Configuration de l'exclusion du partage pour AnyConnect FlexVPN avec ISE

Table des matières

Introduction

Ce document décrit la procédure de configuration de l'exclusion partagée à l'aide d'ISE pour la connexion IKEv2 AnyConnect à un routeur Cisco IOS® XE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expérience de la configuration AnyConnect IPsec sur un routeur
- Configuration de Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocole RADIUS

Composants utilisés

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

- Cisco Catalyst 8000V (C8000V) - 17.12.04
- Client sécurisé Cisco - 5.0.02075
- Cisco ISE - 3.2.0
- Windows 10

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

Diagramme du réseau

Configurations

Afin de compléter la configuration, prenez en considération ces sections.

Configuration du routeur

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

```
radius server ISE
 address ipv4 10.127.197.105 auth-port 1812 acct-port 1813
 timeout 120
 key cisco123

aaa new-model
aaa group server radius FlexVPN_auth_server
 server name ISE

aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network a-eap-author-grp local
```

2. Configurez un point de confiance pour installer le certificat du routeur. Comme l'authentification locale du routeur est de type RSA, le périphérique nécessite que le serveur s'authentifie lui-même à l'aide d'un certificat. Vous pouvez consulter Inscription de certificat pour une ICP -1 et Inscription de certificat pour une ICP -2 pour plus de détails sur la création du certificat :

```
crypto pki trustpoint flex
 enrollment terminal
 ip-address none
```

```
 subject-name CN=flexserver.cisco.com
 revocation-check none
 rsakeypair flex1
 hash sha256
```

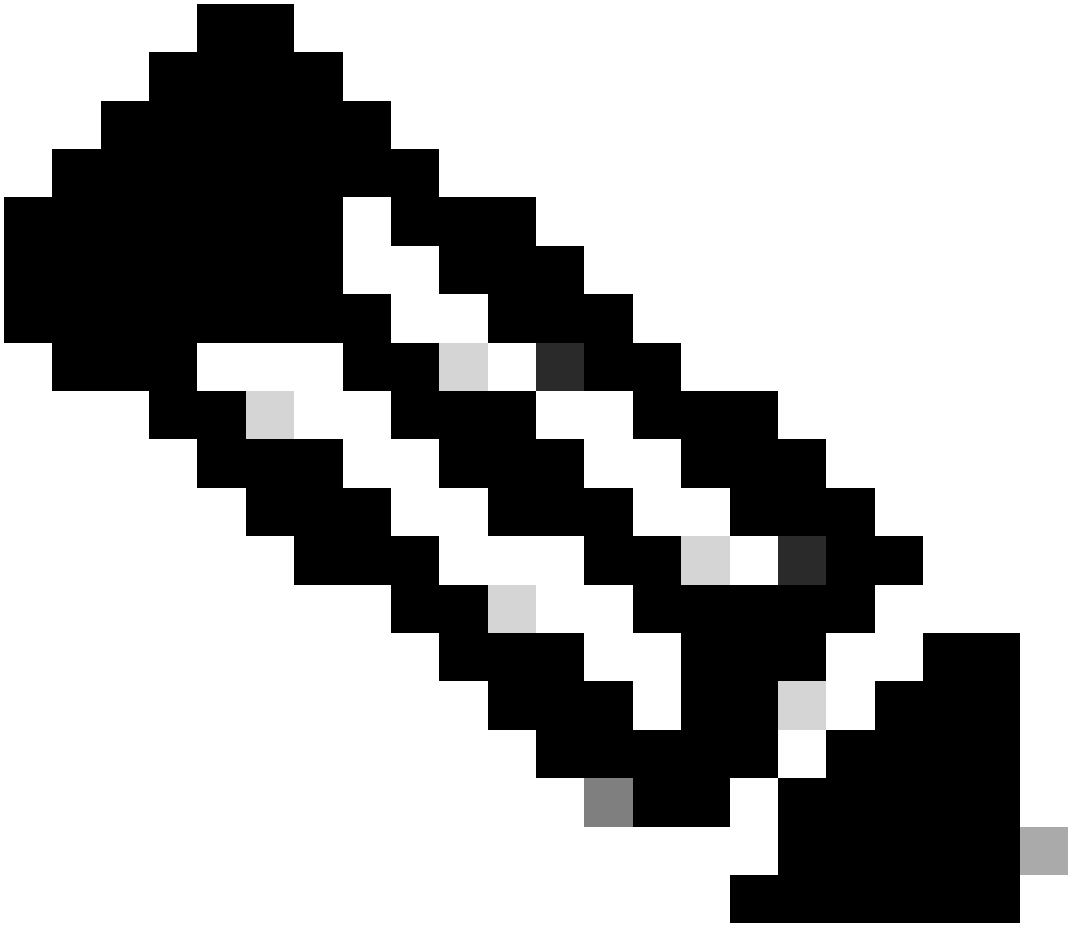
3. Définissez un pool local IP pour attribuer des adresses aux clients VPN AnyConnect lors d'une connexion AnyConnect réussie :

```
ip local pool ACPOOL 172.16.10.5 172.16.10.30
```

4. Créez une stratégie d'autorisation locale IKEv2 :

Les attributs définis dans cette politique ainsi que les attributs envoyés depuis le serveur Radius sont appliqués aux utilisateurs

```
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 dns 8.8.8.8
```



Remarque : Si la stratégie d'autorisation IKEv2 personnalisée n'est pas configurée, la stratégie d'autorisation par défaut appelée default est utilisée pour l'autorisation. Les attributs spécifiés dans la stratégie d'autorisation IKEv2 peuvent également être transmis via le serveur RADIUS. Vous devez pousser l'attribut split-exclude à partir du serveur RADIUS.

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-prop1
 encryption aes-cbc-256
 integrity sha256
 group 19

crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop1
```

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
```

7. Configurez une interface de bouclage avec une adresse IP factice. Les interfaces d'accès virtuel lui empruntent l'adresse IP :

```
interface Loopback100
 ip address 10.0.0.1 255.255.255.255
```

8. Configurez un modèle virtuel à partir duquel les interfaces d'accès virtuel sont clonées :

```
interface Virtual-Template100 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
```

9. Téléchargez le profil client AnyConnect sur le bootflash du routeur et définissez le profil comme indiqué :

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

10. Configurez un profil IKEv2 contenant toutes les informations relatives à la connexion :

```
crypto ikev2 profile prof1
 match identity remote key-id *$AnyConnectClient$*
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint flex
 aaa authentication eap FlexVPN_auth
 aaa authorization group eap list a-eap-author-grp ikev2-auth-policy
 aaa authorization user eap cached
 virtual-template 100
 anyconnect profile acvpn
```

Ils sont utilisés dans le profil IKEv2 :

- match identity remote key-id *$AnyConnectClient$* : fait référence à l'identité du client. AnyConnect utilise *$AnyConnectClient$* comme identité IKE par défaut de type key-id. Toutefois, cette identité peut être modifiée manuellement dans le profil AnyConnect pour correspondre aux besoins de déploiement.
- authentication remote - Mentionne que le protocole EAP doit être utilisé pour l'authentification du client.
- authentication local - Mentionne que les certificats doivent être utilisés pour l'authentification locale.
- aaa authentication eap - Lors de l'authentification EAP, le serveur RADIUS FlexVPN_auth est utilisé.
- aaa authorization group eap list - Pendant l'autorisation, la liste réseau a-eap-author-grp utilisée avec la stratégie d'autorisation ikev2-auth-policy.
- aaa authorization user eap cached - Active l'autorisation utilisateur implicite.
- virtual-template 100 : définit le modèle virtuel à cloner.
- anyconnect profile acvpn - Le profil client défini à l'étape 9. est appliqué ici à ce profil IKEv2.

11. Configurez le profil IPsec :

```
crypto ipsec profile AnyConnect-EAP
 set transform-set TS
 set ikev2-profile prof1
```

12. Ajoutez le profil IPsec au modèle virtuel :

```
interface Virtual-Template100 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

13. 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
```

14. Configurez la stratégie SSL et spécifiez l’adresse IP WAN du routeur comme adresse locale pour le téléchargement du profil :

```
crypto ssl policy ssl-server
 pki trustpoint flex sign
 ip address local 10.106.67.33 port 443
```

```
crypto ssl profile ssl_prof
 match policy ssl-server
```

Extrait du profil client AnyConnect (profil XML) :

Avant Cisco IOS XE 16.9.1, les téléchargements automatiques de profils à partir de la tête de réseau n'étaient pas disponibles. Après 16.9.1, il est possible de télécharger le profil à partir de la tête de réseau.

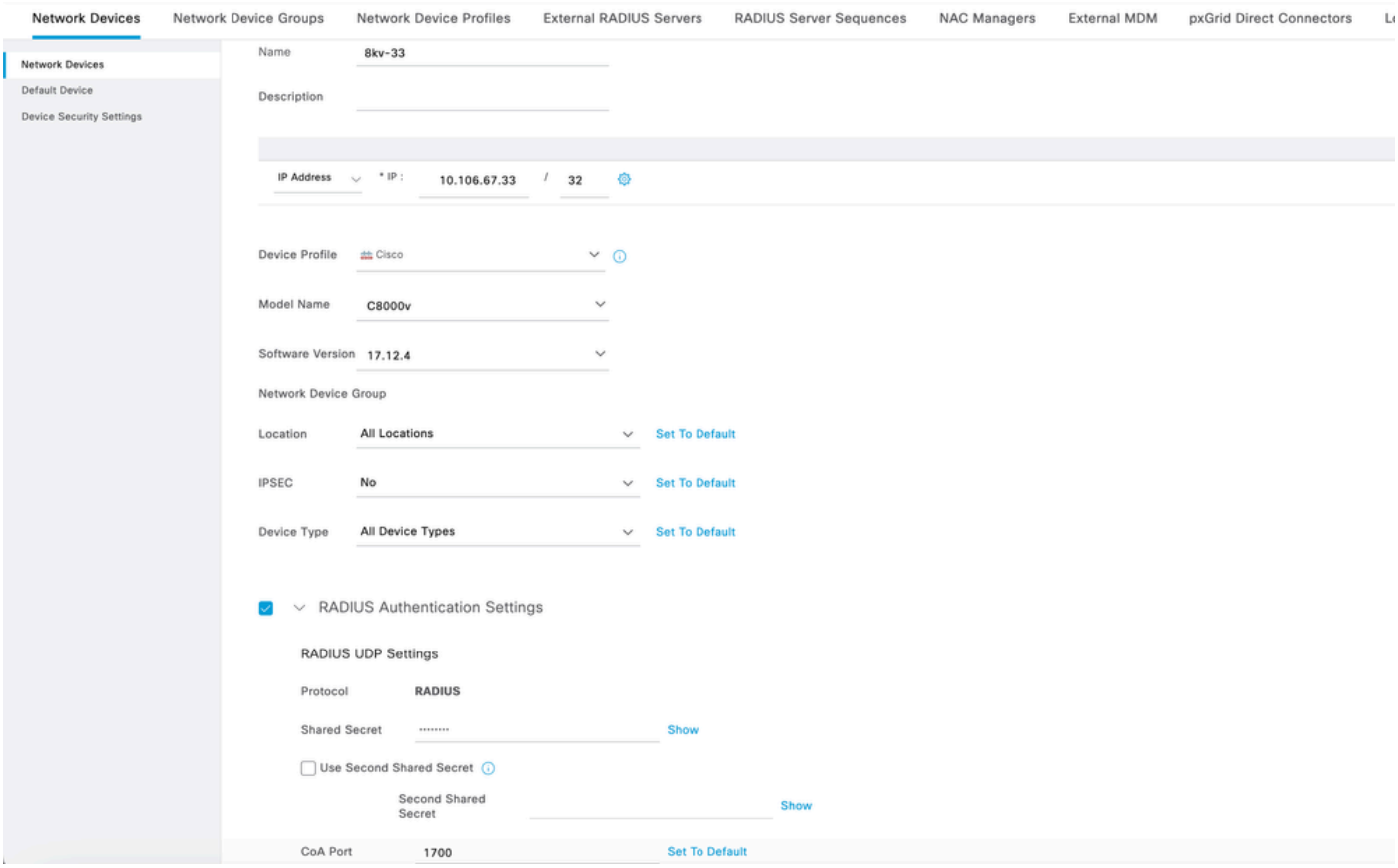
<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>

<HostName>

Flex

</HostName>
<HostAddress>
```

```
flexserver.cisco.com

</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>

EAP-MD5

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

Configuration d'Identity Services Engine (ISE)

1. Enregistrez le routeur comme périphérique réseau valide sur ISE et configurez la clé secrète partagée pour RADIUS. Pour cela, accédez à Administration > Network Resources > Network Devices. Cliquez sur Add pour configurer le routeur en tant que client AAA :

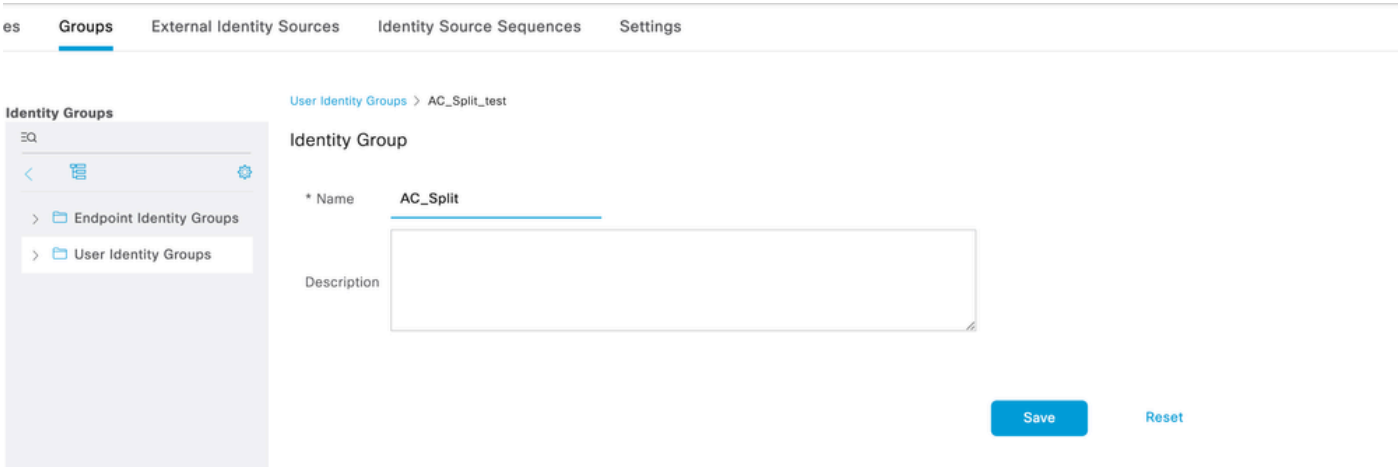


Ajouter un périphérique réseau

2. Créez des groupes d'identité :

Définissez des groupes d'identité pour associer des utilisateurs ayant des caractéristiques similaires et qui partagent des autorisations similaires. Elles sont utilisées dans les étapes suivantes. Accédez à Administration > Identity Management > Groups > User Identity Groups,

puis cliquez sur Add:



Créer un groupe d'identités

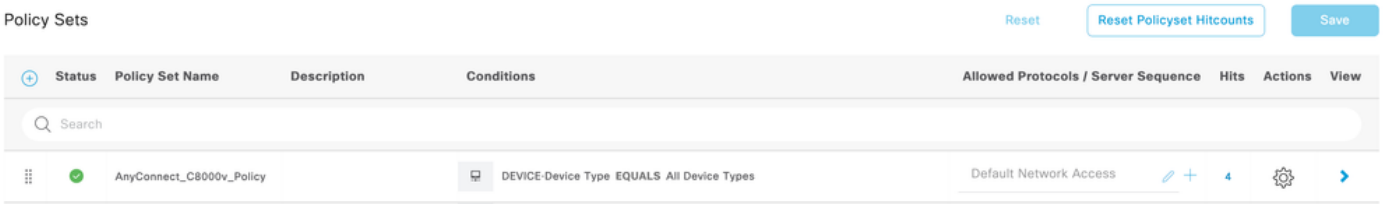
3. Associez des utilisateurs à des groupes d'identité :

Associez les utilisateurs au groupe d'identité approprié. Accédez à Administration > Identity Management > Identities > Users.

Ajouter un utilisateur au groupe d'identités

4. Créer un ensemble de stratégies :

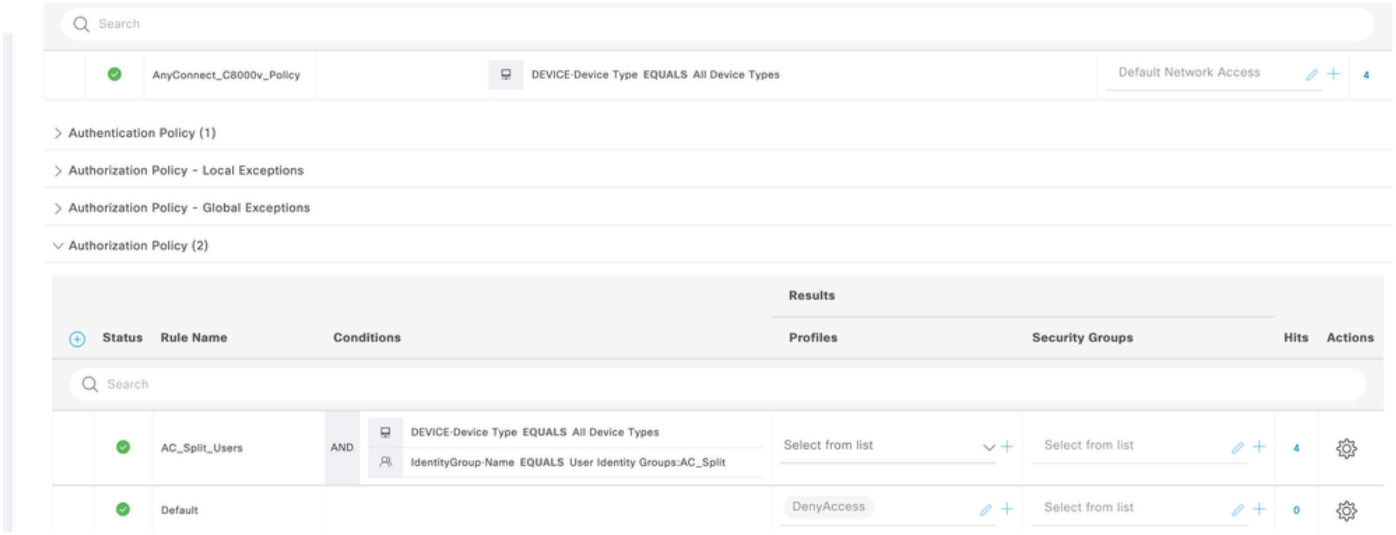
Définissez un nouvel ensemble de stratégies et définissez les conditions qui correspondent à la stratégie. Dans cet exemple, tous les types de périphériques sont autorisés dans ces conditions. Pour ce faire, accédez à Policy>Policy sets :



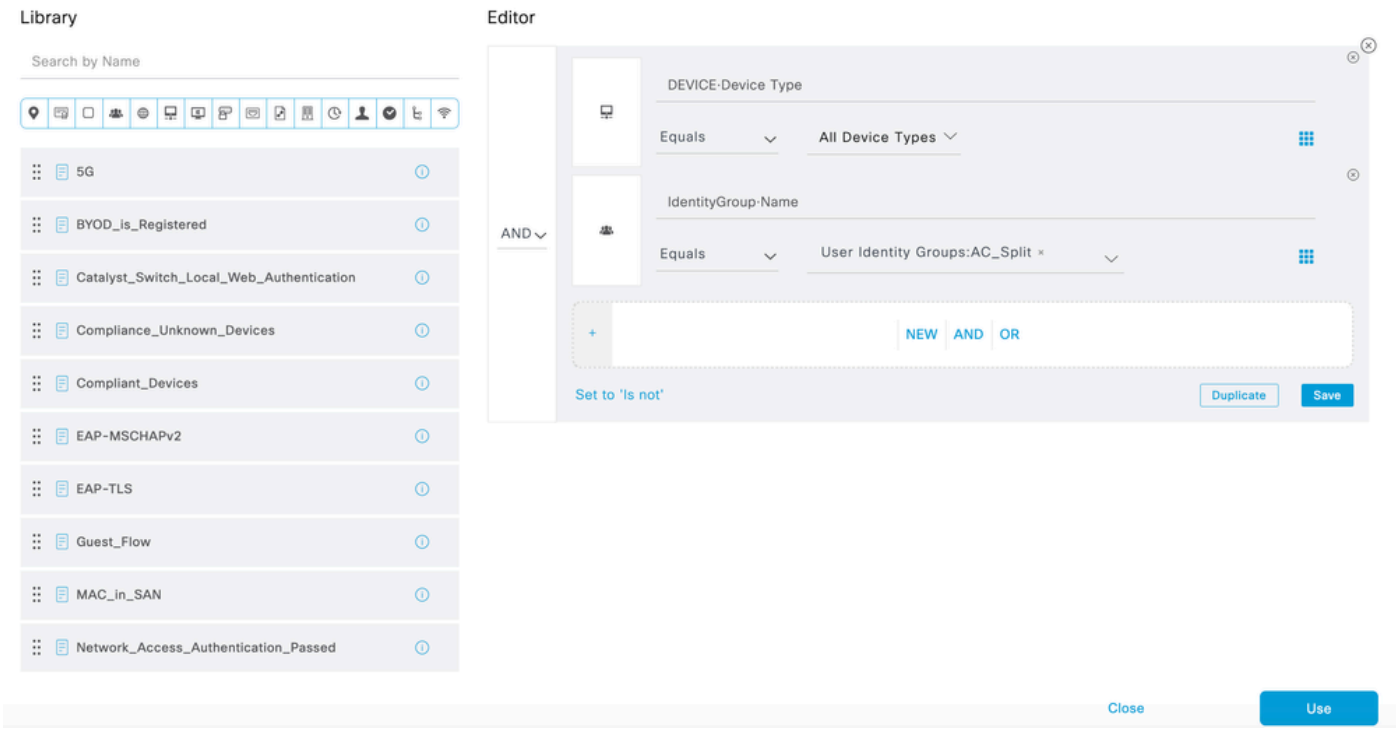
Créer un ensemble de stratégies

5. Créez une stratégie d'autorisation :

Définissez une nouvelle stratégie d'autorisation avec les conditions requises pour correspondre à la stratégie. Veillez à inclure comme condition les groupes d'identité créés à l'étape 2.



Créer une stratégie d'autorisation

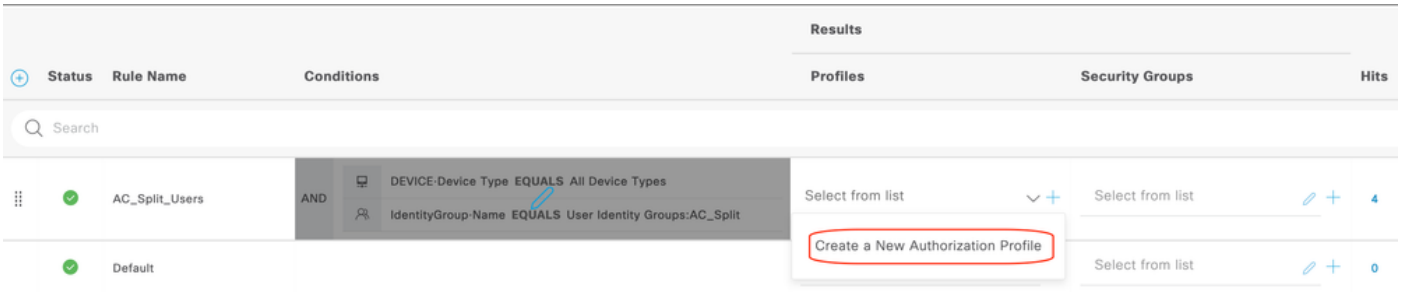


Choisir des conditions dans la stratégie d'autorisation

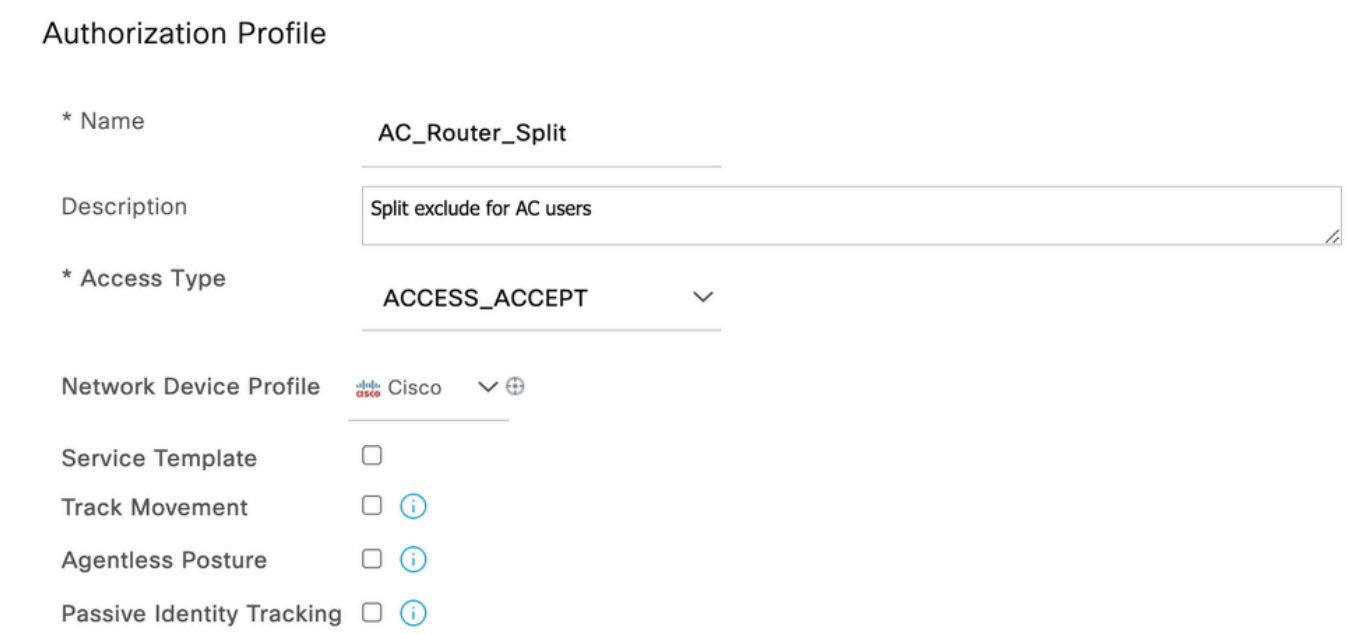
6. Créer un profil d'autorisation :

Le profil d'autorisation inclut les actions qui sont entreprises lorsque la stratégie d'autorisation est mise en correspondance. Créez un nouveau profil d'autorisation qui inclut les attributs suivants :

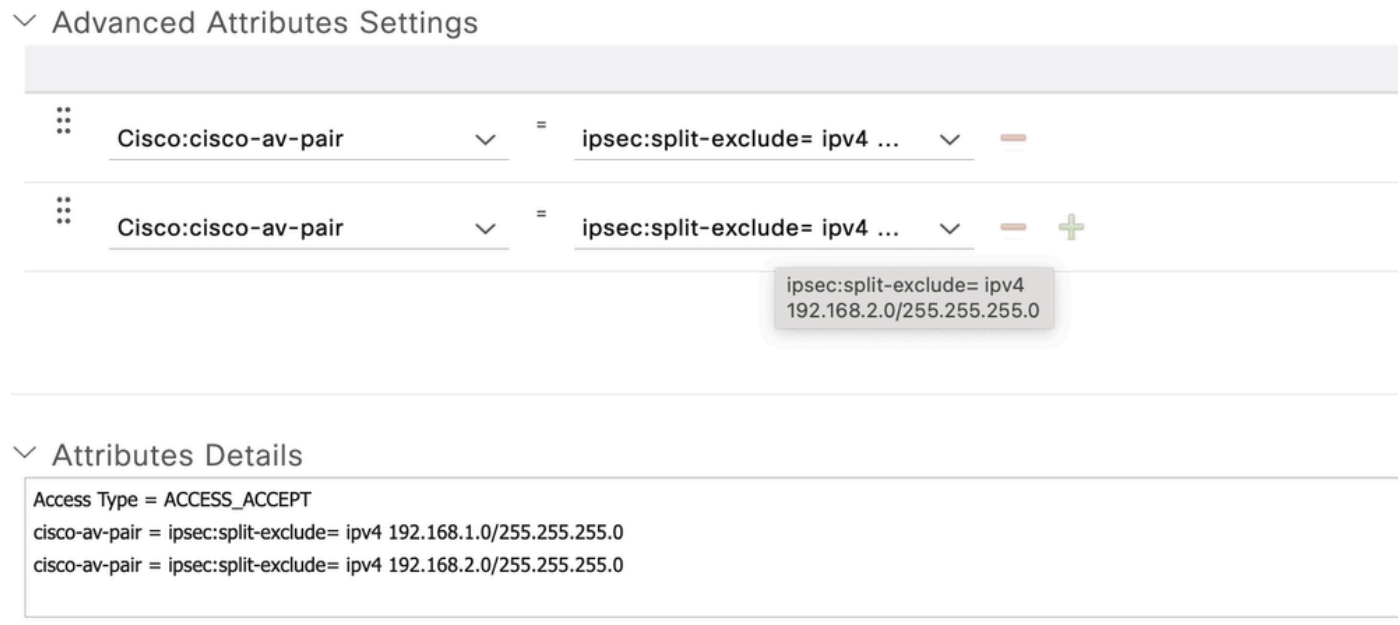
Type d'accès = ACCESS_ACCEPT
cisco-av-pair = ipsec : split-exclude= ipv4 <réseau_ip>/<masque_sous-réseau>



Créer un nouveau profil d'autorisation

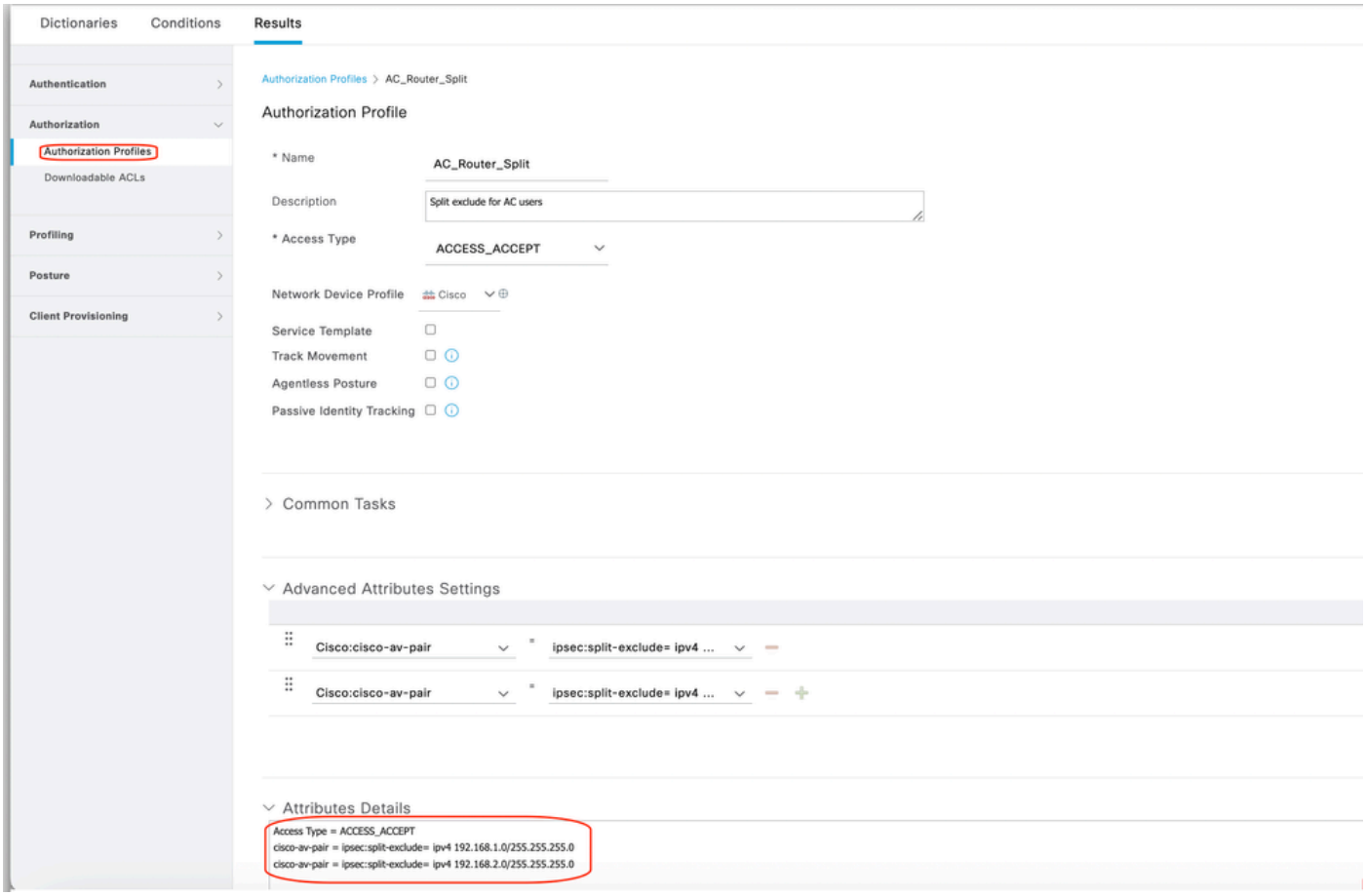


Configuration du profil d'autorisation



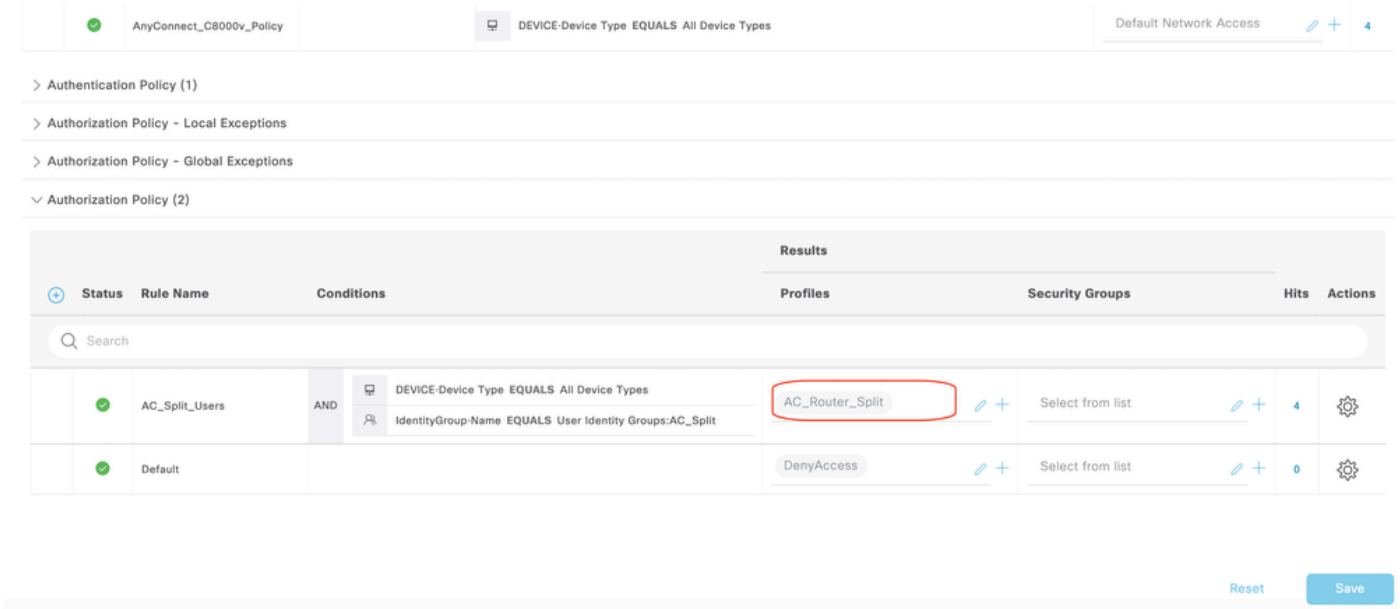
Configurer les attributs dans le profil d'autorisation

7. Vérifiez la configuration du profil d'autorisation.



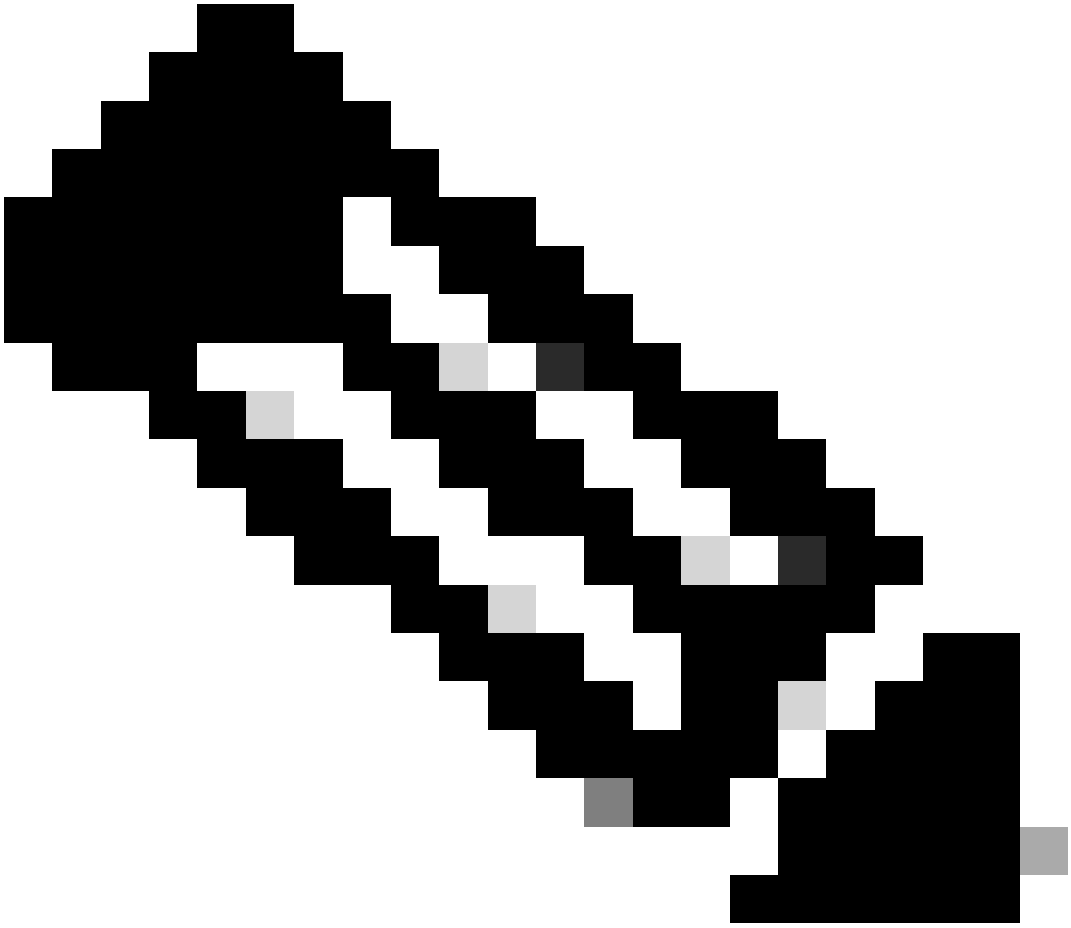
Révision de la configuration du profil d'autorisation

8. Il s'agit de la stratégie d'autorisation dans la configuration du jeu de stratégies après avoir sélectionné les profils requis :



Config. stratégie d'autorisation finale

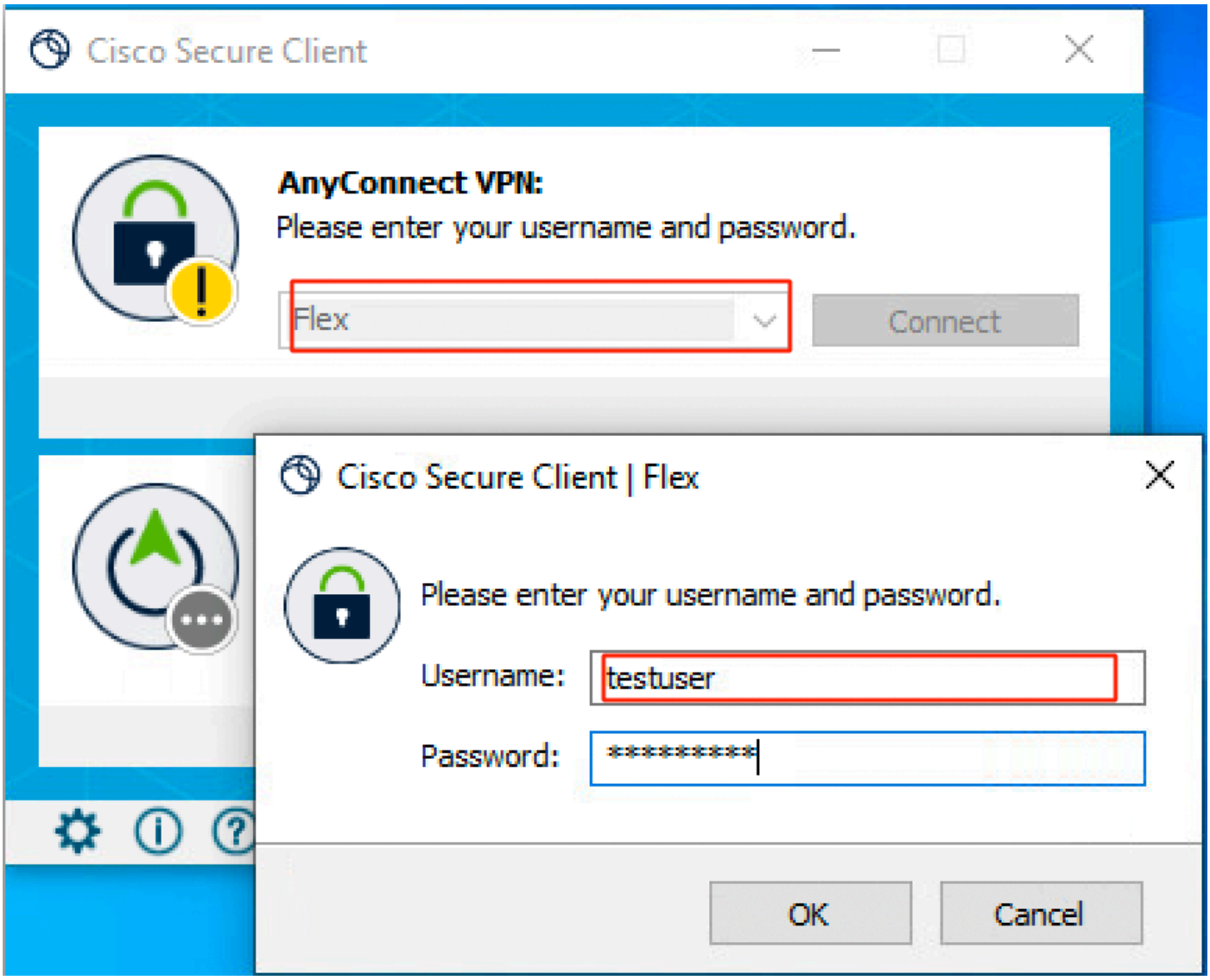
Avec cet exemple de configuration, vous pouvez exclure des réseaux de passer par le VPN via la configuration ISE en fonction du groupe d'identité auquel l'utilisateur appartient.



Remarque : Un seul sous-réseau à exclusion fractionnée peut être envoyé au PC client lors de l'utilisation de la tête de réseau Cisco IOS XE pour une connexion VPN d'annonce de routeur. Ceci a été résolu par l'ID de bogue Cisco CSCwj38106 et plusieurs sous-réseaux à exclusion fractionnée peuvent être envoyés depuis 17.12.4. Référez-vous au bogue pour plus de détails sur les versions corrigées.

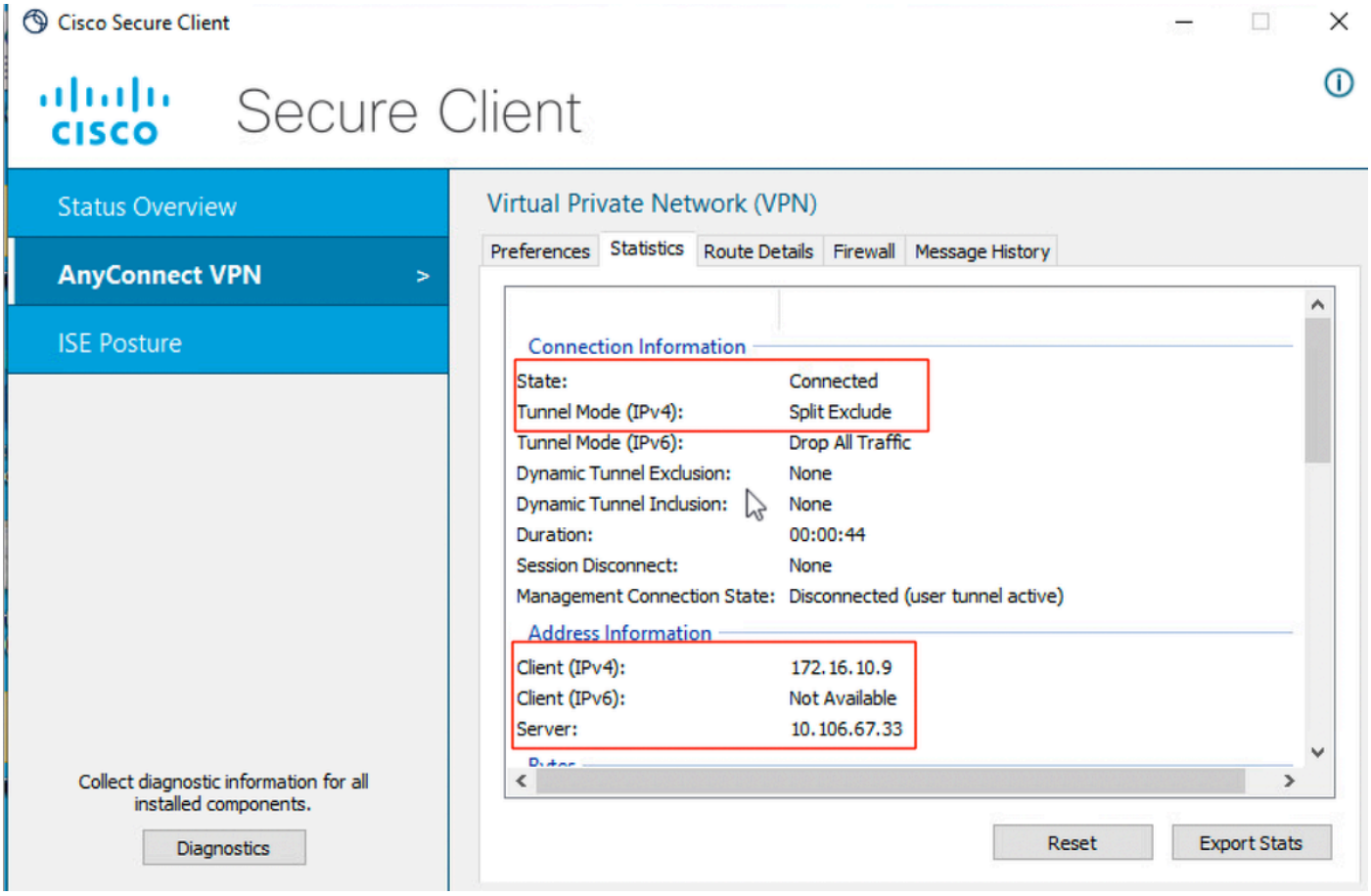
Vérifier

1. Afin de tester l'authentification, connectez-vous au C8000V à partir du PC de l'utilisateur via AnyConnect et entrez les informations d'identification.



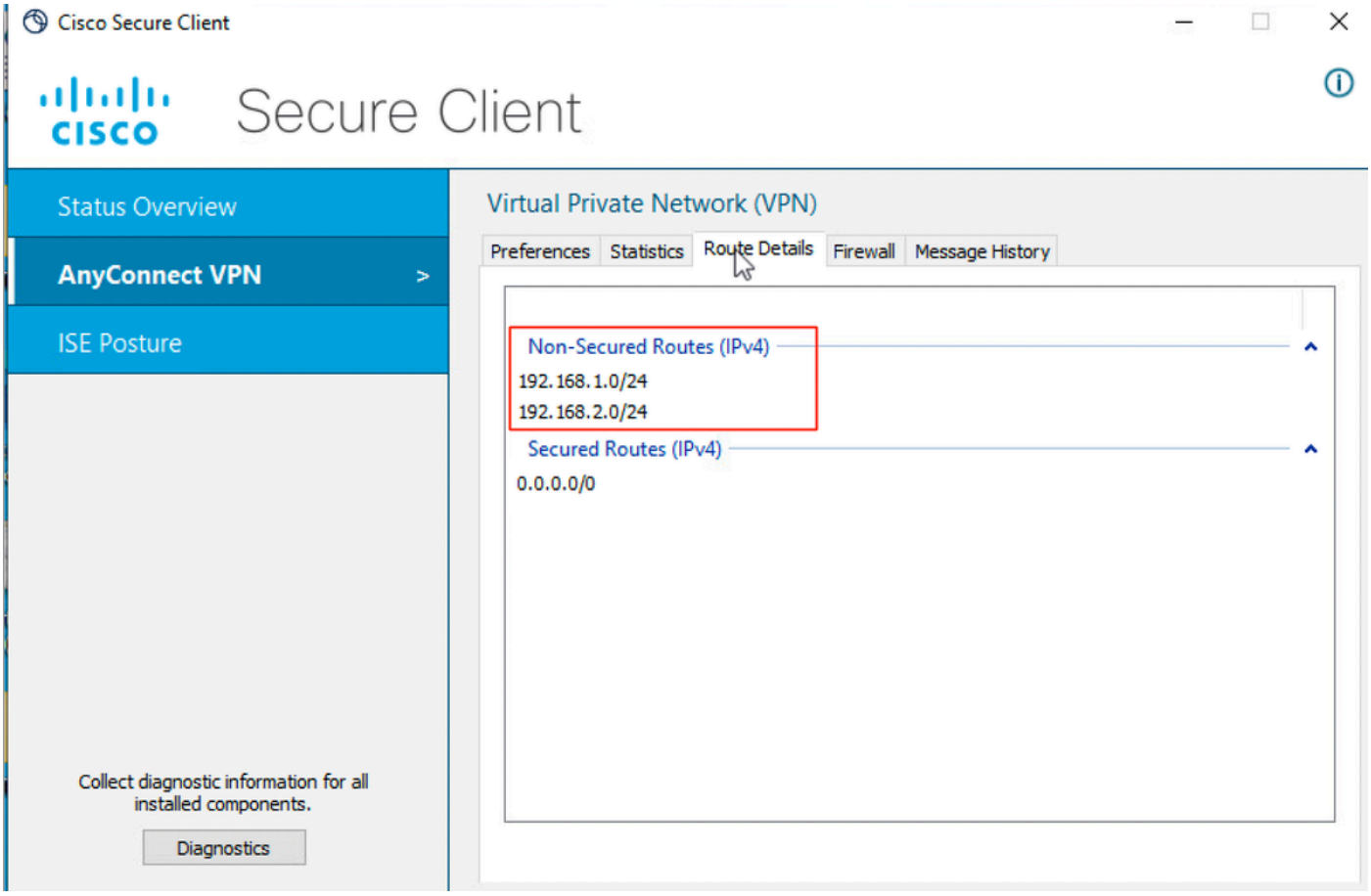
Se connecter à AnyConnect

2. Une fois la connexion établie, cliquez sur l'icône du rapport (coin inférieur gauche) et accédez à AnyConnect VPN > Statistics. Confirmez que le mode tunnel doit être Split Exclude.



Valider les statistiques

Accédez à AnyConnect VPN > Route details et vérifiez que les informations affichées correspondent aux routes sécurisées et non sécurisées.



Valider les détails de la route

Vous pouvez également vérifier les détails de connexion sur la tête de réseau VPN :

1. IKEv2 parameters

<#root>

8kv#

show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status

1 10.106.67.33/4500 10.106.50.91/55811 none/none READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA, Auth verify: EAP

Life/Active Time: 86400/22 sec

CE id: 1012, Session-id: 6

Local spi: E8C6C5EEF0F0EF72 Remote spi: 7827644A7CA8F1A5

Status Description: Negotiation done

Local id: 10.106.67.33

Remote id: *$AnyConnectClient$*

Remote EAP id: testuser

Local req msg id: 0 Remote req msg id: 6

Local next msg id: 0 Remote next msg id: 6

Local req queued: 0 Remote req queued: 6

Local window: 5 Remote window: 1

DPD configured for 0 seconds, retry 0

Fragmentation not configured.

Dynamic Route Update: disabled

Extended Authentication configured.

NAT-T is detected outside

Cisco Trust Security SGT is disabled

Assigned host addr: 172.16.10.10

Initiator of SA : No

Post NATed Address : 10.106.67.33

PEER TYPE: Other

IPv6 Crypto IKEv2 SA

2.This is the crypto session detail for the VPN session:

<#root>

8kv#

show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

X - IKE Extended Authentication, F - IKE Fragmentation

R - IKE Auto Reconnect, U - IKE Dynamic Route Update

S - SIP VPN

Interface: Virtual-Access1

Profile: prof1

Uptime: 00:00:44

Session status: UP-ACTIVE

Peer: 10.106.50.91 port 55811 fvrf: (none) ivrf: (none)

```
Phase1_id: *$AnyConnectClient$*

Desc: (none)

Session ID: 16

IKEv2 SA: local 10.106.67.33/4500 remote 10.106.50.91/55811 Active

Capabilities:NX connid:1 lifetime:23:59:16

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 172.16.10.10

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 114 drop 0 life (KB/Sec) 4607987/3556

Outbound: #pkts enc'ed 96 drop 0 life (KB/Sec) 4608000/3556
```

3. Verify on ISE live logs.

Dépannage

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 condition peer ipv4 <public_ip>
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 :

Utilisez les journaux RADIUS en direct en naviguant jusqu'à Operations > Live logs.

Scénario de travail

Voici le débogage de la connexion réussie :

<#root>

```
*Oct 13 10:01:25.928: RADIUS/ENCODE(0000012D):Orig. component type = VPN IPSEC
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): dropping service type, "radius-server attribute 6 on-for
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IP: 0.0.0.0
*Oct 13 10:01:25.929: vrfid: [65535] ipv6 tableid : [0]
*Oct 13 10:01:25.929: idb is NULL
*Oct 13 10:01:25.929: RADIUS(0000012D): Config NAS IPv6: ::
*Oct 13 10:01:25.929: RADIUS/ENCODE(0000012D): acct_session_id: 4291
*Oct 13 10:01:25.929: RADIUS(0000012D): sending
*Oct 13 10:01:25.929: RADIUS/ENCODE: Best Local IP-Address 10.106.67.33 for Radius-Server 10.127.197.10
*Oct 13 10:01:25.929: RADIUS: Message Authenticator encoded
*Oct 13 10:01:25.929: RADIUS(0000012D): Send Access-Request to 10.127.197.105:1812 id 1645/24, len 344
RADIUS: authenticator 85 AC BF 77 BF 42 0B C7 - DE 85 A3 9A AF 40 E5 DC
*Oct 13 10:01:25.929: RADIUS: Service-Type [6] 6 Login [1]
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 26
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 45
```

***Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 39 "isakmp-phase1-id=*$AnyConnectClient$*"**

```
*Oct 13 10:01:25.929: RADIUS: Calling-Station-Id [31] 14 "10.106.50.91"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 64
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L40A6A4321ZO2L40A6A325BZH1194CC58
*Oct 13 10:01:25.929: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.929: RADIUS: Vendor, Cisco [26] 21
*Oct 13 10:01:25.929: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
*Oct 13 10:01:25.929: RADIUS: EAP-Message [79] 24
RADIUS: 02 8E 00 16 04 10 8A 09 BB 0D 4B A9 D6 2B 59 1C C8 FE 1C 90 56 F5 [ K+YV]
*Oct 13 10:01:25.929: RADIUS: Message-Authenticato[80] 18
RADIUS: 54 85 1B AC BE A8 DA EF 24 AE 4D 28 46 32 8C 48 [ T$M(F2H]
*Oct 13 10:01:25.929: RADIUS: State [24] 90
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 30 41 36 41 34 33 32 31 5A 4F 32 4C 34 [2L40A6A4321ZO2L4]
RADIUS: 30 41 36 41 33 32 35 42 5A 48 31 31 39 34 43 43 [0A6A325BZH1194CC]
RADIUS: 35 38 5A 4E 31 32 3B 33 30 53 65 73 73 69 6F 6E [58ZN12;30Session]
RADIUS: 49 44 3D 69 73 65 2D 70 73 6E 2F 35 31 37 31 33 [ID=ise-psn/51713]
RADIUS: 35 39 30 30 2F 33 38 3B [ 5900/38;]
*Oct 13 10:01:25.929: RADIUS: NAS-IP-Address [4] 6 10.106.67.33
*Oct 13 10:01:25.929: RADIUS(0000012D): Sending a IPv4 Radius Packet
*Oct 13 10:01:25.929: RADIUS(0000012D): Started 120 sec timeout
```

***Oct 13 10:01:25.998: RADIUS: Received from id 1645/24 10.127.197.105:1812, Access-Accept, len 239**

```
RADIUS: authenticator BC 19 F2 EE 10 67 80 C5 - 9F D9 30 9A EA 7E 5E D3
*Oct 13 10:01:25.998: RADIUS: User-Name [1] 10 "testuser"
*Oct 13 10:01:25.998: RADIUS: Class [25] 67
RADIUS: 43 41 43 53 3A 4C 32 4C 34 30 41 36 41 34 33 32 [CACS:L2L40A6A432]
RADIUS: 31 5A 4F 32 4C 34 30 41 36 41 33 32 35 42 5A 48 [1ZO2L40A6A325BZH]
RADIUS: 31 31 39 34 43 43 35 38 5A 4E 31 32 3A 69 73 65 [1194CC58ZN12:ise]
RADIUS: 2D 70 73 6E 2F 35 31 37 31 33 35 39 30 30 2F 33 [-psn/517135900/3]
RADIUS: 38 [ 8]
*Oct 13 10:01:25.998: RADIUS: EAP-Message [79] 6
RADIUS: 03 8E 00 04
*Oct 13 10:01:25.998: RADIUS: Message-Authenticato[80] 18
RADIUS: F9 61 C1 FD 6D 26 31 A2 89 04 72 BC DD 32 A9 29 [ am&1r2)]
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
```

`*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0"`

```
*Oct 13 10:01:25.998: RADIUS: Vendor, Cisco [26] 59
```

`*Oct 13 10:01:25.998: RADIUS: Cisco AVpair [1] 53 "ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0"`

```
*Oct 13 10:01:25.998: RADIUS(0000012D): Received from id 1645/24
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
8kv#
```

Références

- Configurer la tête de réseau FlexVPN pour l'accès à distance IKEv2 à l'aide de la base de données utilisateur locale
- Configurer AnyConnect Flexvpn avec authentification EAP et DUO
- Configuration de l'accès à distance AnyConnect IKEv2 avec EAP-MD5

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.