使用ISE为AnyConnect FlexVPN配置拆分排除

目录

简介

本文档介绍使用ISE为与Cisco IOS® XE路由器的IKEv2 AnyConnect连接配置split-exclude的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 在路由器上配置AnyConnect IPsec的经验
- 思科身份服务引擎(ISE)配置
- 思科安全客户端(CSC)
- RADIUS协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 8000V(C8000V)- 17.12.04
- 思科安全客户端 — 5.0.02075
- 思科ISE - 3.2.0
- Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

网络图

配置

要完成配置，请考虑以下部分。

路由器配置

1.在设备上配置RADIUS服务器进行身份验证和本地授权：

```
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.配置信任点以安装路由器证书。由于路由器的本地身份验证类型为RSA，因此设备要求服务器使用证书对自身进行身份验证。有关证书创建的详细信息，请参阅PKI -1的证书注册和PKI -2的证书注册:

```
crypto pki trustpoint flex
 enrollment terminal
 ip-address none
 subject-name CN=flexserver.cisco.com
 revocation-check none
 rsakeypair flex1
 hash sha256
```

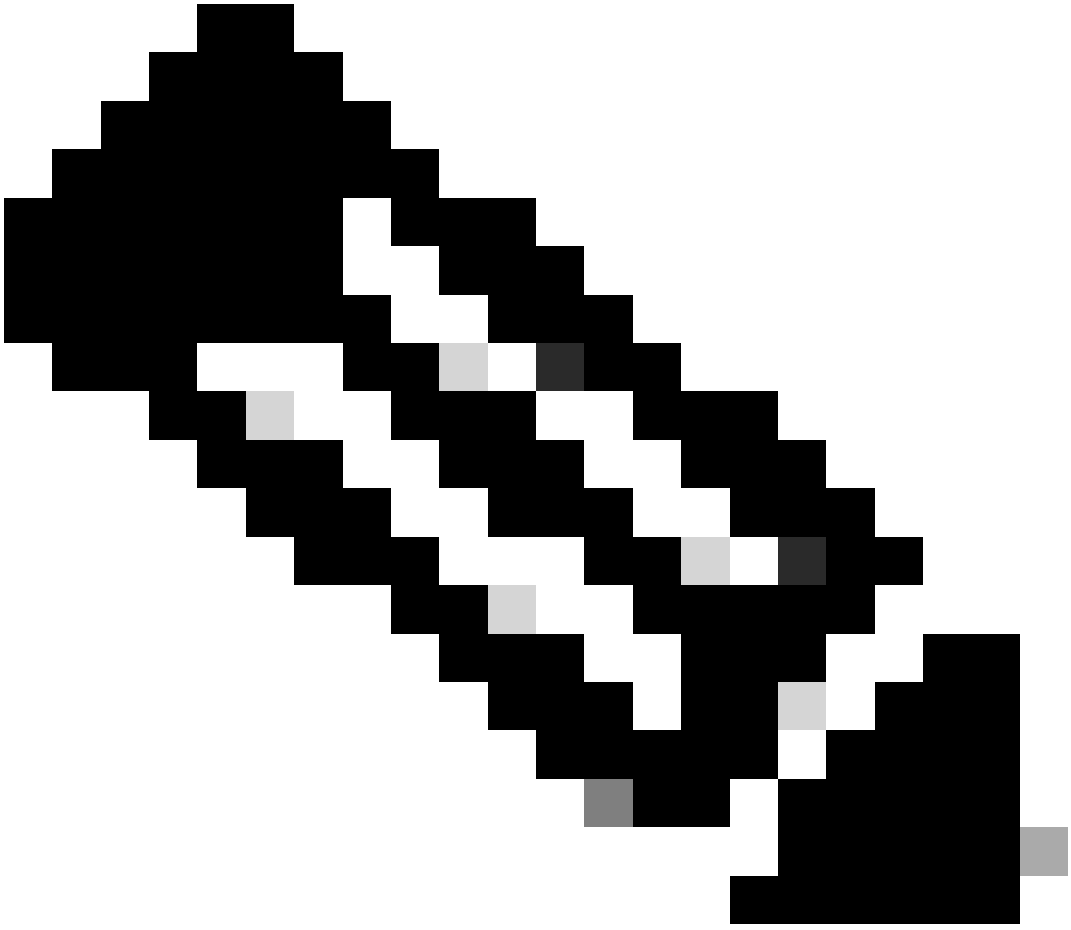
3.定义IP本地池，以便在AnyConnect连接成功时为AnyConnect VPN客户端分配地址：

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

4.创建IKEv2本地授权策略：

此策略中定义的属性以及从Radius服务器推送的属性将应用于用户

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



注意：如果未配置自定义IKEv2授权策略，则使用名为default的默认授权策略进行授权。在

IKEv2授权策略下指定的属性也可以通过RADIUS服务器推送。您需要从RADIUS服务器推送split-exclude属性。

5（可选）。 创建IKEv2建议和策略（如果未配置，则使用智能默认值）：

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

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

6（可选）。 配置转换集（如果未配置，则使用智能默认值）：

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

7.使用某些虚构IP地址配置环回接口。虚拟访问接口从它借用IP地址：

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

8.配置从中克隆虚拟访问接口的虚拟模板：

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

9.将AnyConnect客户端配置文件上传到路由器的bootflash并定义配置文件，如下所示：

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

10.配置包含所有连接相关信息的IKEv2配置文件：

```
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
```

以下内容用于IKEv2配置文件中：

- match identity remote key-id *$AnyConnectClient$$* — 指客户端的身份。AnyConnect使用*$AnyConnectClient$*作为其类型为key-id的默认IKE身份。但是，可以在AnyConnect配置文件中手动更改此身份以满足部署需求。
- authentication remote — 提及EAP协议必须用于客户端身份验证。
- authentication local — 提及必须使用证书进行本地身份验证。
- aaa authentication eap — 在EAP身份验证期间，使用RADIUS服务器FlexVPN_auth。
- aaa authorization group eap list — 在授权过程中，网络列表a-eap-author-grp与authorization policyikev2-auth-policy一起使用。
- aaa authorization user eap cached — 启用隐式用户授权。
- virtual-template 100 -定义要克隆的虚拟模板。
- anyconnect profile acvpn — 第9步中定义的客户端配置文件。应用于此IKEv2配置文件。

11.配置IPsec配置文件：

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

12.将IPsec配置文件添加到虚拟模板：

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

13.在路由器上禁用基于HTTP-URL的证书查找和HTTP服务器：

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

14.配置SSL策略并将路由器的WAN IP指定为下载配置文件的本地地址：

```
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客户端配置文件（XML配置文件）的代码段：

在Cisco IOS XE 16.9.1版本之前，不能从头端自动下载配置文件。在16.9.1之后，可以从头端下载配置文件。

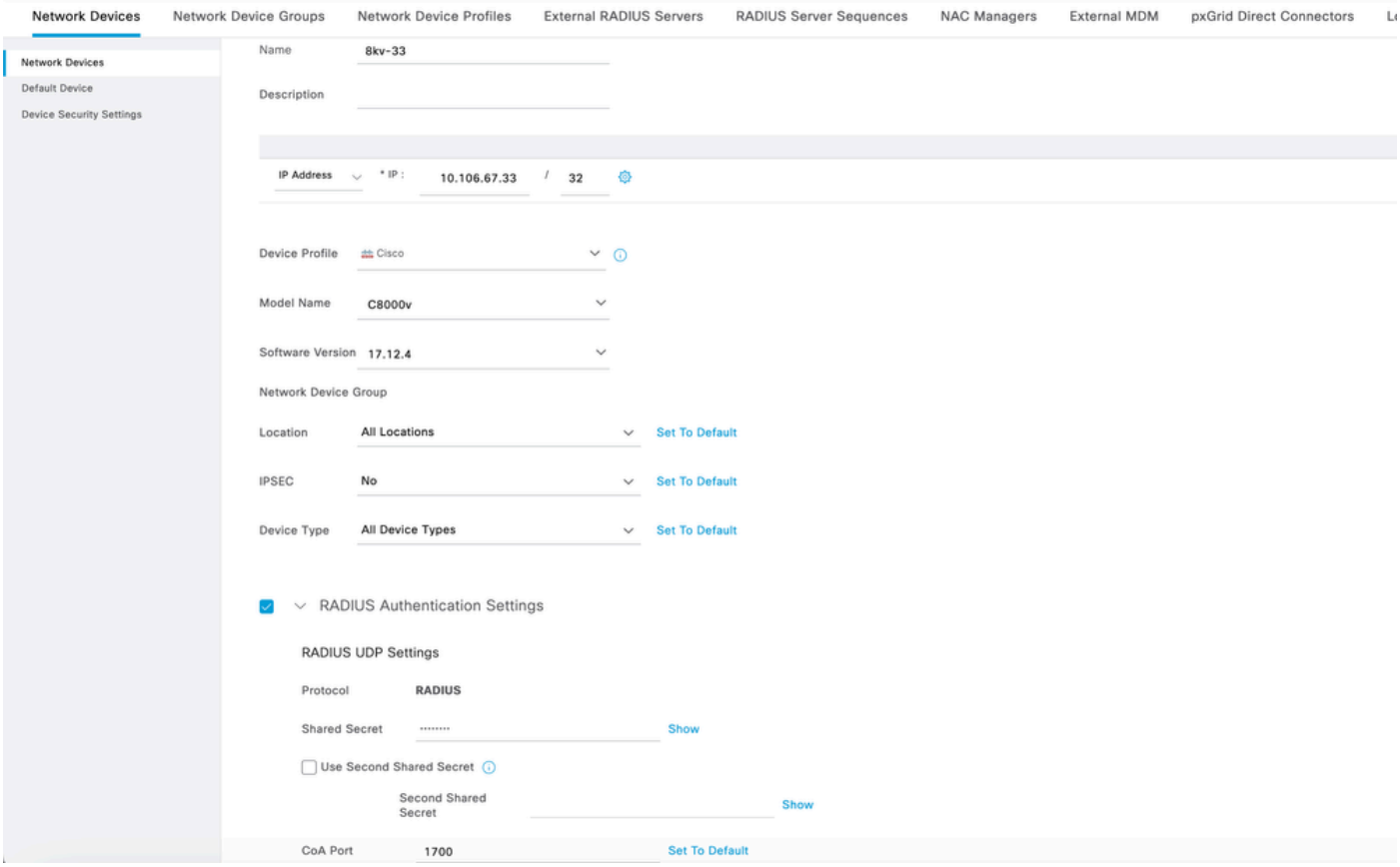
<#root>

```
<?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>
```

身份服务引擎(ISE)配置

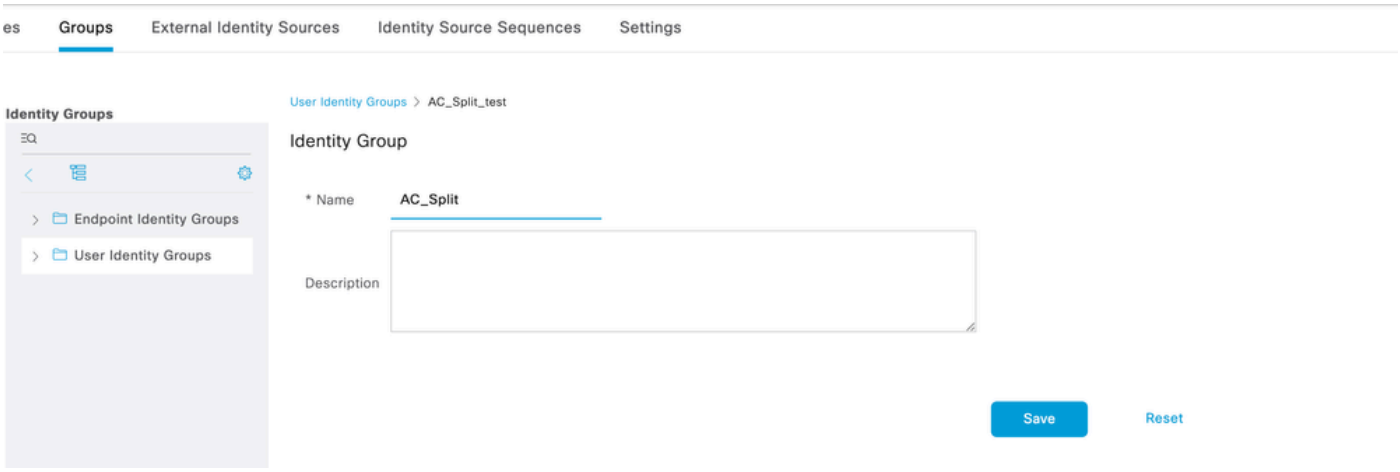
1.将路由器注册为ISE上的有效网络设备并配置RADIUS的共享密钥。为此，请导航到管理>网络资源>网络设备。单击添加将路由器配置为AAA客户端：



添加网络设备

2.创建身份组：

定义身份组，以关联具有相似特征以及共享相似权限的用户。这些将在后续步骤中使用。依次导航到管理(Administration)>身份管理(Identity Management)> 组(Groups)>用户身份组(User Identity Groups)，然后点击添加(Add):



创建身份组

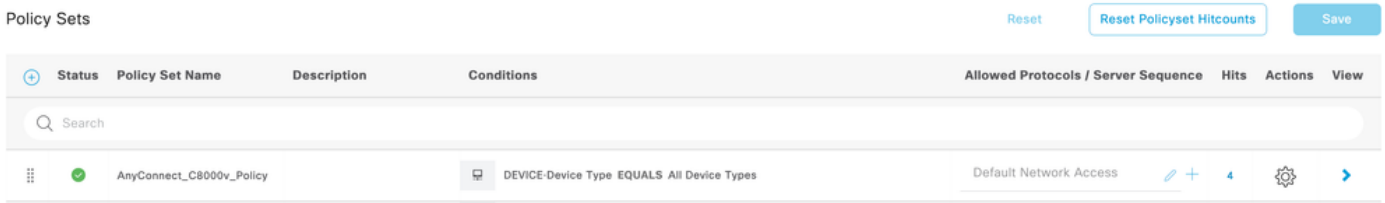
3.将用户与身份组关联：

将用户关联到正确的身份组。导航到管理>身份管理 > 身份>用户。

将用户添加到身份组

4.创建策略集：

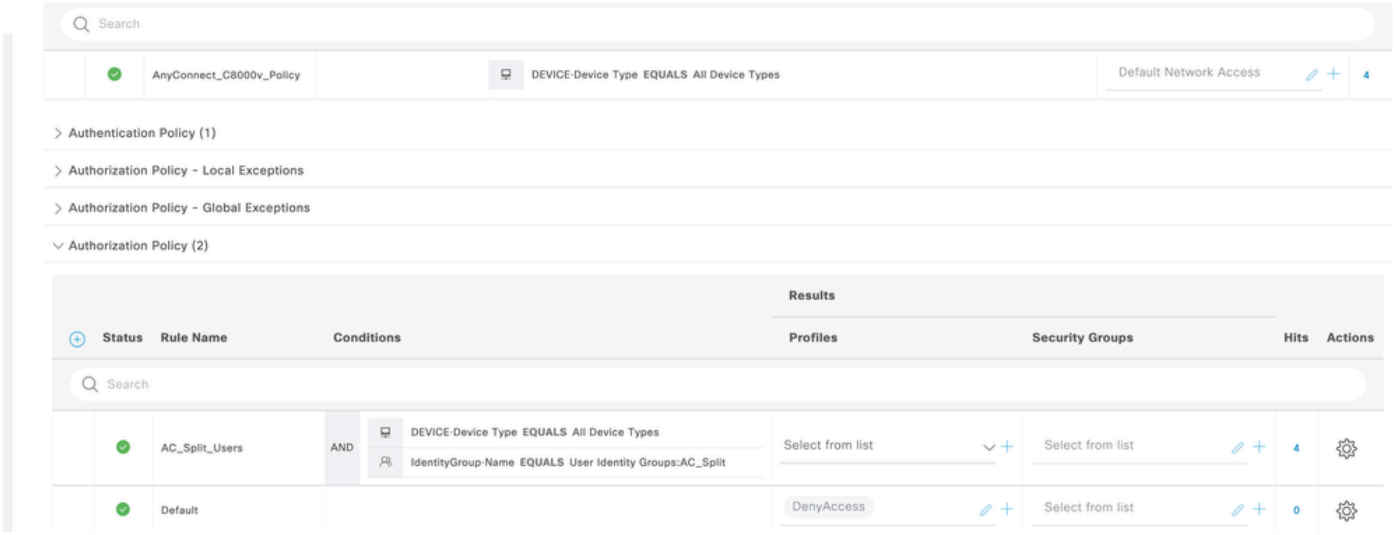
定义新的策略集并定义与策略匹配的条件。在本例中，在这些条件下允许所有设备类型。为此，请导航到Policy>Policy sets:



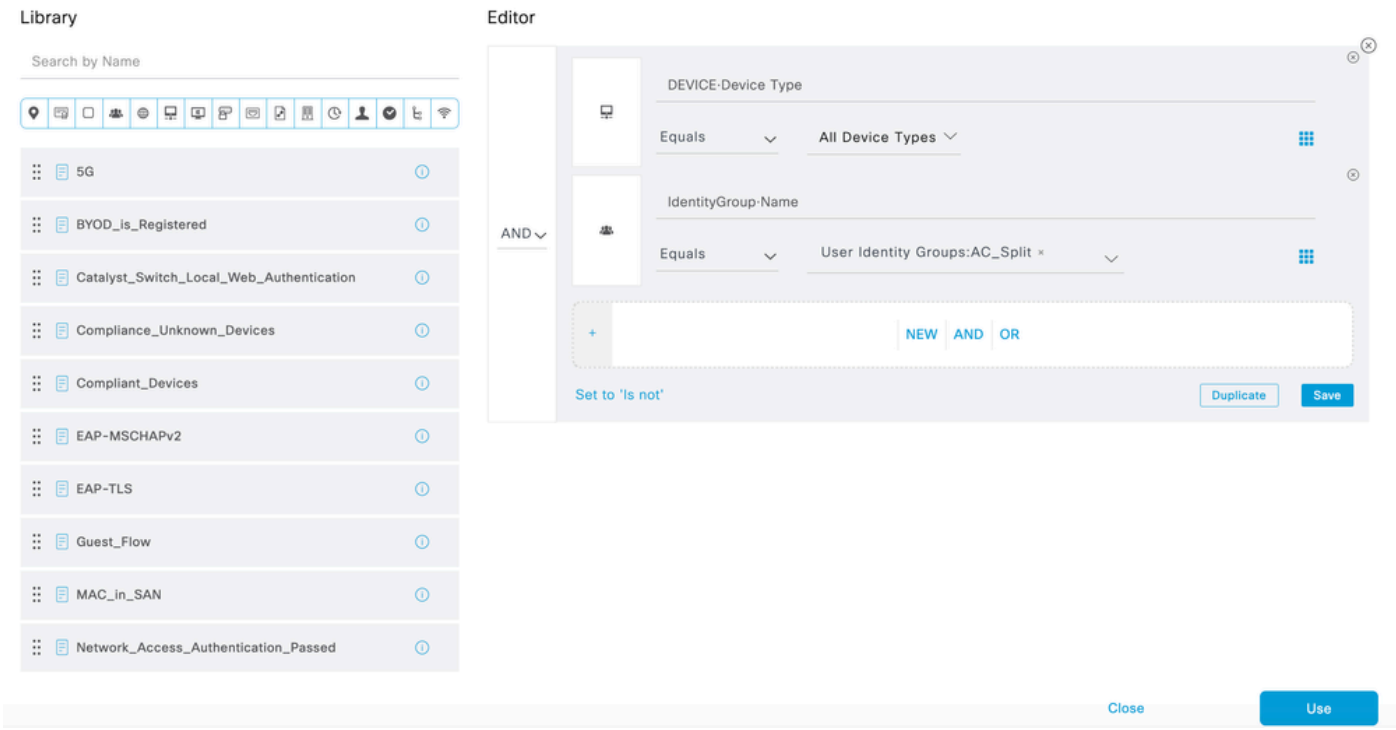
创建策略集

5.创建授权策略：

定义新的授权策略以及匹配策略的所需条件。确保将步骤2中创建的身份组作为条件包含在内。



创建授权策略

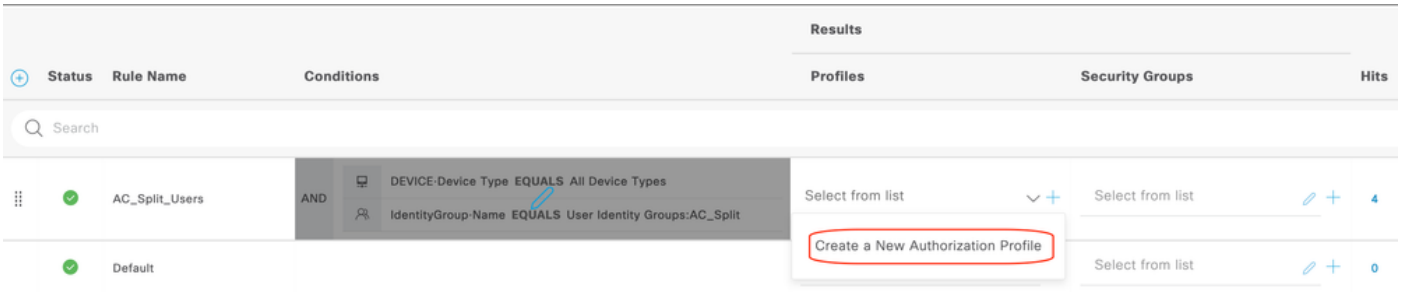


选择授权策略中的条件

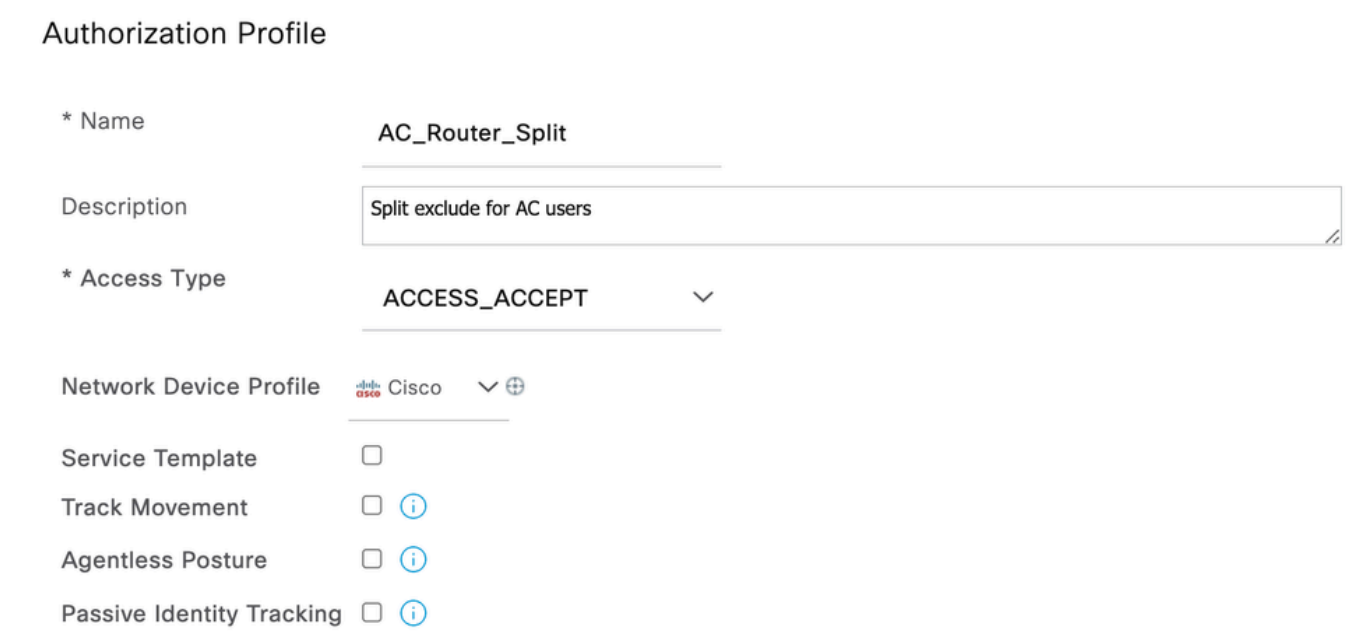
6.创建授权配置文件：

授权配置文件包括匹配授权策略时执行的操作。创建新的授权配置文件，其中包括以下属性：

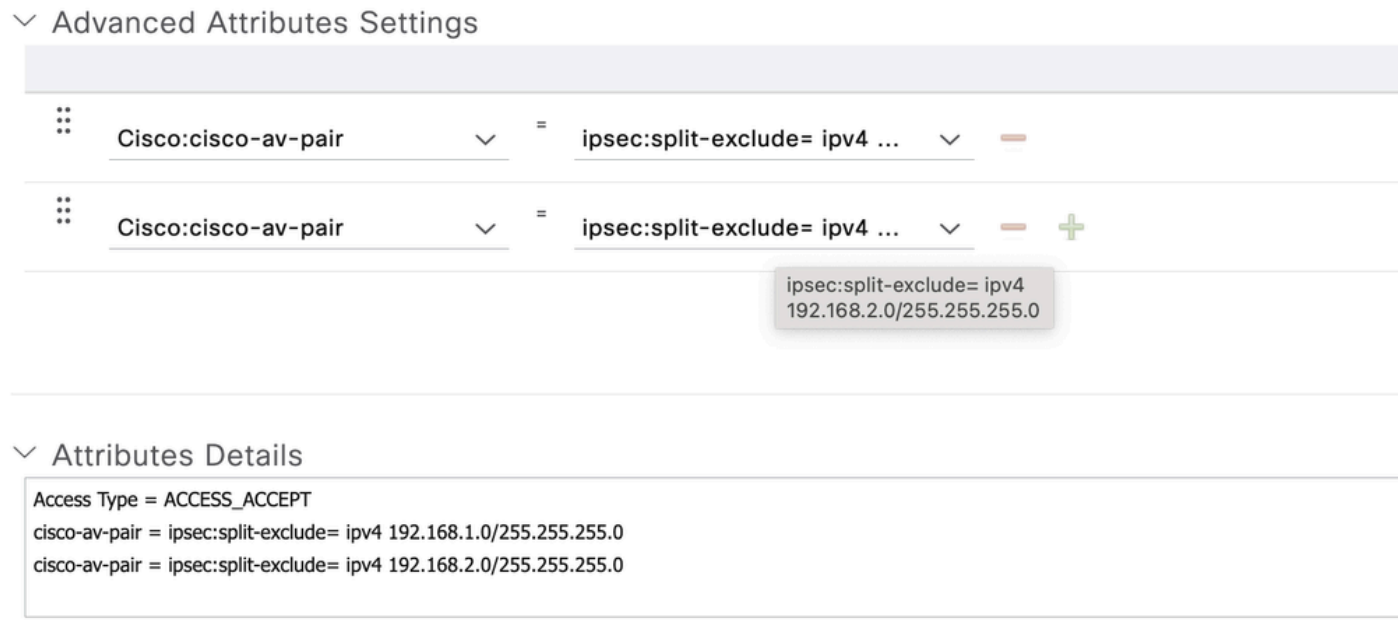
访问类型= ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <ip_network>/<subnet_mask>



创建新的授权配置文件

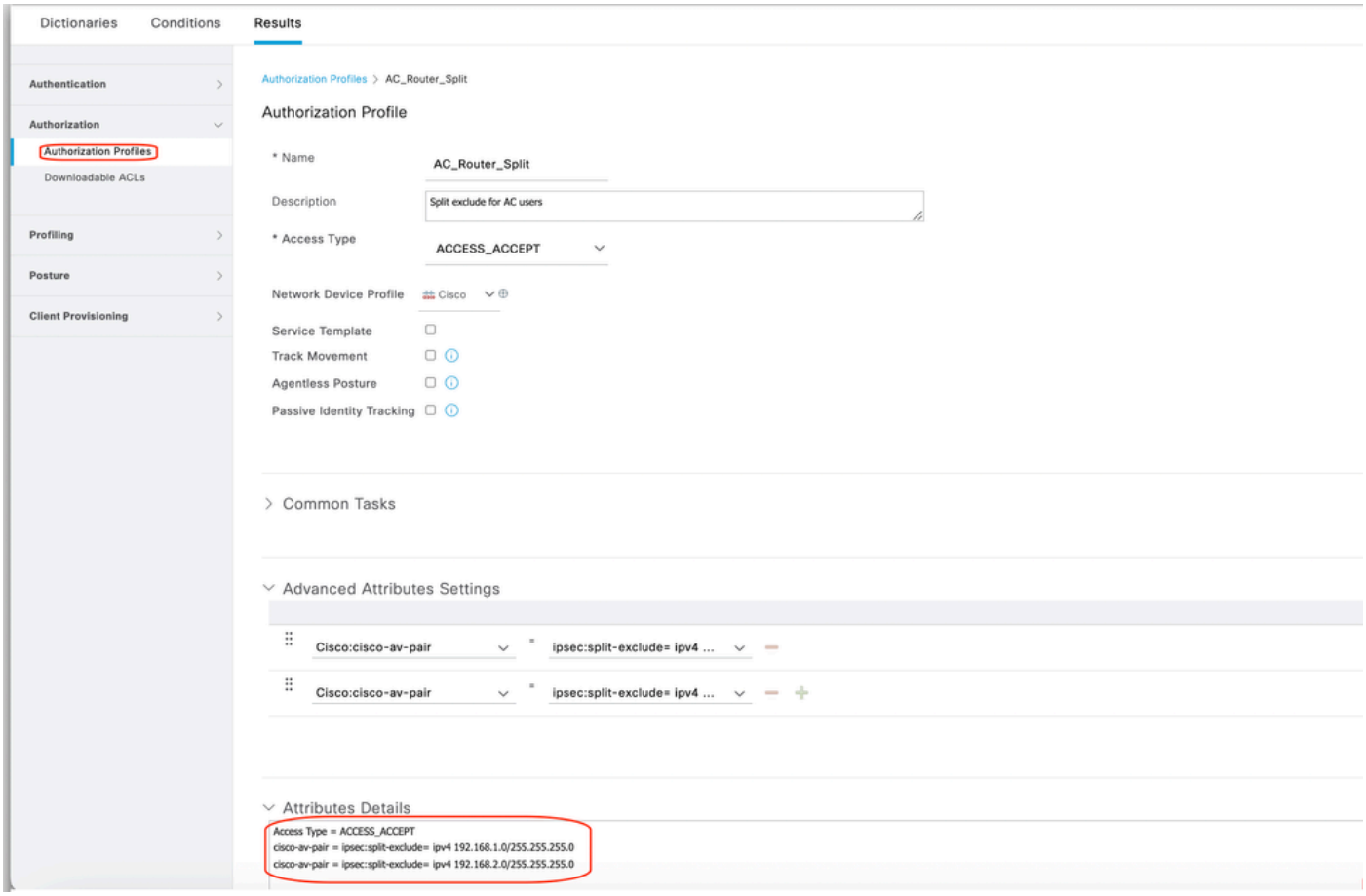


授权配置文件配置



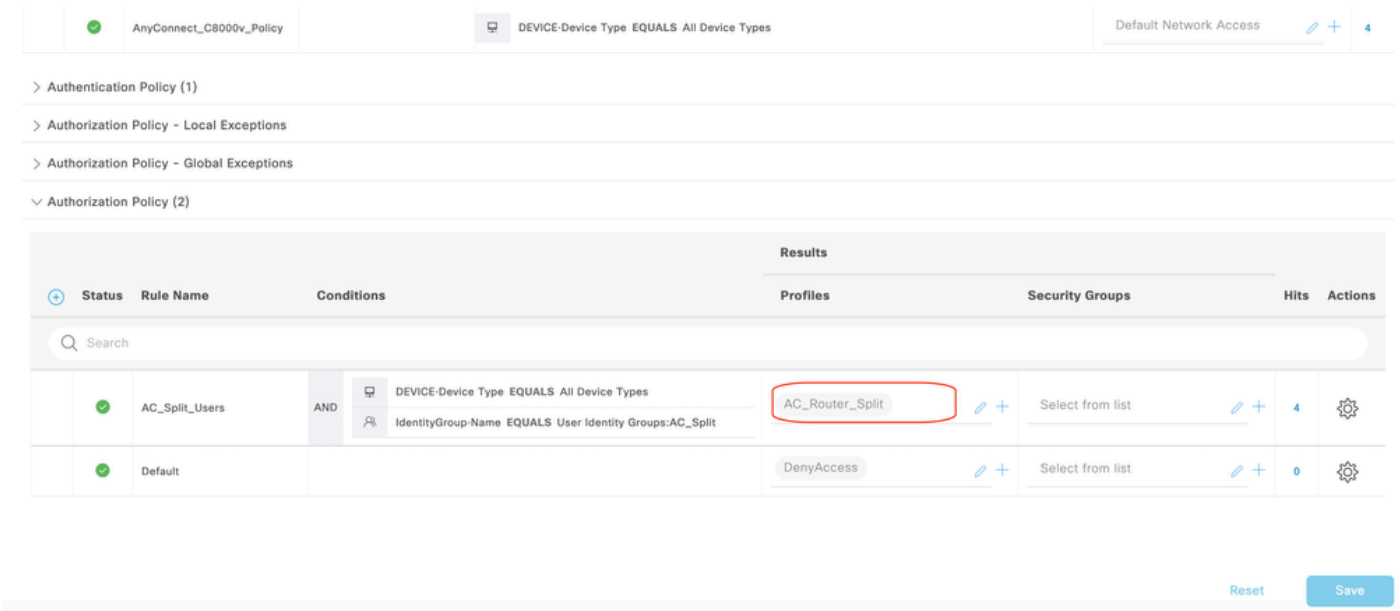
配置授权配置文件中的属性

7.检查授权配置文件配置。



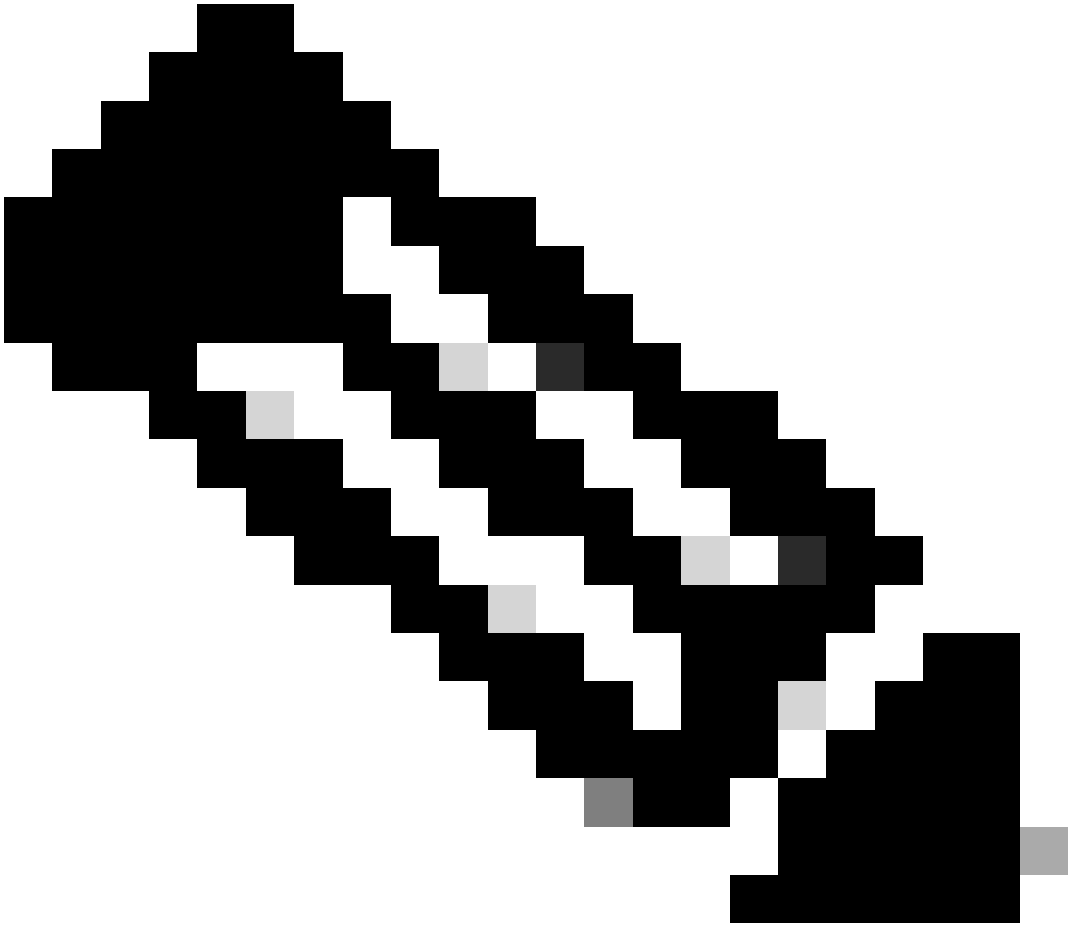
检查授权配置文件配置

8.在选择所需的配置文件后，这是策略集配置中的授权策略：



最终授权策略配置

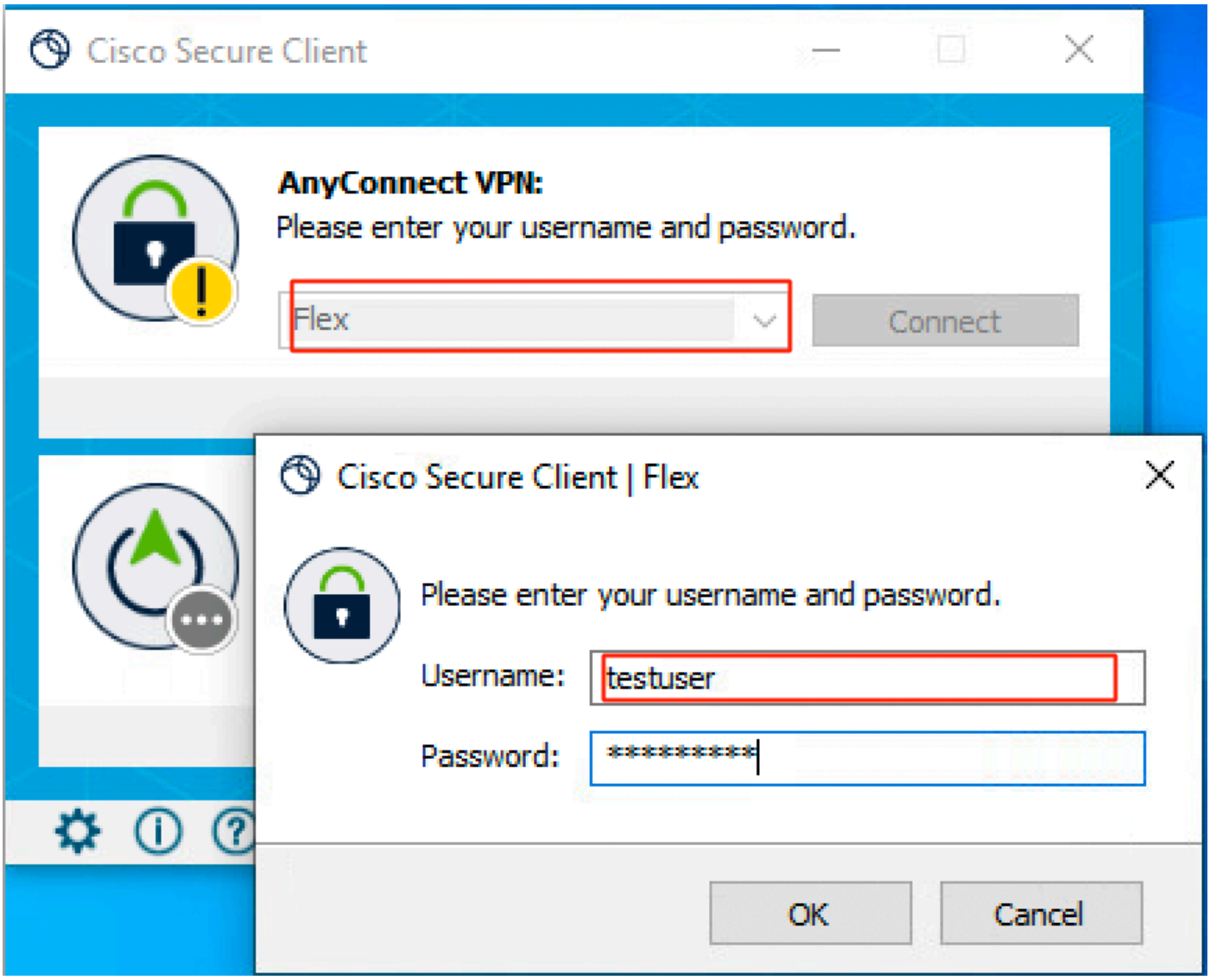
在此配置示例中，您可以根据用户所属的身份组排除通过ISE配置通过VPN的网络。



注意：当使用Cisco IOS XE头端进行RA VPN连接时，只能将一个拆分排除子网推送到客户端PC。这个问题已由Cisco Bug ID CSCwj38106解决，并且可从版本17.12.4推送到多个拆分排除子网。有关固定版本的更多详细信息，请参阅Bug。

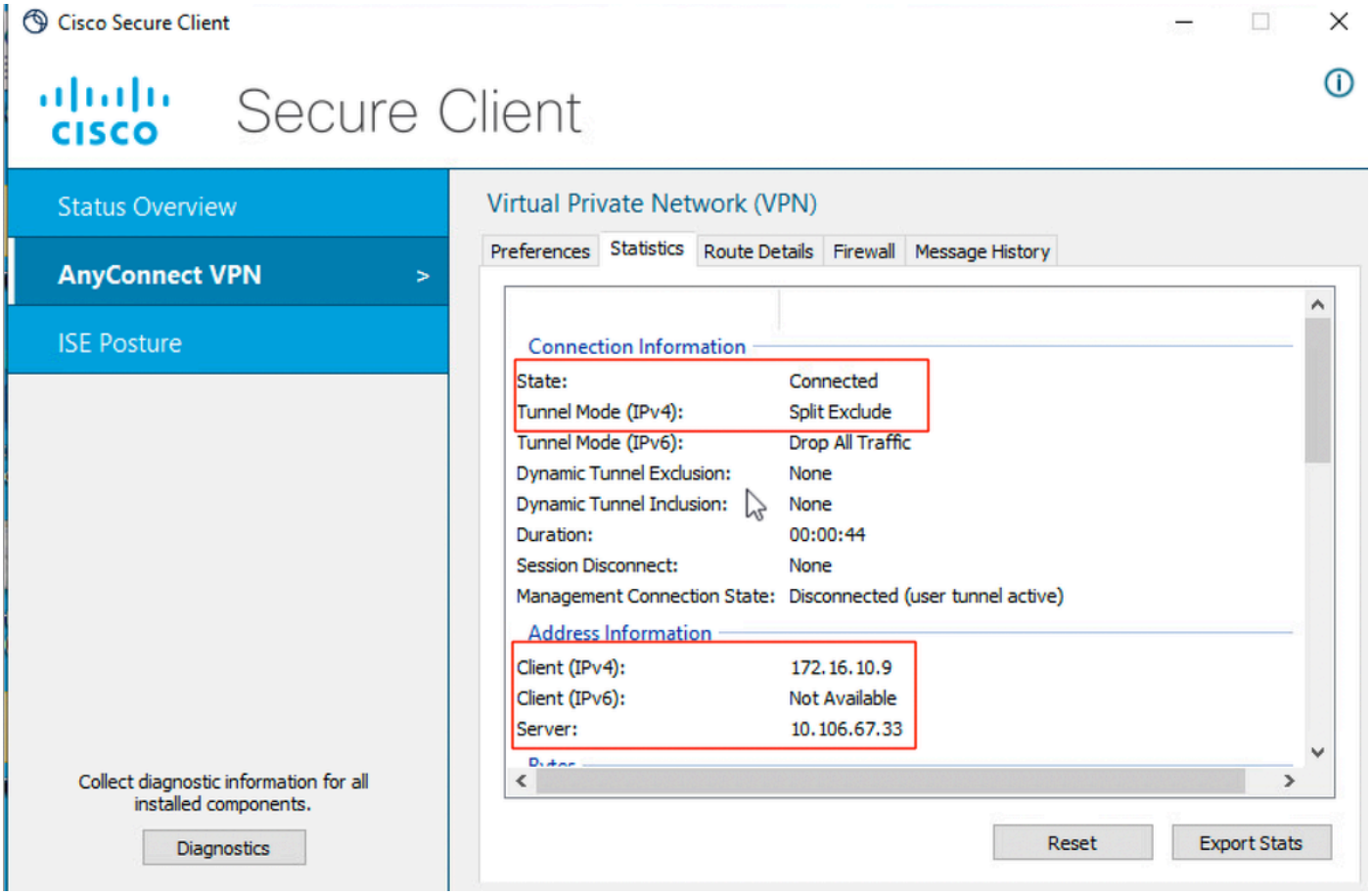
验证

1.为了测试身份验证，请通过AnyConnect从用户的PC连接到C8000V并输入凭证。



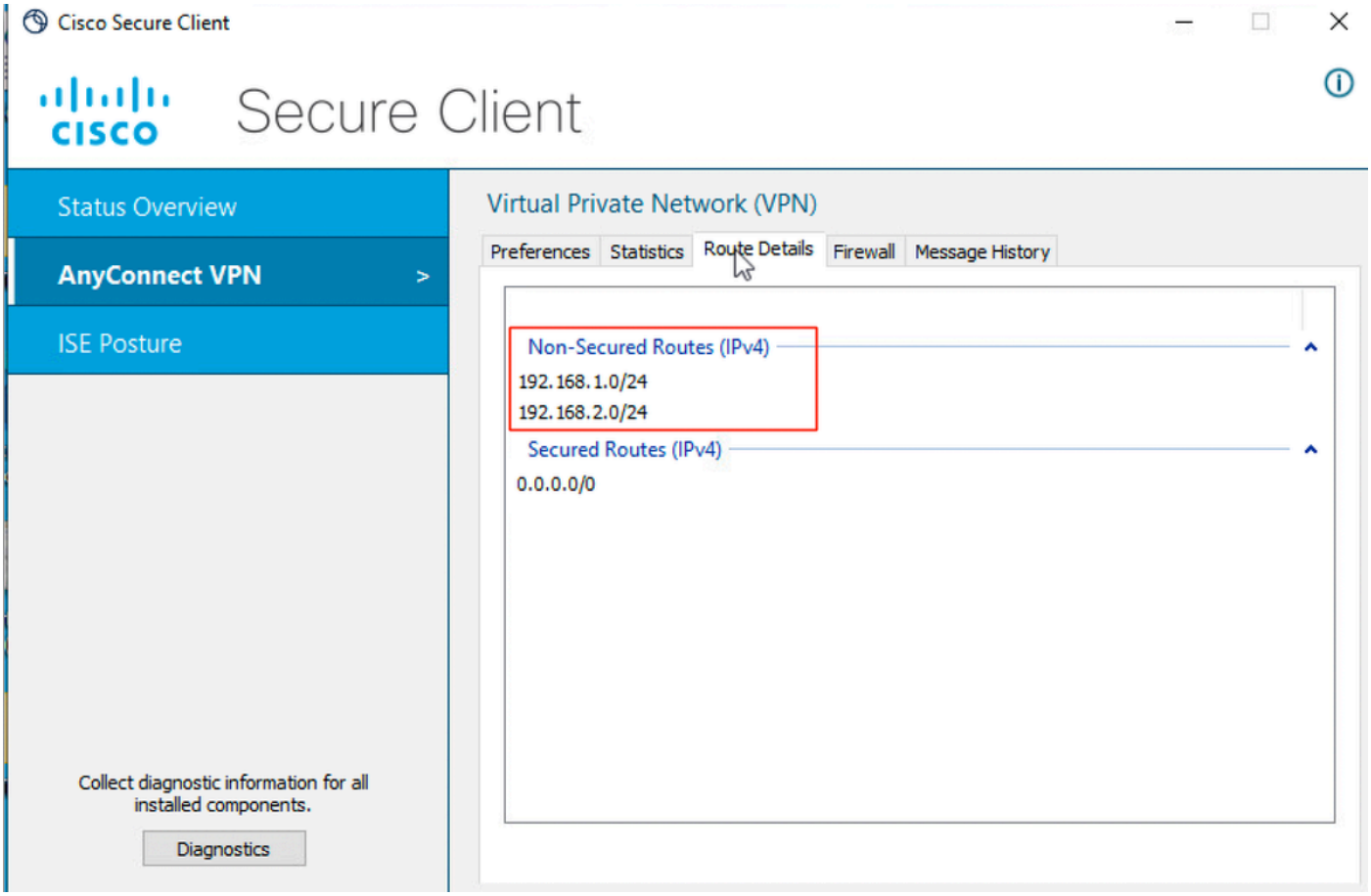
登录AnyConnect

2.建立连接后，单击齿轮图标（左下角）并导航到AnyConnectVPN > 统计信息。确认Tunnel Mode to be Split Exclude。



验证统计信息

导航到AnyConnectVPN > Route details，并确认显示的信息与安全路由和非安全路由对应。



验证路由详细信息

您还可以验证VPN头端上的连接详细信息：

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.

故障排除

在Cisco路由器上:

1. 使用IKEv2和IPsec调试验证头端和客户端之间的协商。

```
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. 使用AAA调试验证本地和/或远程属性的分配。

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

在ISE上：

导航到Operations > Live logs以使用RADIUS实时日志。

工作场景

这是成功连接的调试：

<#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

- 使用本地用户数据库为IKEv2远程访问配置FlexVPN前端
- 配置采用EAP和DUO身份验证的AnyConnect Flexvpn
- 使用EAP-MD5配置AnyConnect IKEv2远程访问

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。