ISEを使用したAnyConnect FlexVPNのスプリット除外の設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[設定](#)

- [ネットワーク図](#)
- [コンフィギュレーション](#)
  - [ルータの設定](#)
  - [Identity Services Engine（ISE）の設定](#)

[確認](#)

[トラブルシュート](#)

[参考資料](#)

はじめに

このドキュメントでは、Cisco IOS® XEルータへのIKEv2 AnyConnect接続にISEを使用してスプリット除外を設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ルータでのAnyConnect IPSec設定の経験
- Cisco Identity Services Engine(ISE)の設定
- Cisco Secure Client(CSC)
- RADIUS プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

ネットワーク図

コンフィギュレーション

設定を完了するには、次のセクションを考慮してください。

ルータの設定

1. デバイス上で認証およびローカル認証を行うようにRADIUSサーバを設定します。

```
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. トラストポイントを設定してルータ証明書をインストールする。ルータのローカル認証のタイプはRSAであるため、デバイスではサーバが証明書を使用して自身を認証する必要があります。証明書の作成の詳細については、「PKI -1の証明書の登録」および「PKI -2の証明書の登録」を参照してください。

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

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

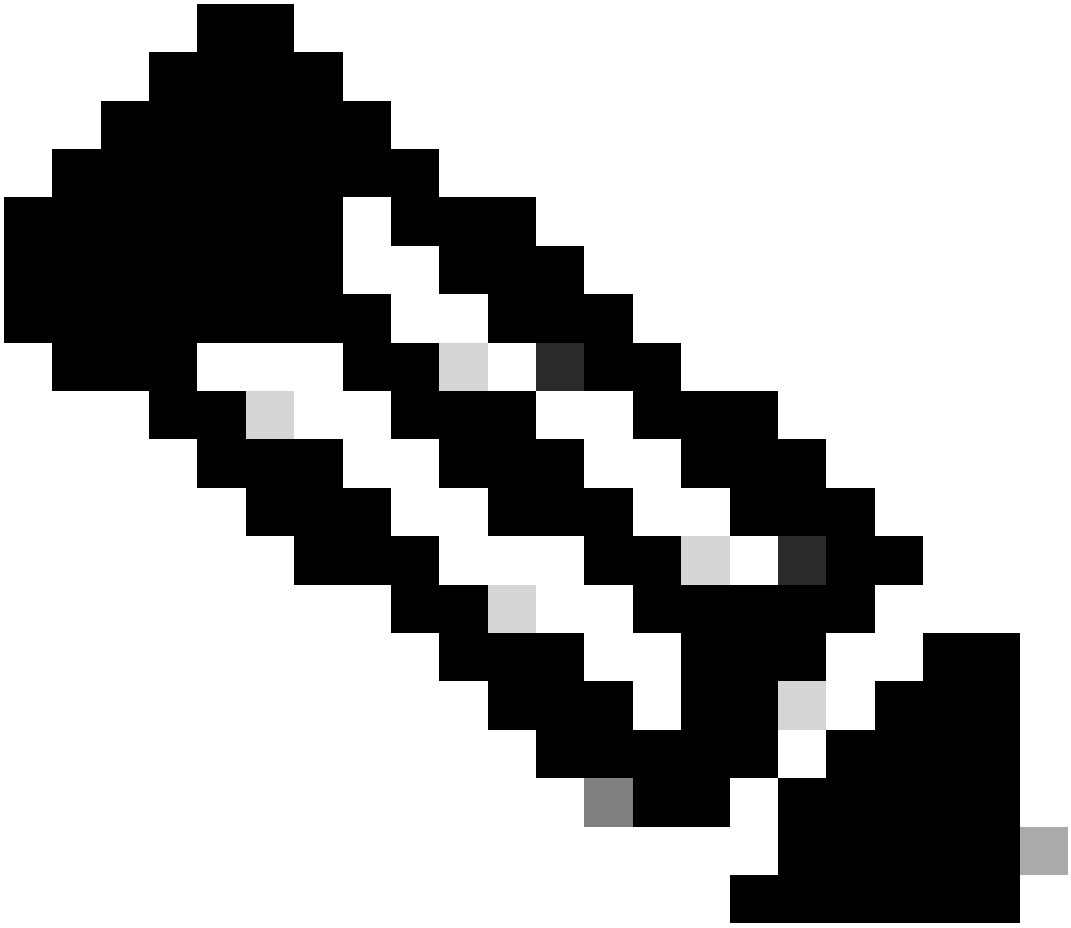
3. AnyConnect接続が成功した場合に、AnyConnect VPNクライアントにアドレスを割り当てるIPローカルプールを定義します。

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

4. IKEv2ローカル許可ポリシーを作成します。

このポリシーで定義された属性は、RADIUSサーバからプッシュされる属性と一緒にユーザに適用されます

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



注：カスタムIKEv2許可ポリシーが設定されていない場合、defaultという名前のデフォルトの許可ポリシーが許可に使用されます。IKEv2許可ポリシーで指定された属性は、RADIUSサーバ経由でプッシュすることもできます。RADIUSサーバからsplit-exclude属性をプッシュする必要があります。

5（オプション）。 IKEv2プロポーザルおよびポリシーを作成します（設定されていない場合は、スマートデフォルトが使用されます）。

```
crypto ikev2 proposal IKEv2-prop1
 encryption aes-cbc-256
 integrity sha256
 group 19

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

6（オプション）。トランスフォームセットを設定します（設定されていない場合は、スマートデフォルトが使用されます）。

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

7. ループバックインターフェイスにダミーIPアドレスを設定します。バーチャルアクセスインターフェイスは、そこからIPアドレスを借ります。

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

8. 仮想アクセスインターフェイスのクローニング元の仮想テンプレートを設定します。

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

9. AnyConnectクライアントプロファイルをルータのブートフラッシュにアップロードし、次のようにプロファイルを定義します。

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

10. すべての接続関連情報を含むIKEv2プロファイルを設定します。

```
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
```

これらはIKEv2プロファイルで使用されます。

- match identity remote key-id *$AnyConnectClient$*：クライアントのアイデンティティを参照します。 AnyConnectは*$AnyConnectClient$*をタイプkey-idのデフォルトIKE IDとして使用します。ただし、このIDは、導入のニーズに合わせてAnyConnectプロファイルで手動で変更できます。
- authentication remote：クライアント認証にEAPプロトコルを使用する必要があることを示します。
- authentication local：ローカル認証に証明書を使用する必要があることを示します。
- aaa authentication eap:EAP認証時に、RADIUSサーバFlexVPN_authが使用されます。
- aaa authorization group eap list：認証時に、認証ポリシーikev2-auth-policyとともに使用されるネットワークリストa-eap-author-grp
- aaa authorization user eap cached：暗黙的なユーザ認証を有効にします。
- virtual-template 100：クローニングするバーチャルテンプレートを定義します。
- anyconnect profile acvpn：ステップ9で定義したクライアントプロファイルが、このIKEv2プロファイルに適用されます。

11. IPsecプロファイルを設定します。

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

12. IPsecプロファイルを仮想テンプレートに追加します。

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

13. ルータでHTTP-URLベースの証明書検索およびHTTPサーバを無効にします。

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

14. SSLポリシーを設定し、プロファイルをダウンロードするためのローカルアドレスとしてルータのWAN IPを指定します。

```
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
```

AnyConnectクライアントプロファイル（XMLプロファイル）のスニペット：

Cisco IOS XE 16.9.1より前のリリースでは、ヘッドエンドからのプロファイルの自動ダウンロードは使用できません。16.9.1以降では、ヘッドエンドからプロファイルをダウンロードできます。

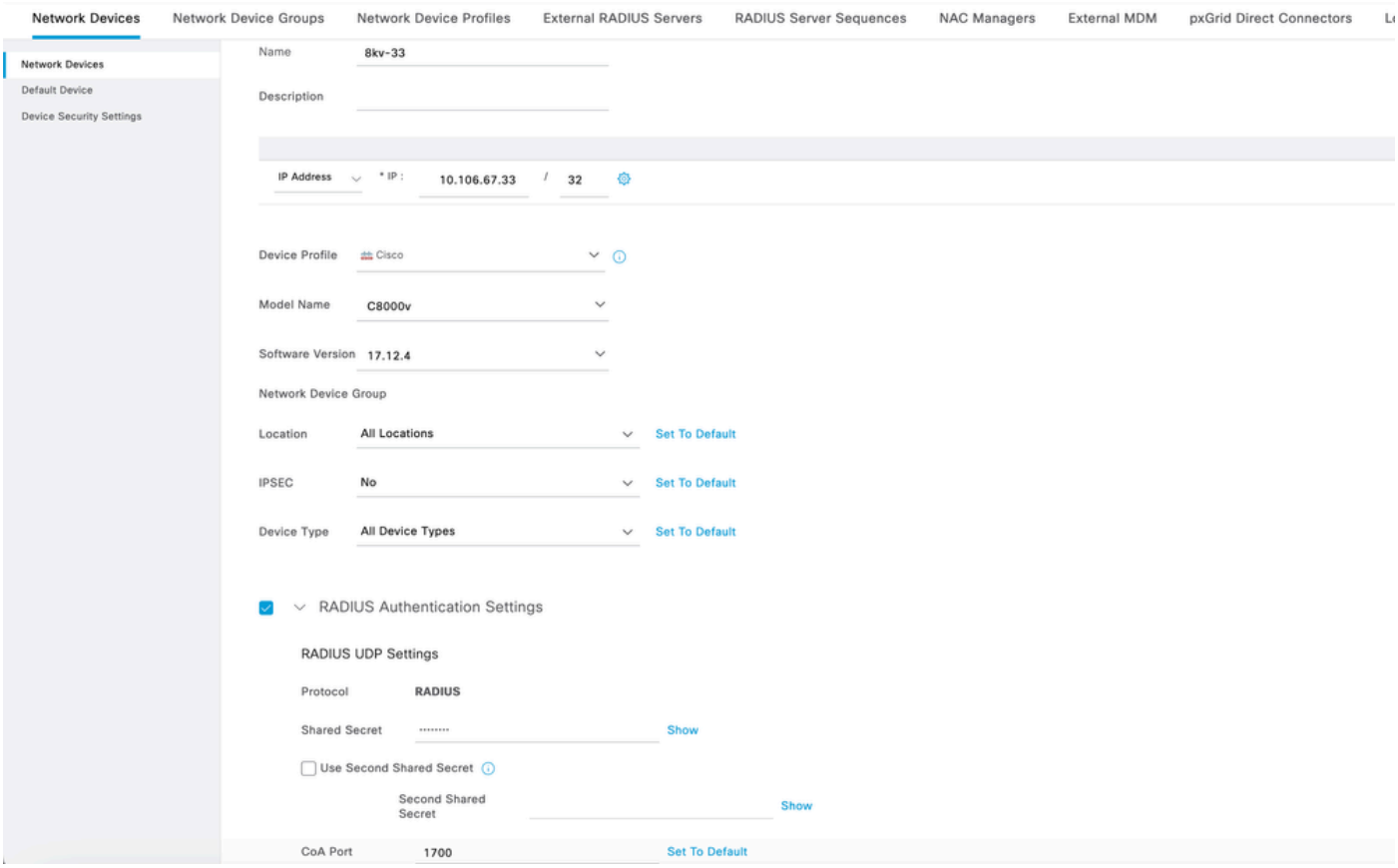
<#root>

```
<?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>
```

Identity Services Engine（ISE）の設定

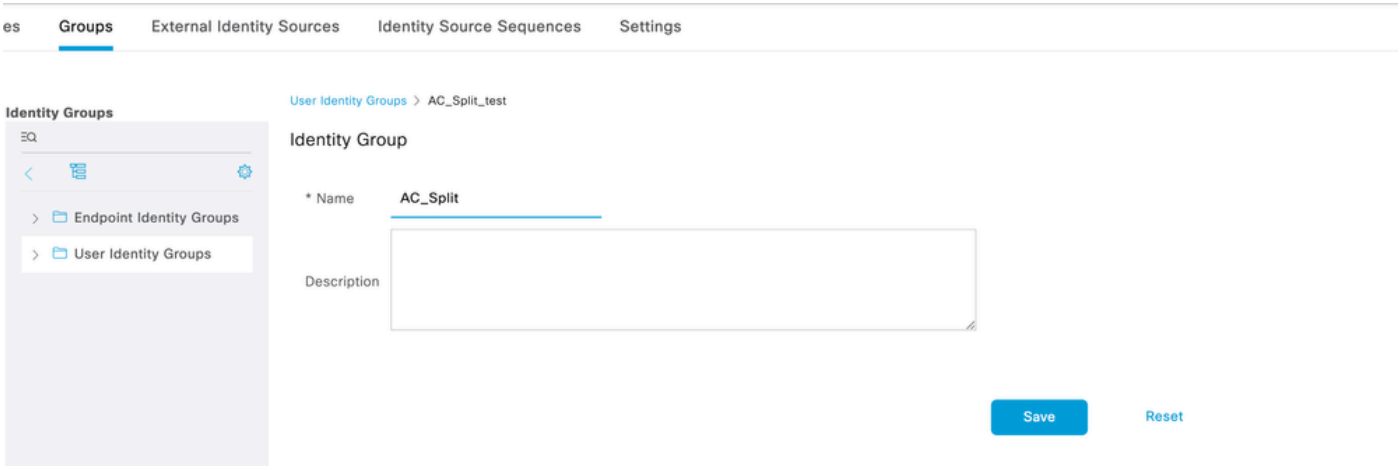
1. ルータをISE上の有効なネットワークデバイスとして登録し、RADIUSの共有秘密キーを設定します。このためには、Administration > Network Resources > Network Devicesの順に選択します。 Addをクリックして、ルータをAAAクライアントとして設定します。



ネットワーク デバイスの追加

2. アイデンティティグループを作成します。

IDグループを定義して、同様の特性を持つユーザと同様の権限を共有するユーザを関連付けます。これらは次の手順で使用します。Administration > Identity Management > Groups > User Identity Groupsの順に移動し、Addをクリックします。



IDグループの作成

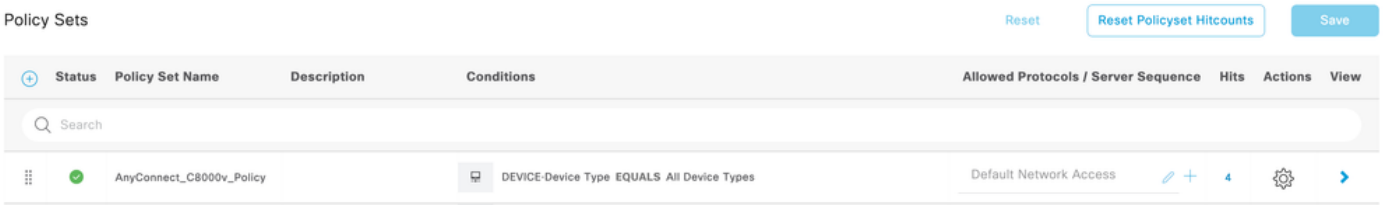
3. ユーザーをIDグループに関連付けます。

ユーザを適切なIDグループに関連付けます。[Administration] > [Identity Management] > [Identities] > [Users] の順に移動します。

IDグループへのユーザの追加

4. ポリシーセットを作成します。

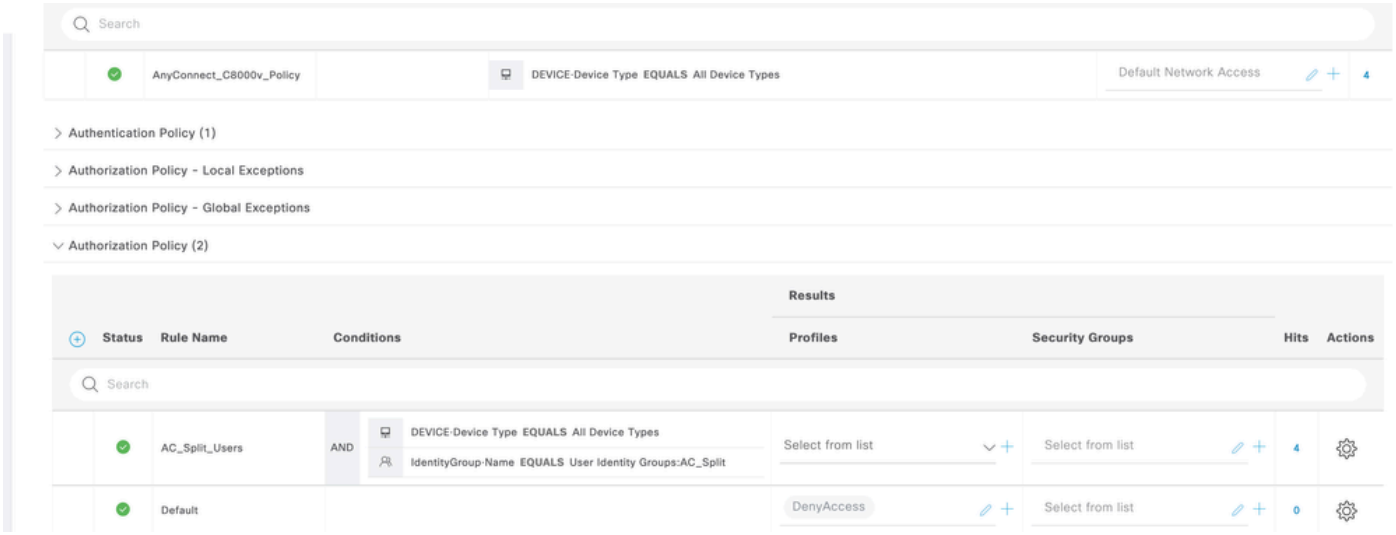
新しいポリシーセットを定義し、ポリシーに一致する条件を定義します。この例では、条件の下ですべてのデバイスタイプが許可されます。これを行うには、Policy>Policy setsの順に移動します。



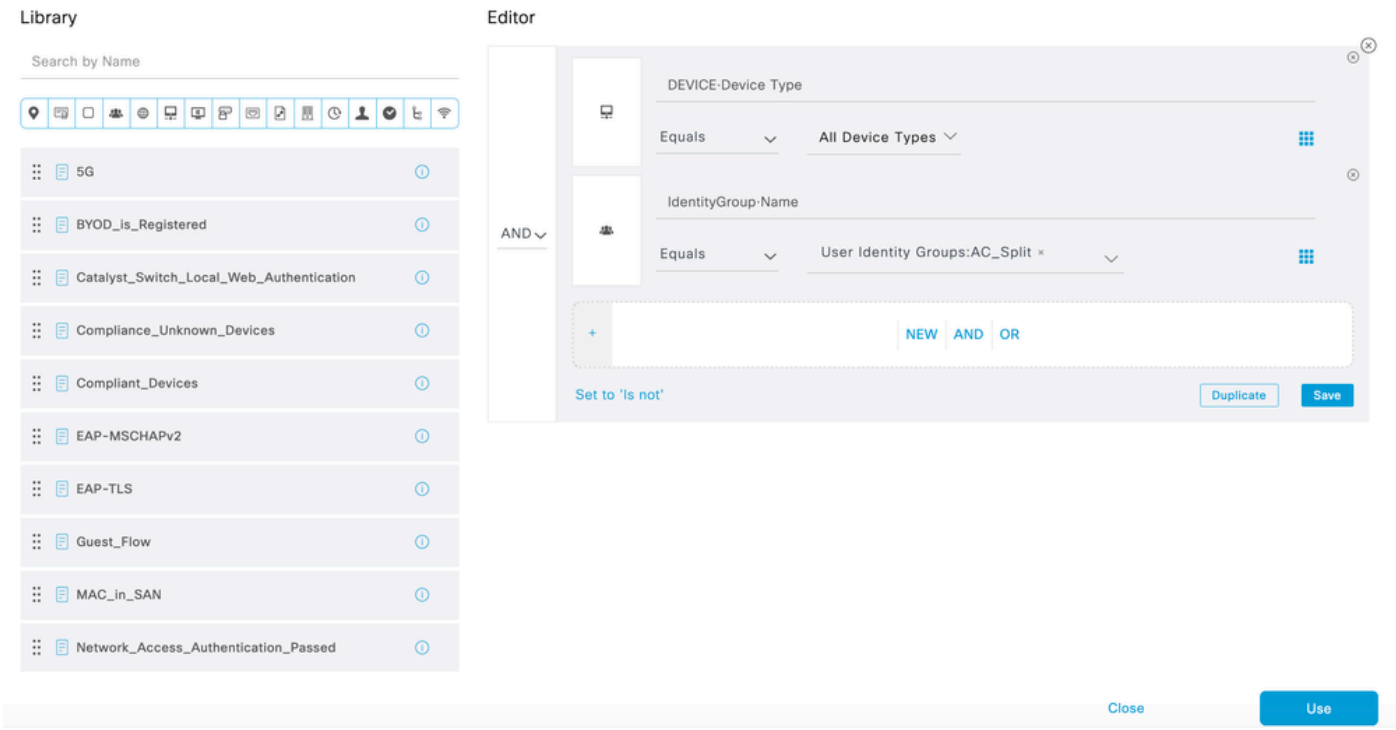
ポリシーセットの作成

5. 許可ポリシーを作成します。

ポリシーに一致するために必要な条件を使用して、新しい認可ポリシーを定義します。ステップ2で作成したIDグループを条件として含めてください。



認証ポリシーの作成

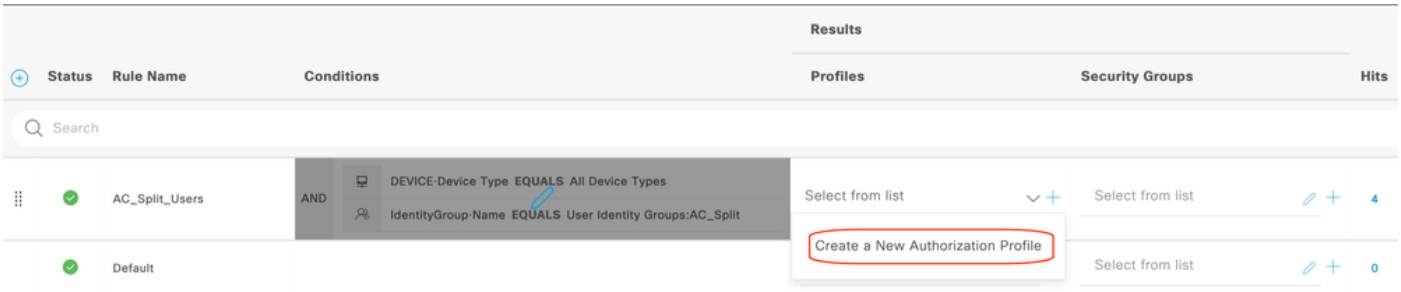


認可ポリシーの条件の選択

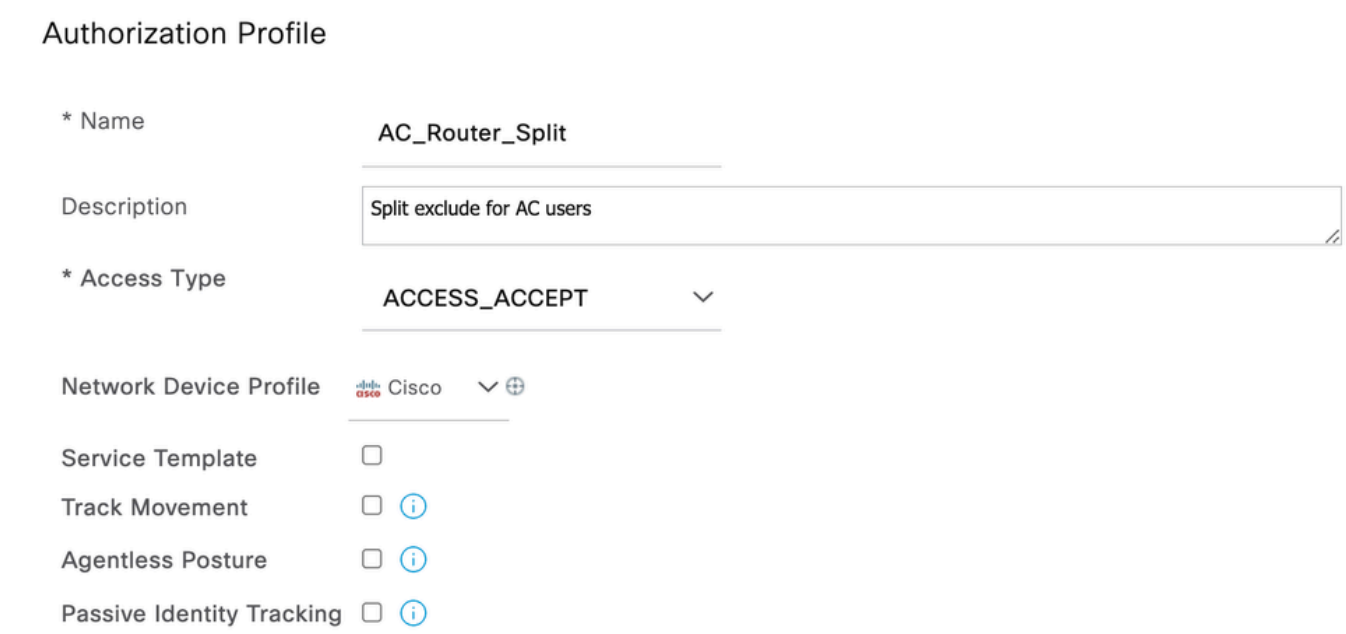
6. 許可プロファイルを作成します。

認可プロファイルには、認可ポリシーが一致した場合に実行されるアクションが含まれます。次の属性を含む新しい認可プロファイルを作成します。

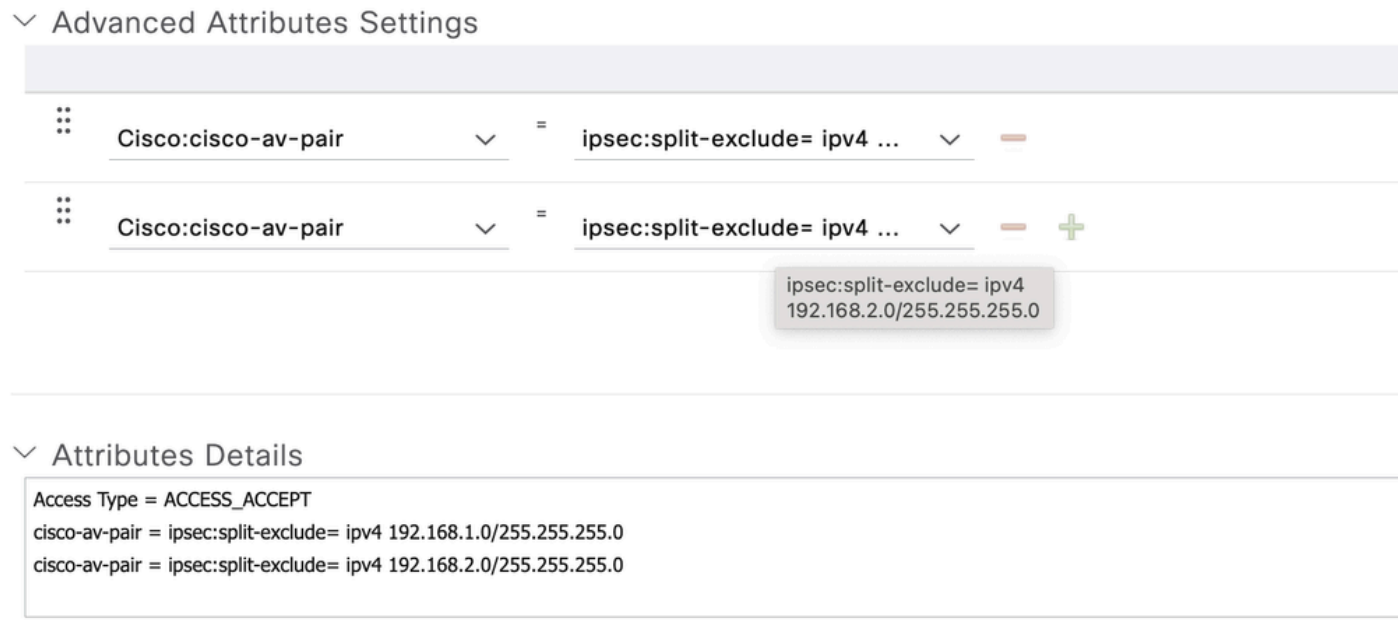
Access Type = ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <ip_network>/<subnet_mask>



新しい認可プロファイルの作成

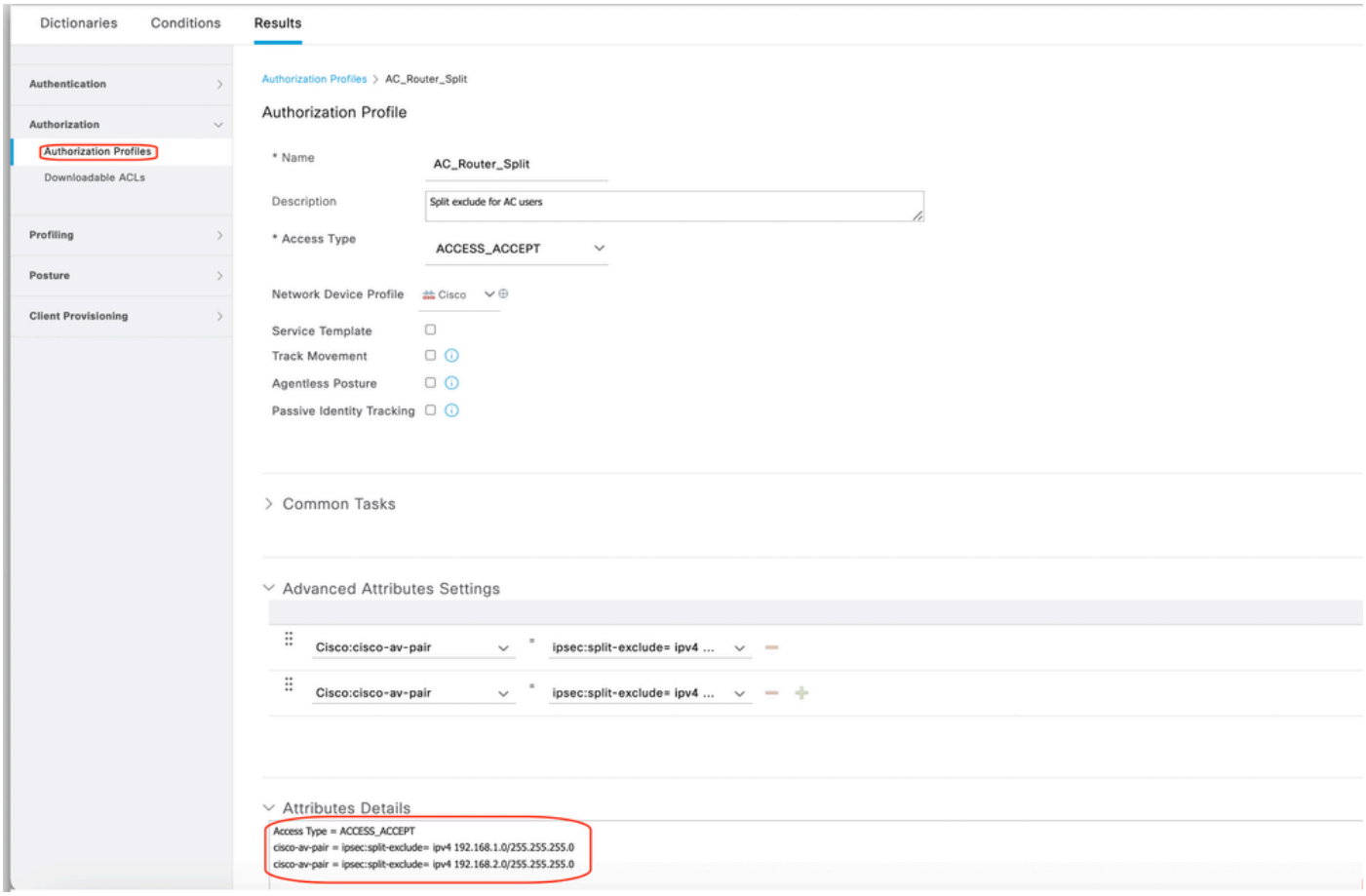


許可プロファイルの設定



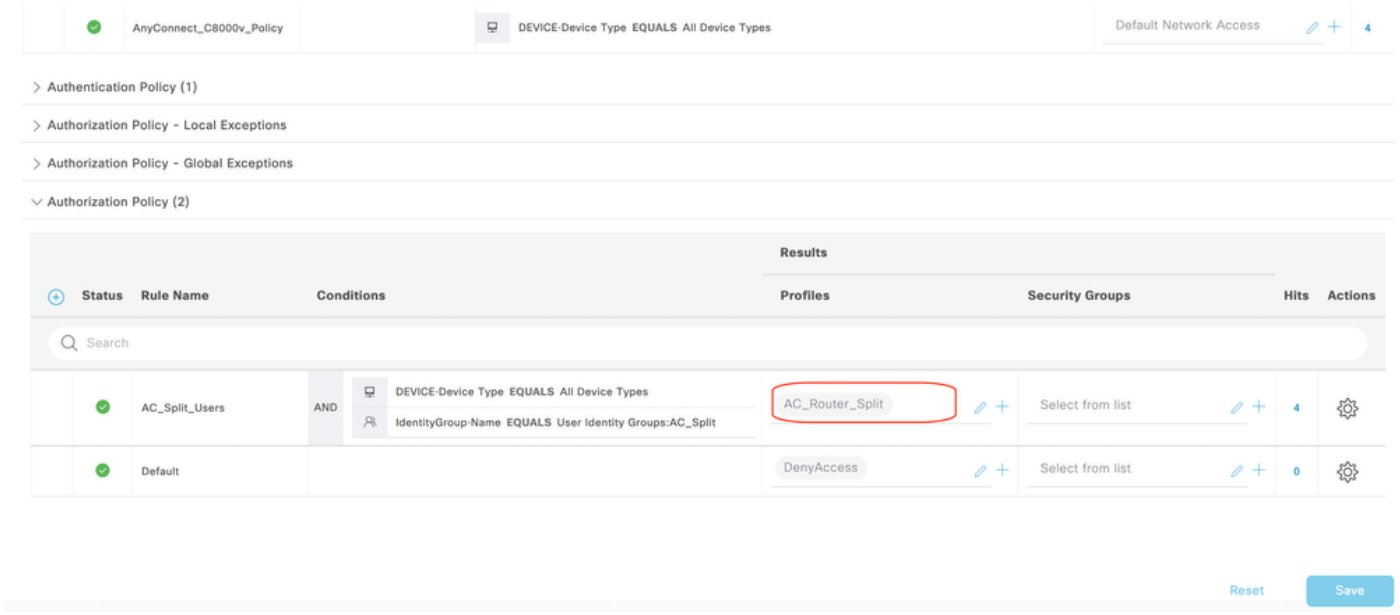
認可プロファイルでの属性の設定

7. 許可プロファイルの設定を確認します。



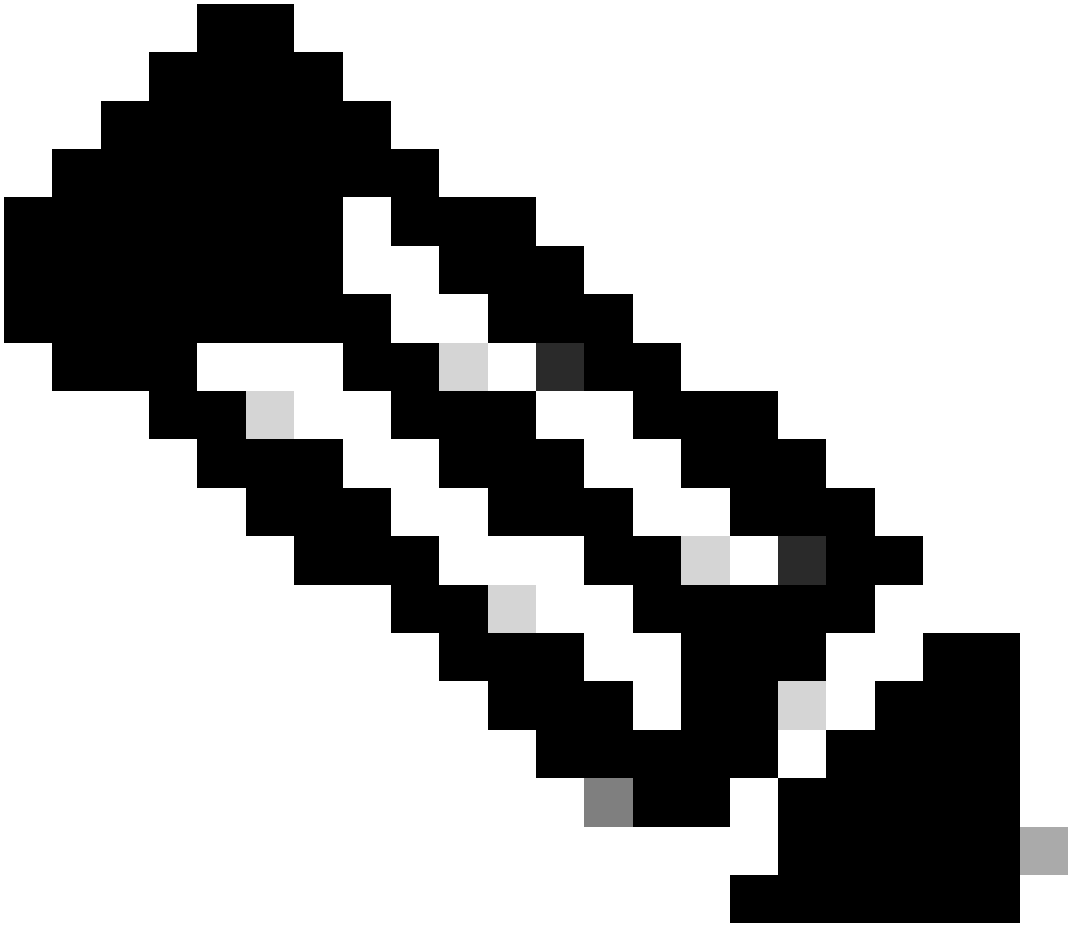
認可プロファイルの設定の確認

8. これは、必要なプロファイルを選択した後のポリシーセット設定の認可ポリシーです。



最終認可ポリシーの設定

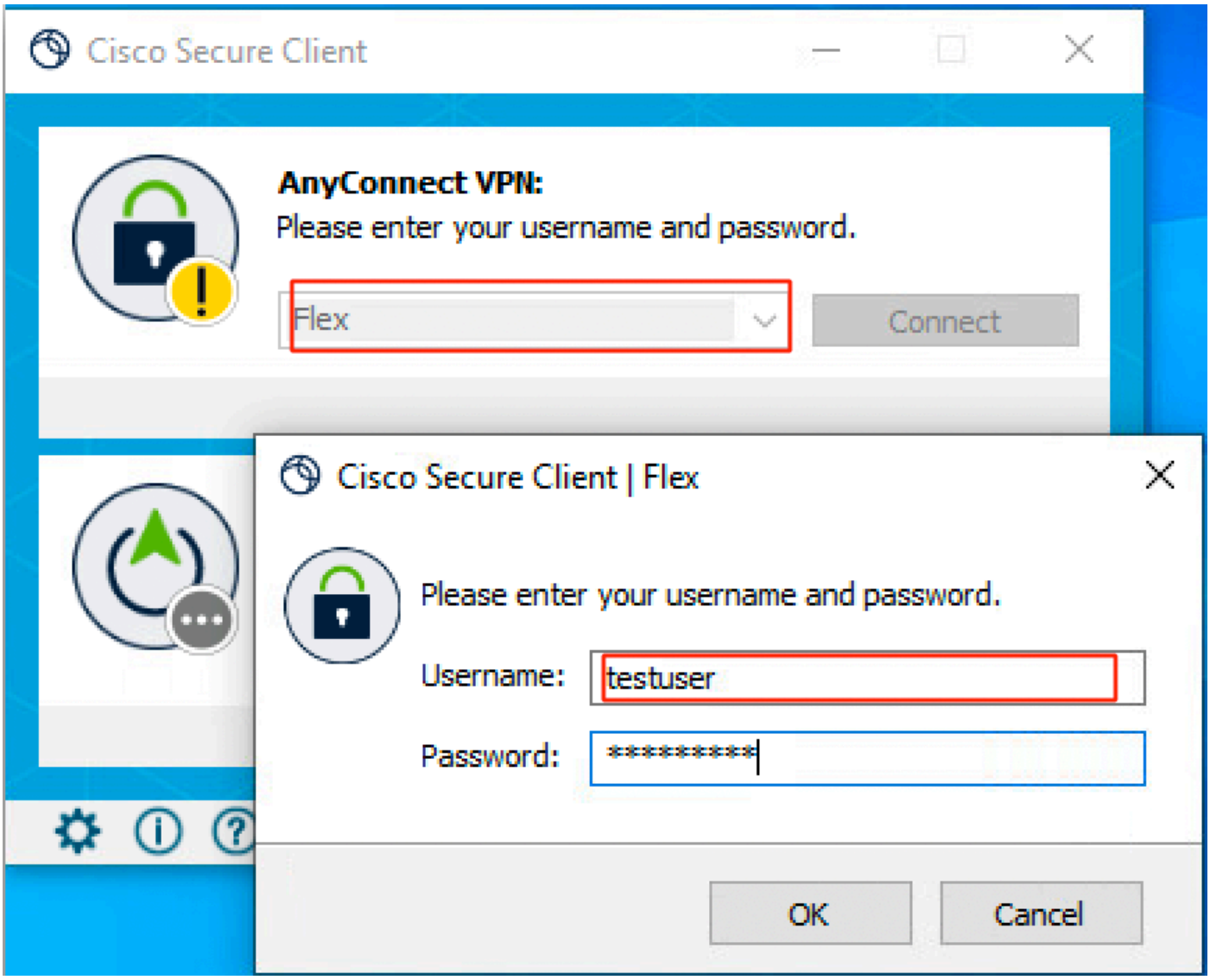
この設定例では、ユーザが属するIDグループに基づいて、ISE設定を介したVPNの通過からネットワークを除外できます。



注:RA VPN接続にCisco IOS XEヘッドエンドを使用する場合、クライアントPCにプッシュできるスプリット除外サブネットは1つだけです。 これについては、Cisco Bug ID CSCwj38106で対処されており、複数のスプリット除外サブネットを17.12.4からプッシュできます。修正済みバージョンの詳細については、バグを参照してください。

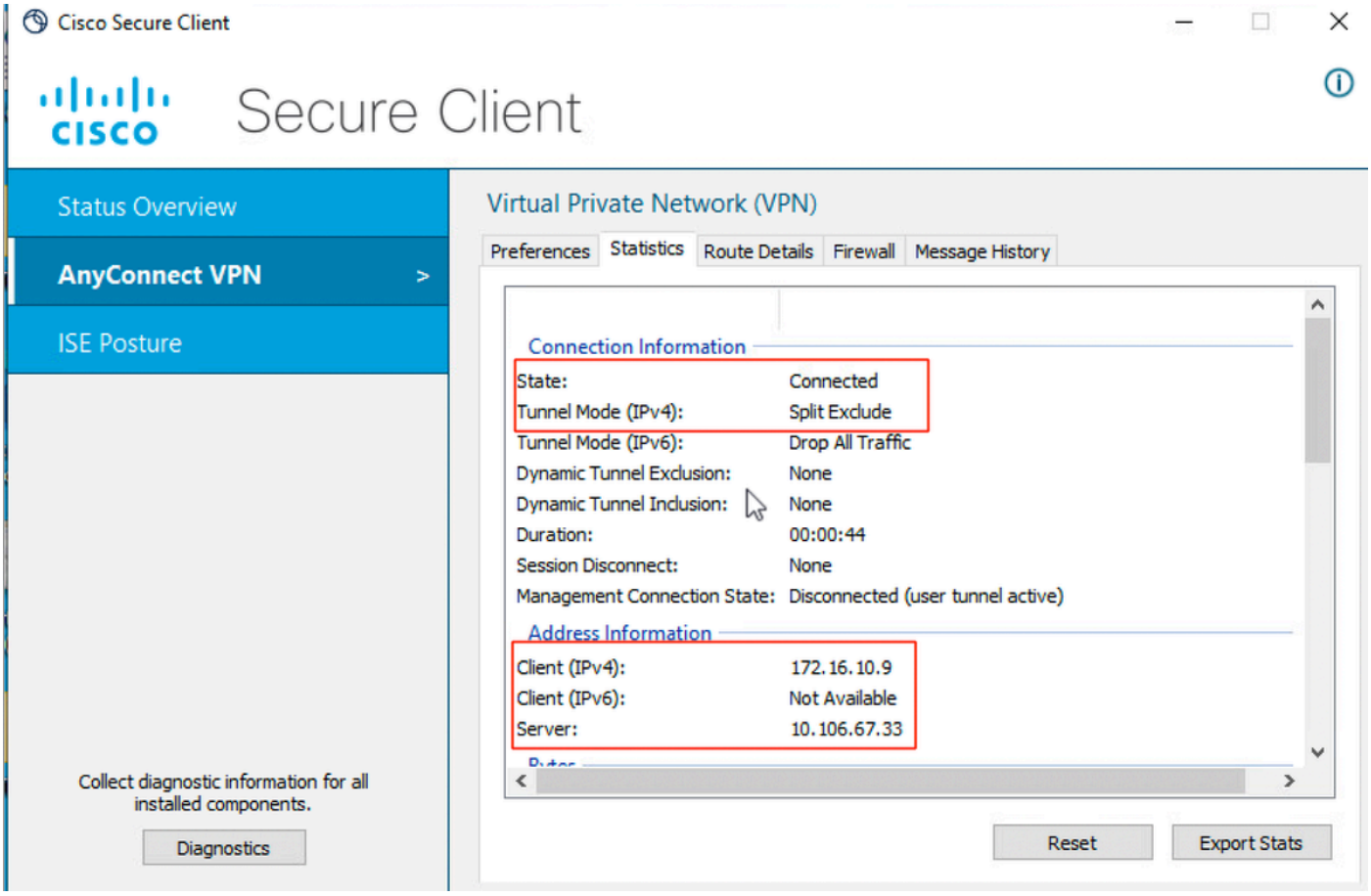
確認

1. 認証をテストするには、ユーザのPCからAnyConnectを使用してC8000Vに接続し、クレデンシャルを入力します。



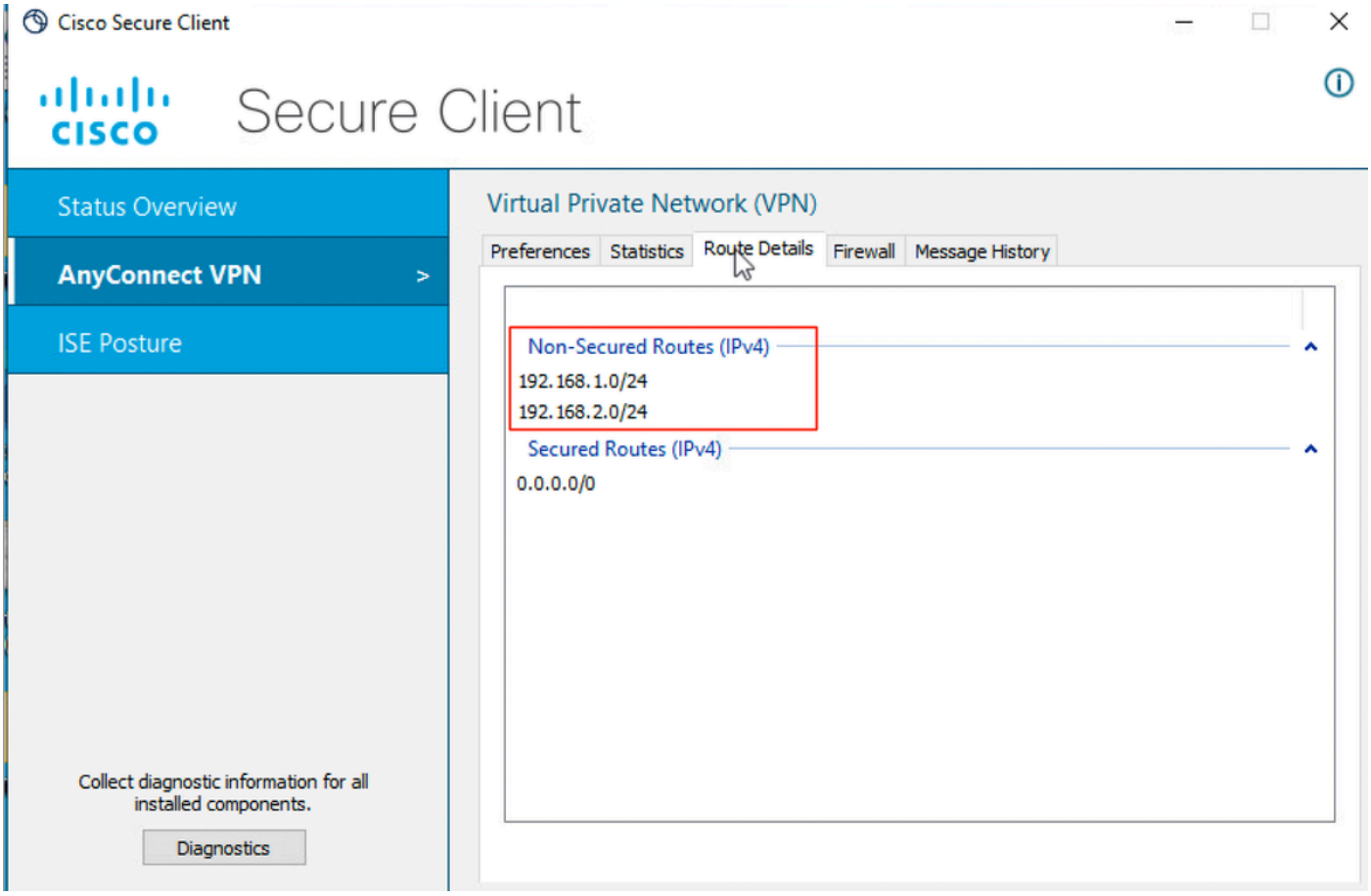
AnyConnectへのログイン

2. 接続が確立されたら、歯車アイコン（左下隅）をクリックして、AnyConnect VPN > Statisticsの順に選択します。スプリット除外するトンネルモードを確認します。



統計情報の検証

AnyConnect VPN > Route detailsの順に移動し、表示される情報がセキュアルートと非セキュアルートに対応していることを確認します。



ルートの詳細の検証

VPNヘッドエンドで接続の詳細を確認することもできます。

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.

トラブルシュート

Ciscoルータ:

1. ヘッドエンドとクライアント間のネゴシエーションを確認するには、IKEv2およびIPSecのデバッグを使用します。

```
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. AAAデバッグを使用して、ローカル属性やリモート属性の割り当てを確認します。

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

ISEで次を実行します。

Operations > Live logsの順に移動して、RADIUSライブログを使用します。

正常動作シナリオ

接続が成功した場合のデバッグを次に示します。

<#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#
```

参考資料

- ローカルユーザデータベースを使用したIKEv2リモートアクセスのためのFlexVPNヘッドエンドの設定
- EAPおよびDUO認証を使用したAnyConnect Flexvpnの設定
- EAP-MD5によるAnyConnect IKEv2リモートアクセスの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。