P: Configured programmatically by process Crypto INT from console as

Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access2, changed state to up

## Informations connexes

- [Assistance technique de Cisco et téléchargements](#)

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.