Configuración de Split Exclude para AnyConnect FlexVPN con ISE

Contenido

Introducción

Este documento describe el procedimiento para configurar split-exclude mediante ISE para la conexión IKEv2 AnyConnect a un router Cisco IOS® XE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Experiencia con la configuración de AnyConnect IPsec en un router
- Configuración de Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocolo RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

Diagrama de la red

Configuraciones

Para completar la configuración, tenga en cuenta estas secciones.

Configuración del router

1. Configure un servidor RADIUS para la autenticación y autorización local en el dispositivo:

```
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. Configure un punto de confianza para instalar el certificado del router. Dado que la autenticación local del router es de tipo RSA, el dispositivo requiere que el servidor se autentique utilizando un certificado. Puede consultar Inscripción de certificado para PKI -1 y Inscripción de certificado para PKI -2 para obtener más detalles sobre la creación del certificado:

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

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

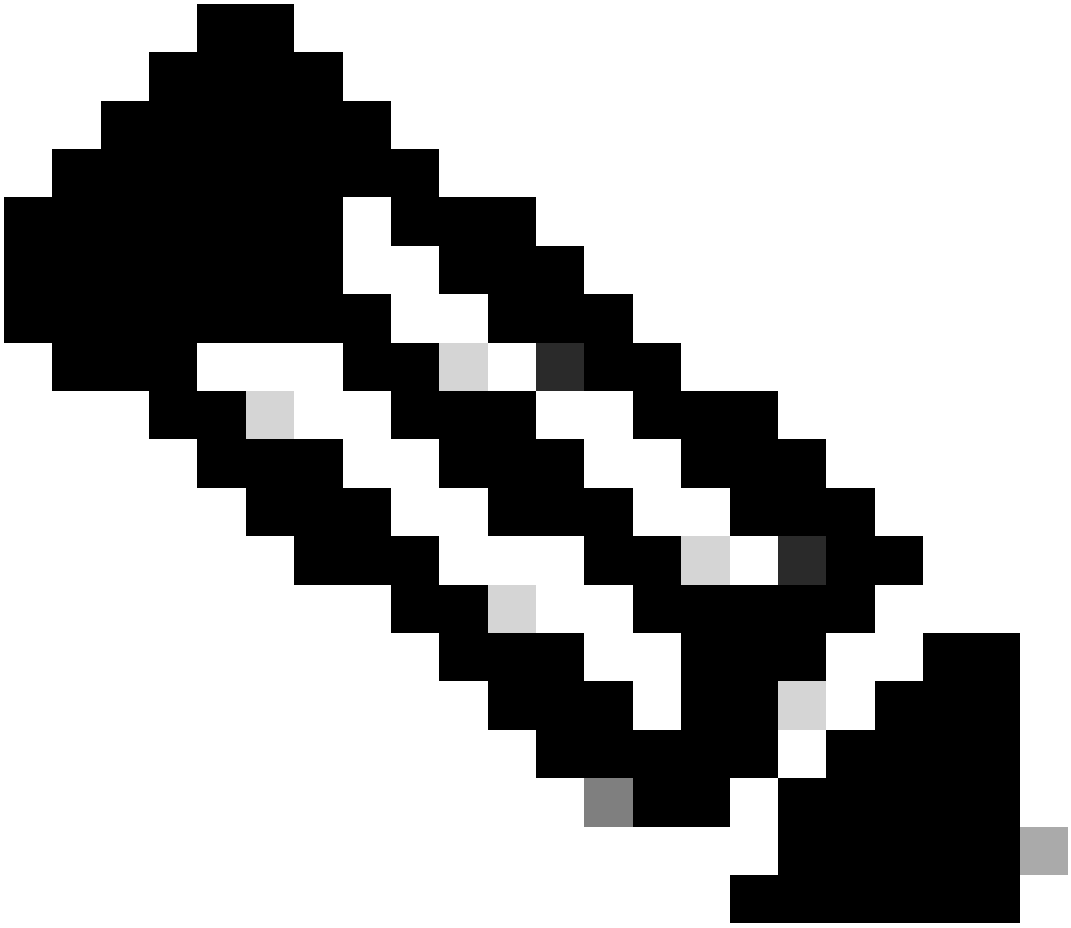
3. Defina un conjunto local de IP para asignar direcciones a los clientes VPN de AnyConnect en caso de conexión correcta de AnyConnect:

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

4. Cree una política de autorización local IKEv2:

Los atributos definidos en esta política junto con los atributos enviados desde el servidor Radius se aplican a los usuarios

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



Nota: Si no se configura la directiva de autorización IKEv2 personalizada, se utiliza la directiva de autorización predeterminada denominada default para la autorización. Los atributos especificados en la directiva de autorización IKEv2 también se pueden enviar a través del servidor RADIUS. Debe insertar el atributo split-exclude desde el servidor RADIUS.

5 (opcional). Cree una propuesta y una política IKEv2 (si no se configura, se utilizan los valores predeterminados inteligentes):

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

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

6 (Opcional). Configure el conjunto de transformación (si no se configura, se utilizan los valores predeterminados inteligentes):

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

7. Configure una interfaz de loopback con alguna dirección IP ficticia. Las interfaces de acceso virtual le piden prestada la dirección IP:

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

8. Configure una plantilla virtual a partir de la cual se clonan las interfaces de acceso virtual:

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

9. Cargue el perfil de cliente de AnyConnect en la memoria de inicialización del router y defina el perfil como se indica a continuación:

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

10. Configure un perfil IKEv2 que contenga toda la información relacionada con la conexión:

```
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
```

Se utilizan en el perfil IKEv2:

- match identity remote key-id *$AnyConnectClient$* - Se refiere a la identidad del cliente. AnyConnect utiliza *$AnyConnectClient$* como su identidad IKE predeterminada de tipo key-id. Sin embargo, esta identidad se puede cambiar manualmente en el perfil de AnyConnect para que coincida con las necesidades de implementación.
- authentication remote - Menciona que el protocolo EAP se debe utilizar para la autenticación del cliente.
- authentication local - Indica que los certificados deben utilizarse para la autenticación local.
- aaa authentication eap - Durante la autenticación EAP, se utiliza el servidor RADIUS FlexVPN_auth.
- aaa authorization group eap list - Durante la autorización, la lista de red a-eap-author-grp se utiliza con la política de autorización ikev2-auth-policy.
- aaa authorization user eap cached: habilita la autorización de usuario implícita.
- virtual-template 100 - Define qué plantilla virtual clonar.
- anyconnect profile acvpn: el perfil de cliente definido en el paso 9 se aplica aquí a este perfil IKEv2.

11. Configure el perfil IPsec:

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

12. Agregue el perfil IPsec a la plantilla virtual:

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

13. Desactive la búsqueda de certificados basada en HTTP-URL y el servidor HTTP en el router:

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

14. Configure la política SSL y especifique la IP de WAN del router como la dirección local para descargar el perfil:

```
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
```

Fragmento del perfil de cliente de AnyConnect (perfil XML):

Antes de Cisco IOS XE 16.9.1, las descargas de perfiles automáticas desde la cabecera no estaban disponibles. Post 16.9.1, es posible descargar el perfil de la cabecera.

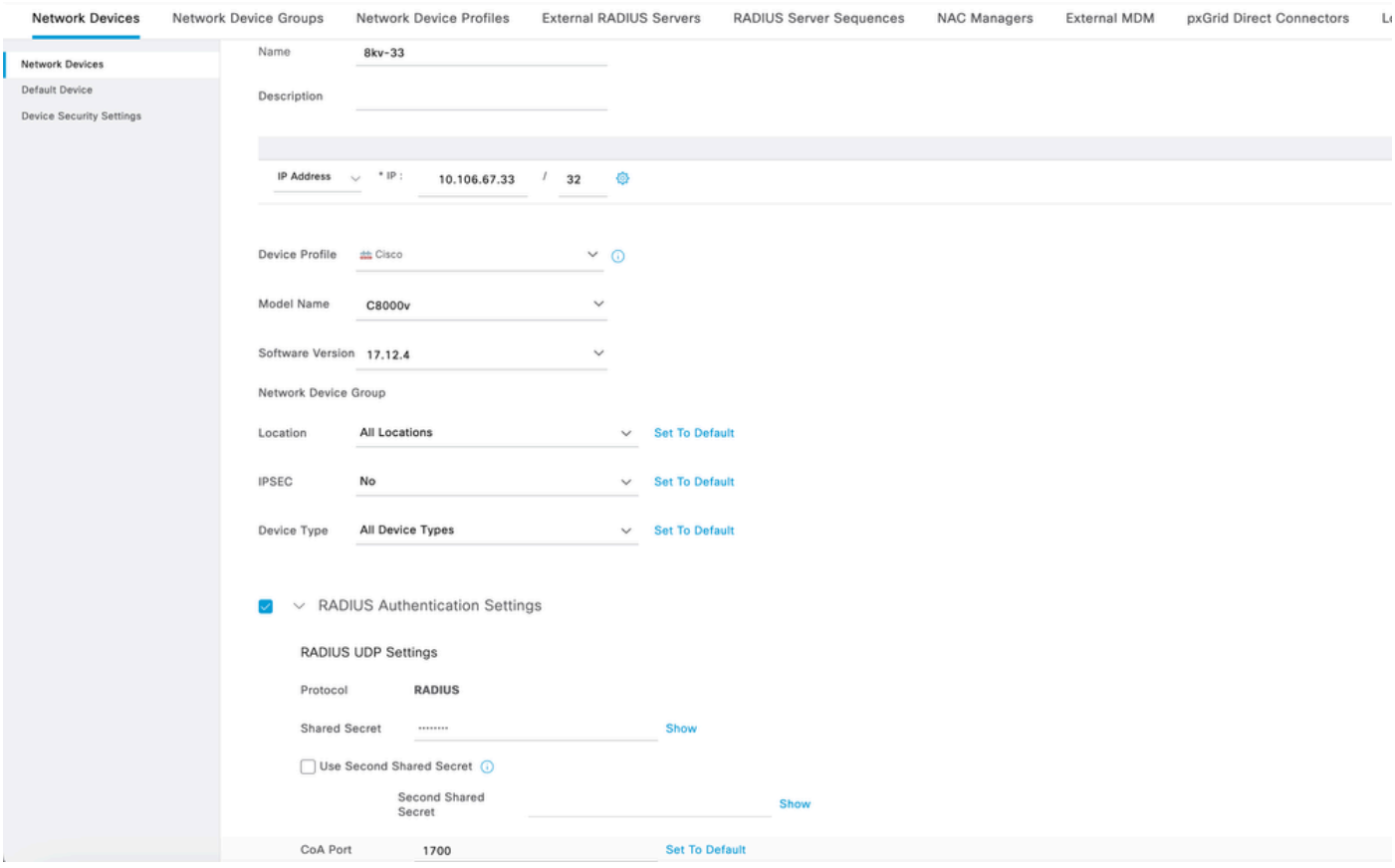
<#root>

```
<?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>
```

Configuración de Identity Services Engine (ISE)

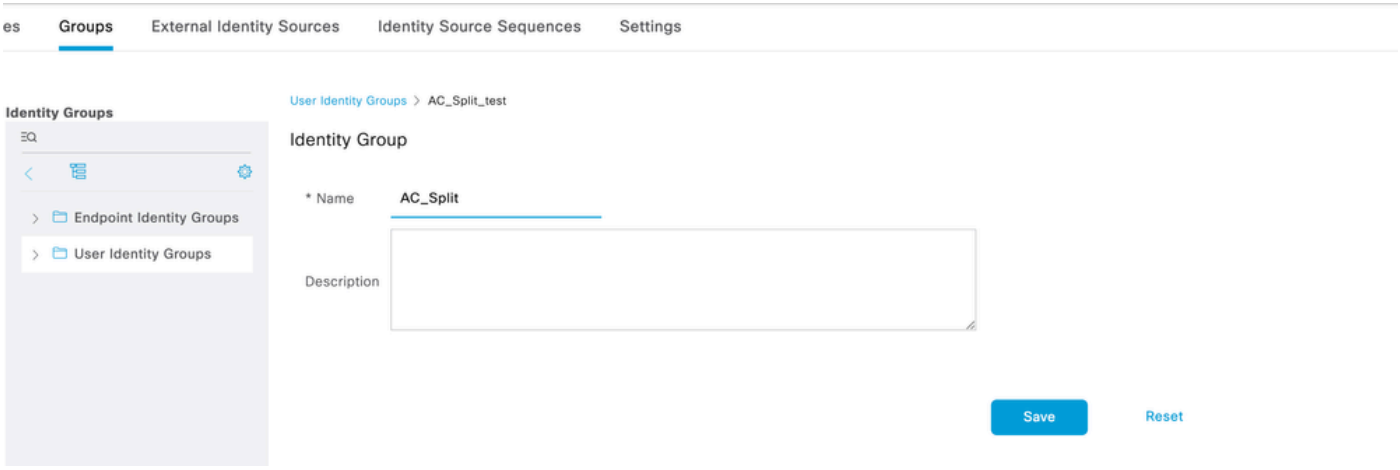
1. Registre el router como un dispositivo de red válido en ISE y configure la clave secreta compartida para RADIUS. Para esto, navegue hasta Administración > Recursos de red > Dispositivos de red. Haga clic en Agregar para configurar el router como un cliente AAA:



Agregar dispositivo de red

2. Crear grupos de identidad:

Defina grupos de identidad para asociar usuarios con características similares y que compartan permisos similares. Estos se utilizan en los siguientes pasos. Vaya a Administration > Identity Management > Groups > User Identity Groups, luego haga clic en Add:



Crear grupo de identidades

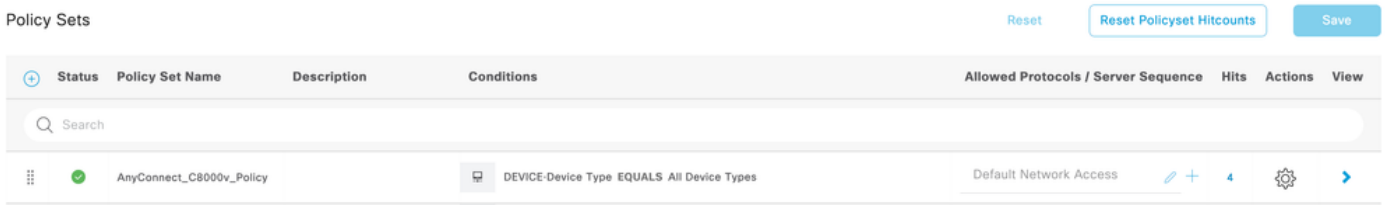
3. Asociar usuarios a grupos de identidad:

Asocie usuarios al grupo de identidad correcto. Vaya a Administration > Identity Management > Identities > Users.

Agregar usuario al grupo de identidades

4. Crear conjunto de políticas:

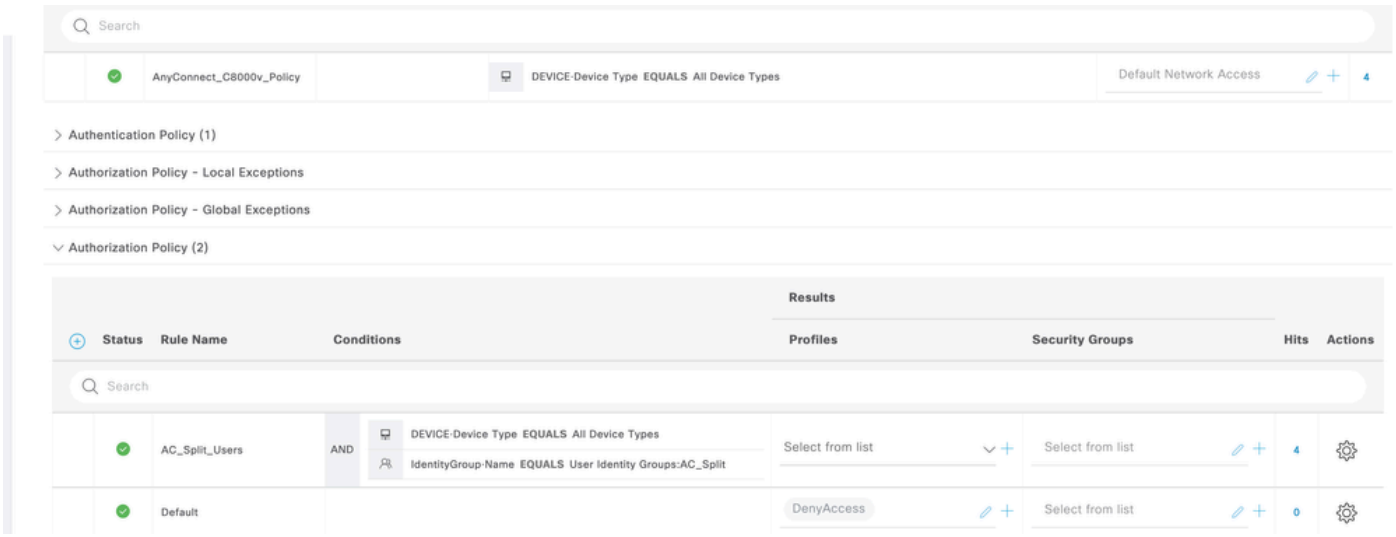
Defina un nuevo conjunto de directivas y las condiciones que coincidan con la directiva. En este ejemplo, se permiten todos los tipos de dispositivos en las condiciones indicadas. Para ello, navegue hasta Política>Conjuntos de políticas:



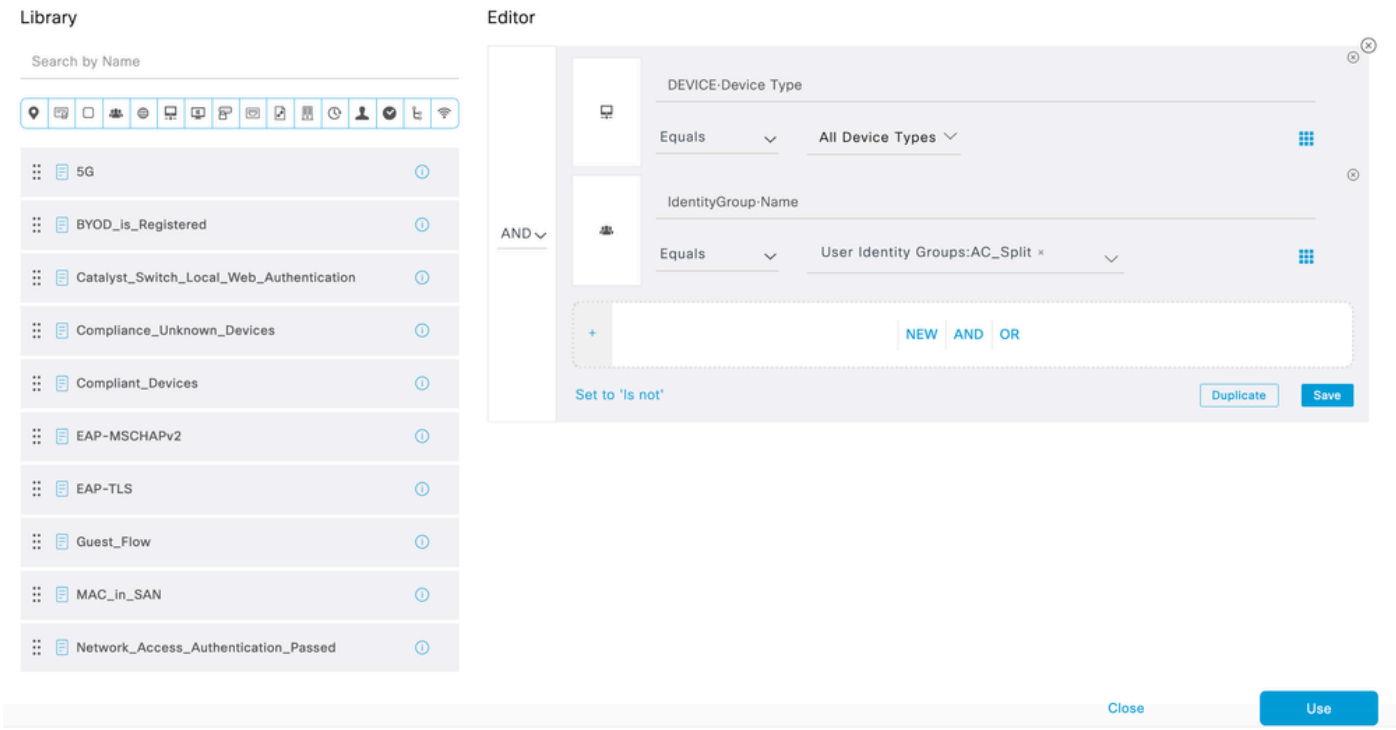
Crear conjunto de políticas

5. Cree una política de autorización:

Defina una nueva directiva de autorización con las condiciones necesarias para que coincida con la directiva. Asegúrese de incluir como condición los grupos de identidad creados en el paso 2.



Crear directiva de autorización

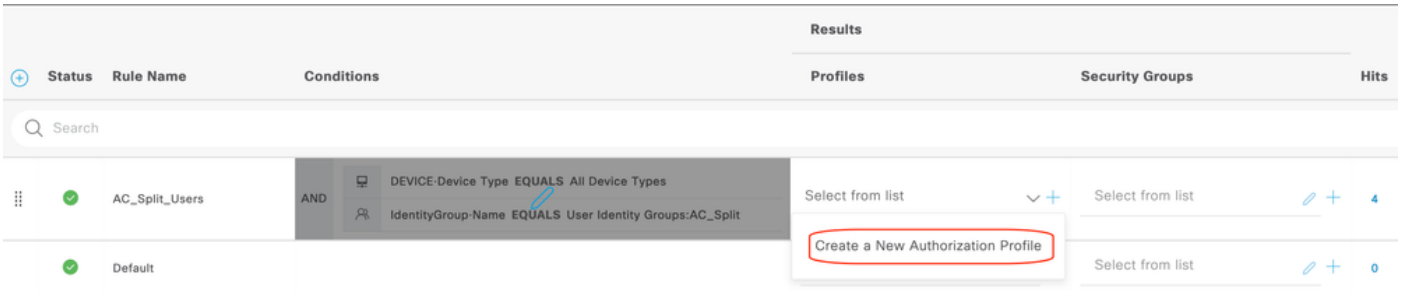


Elegir condiciones en la directiva de autorización

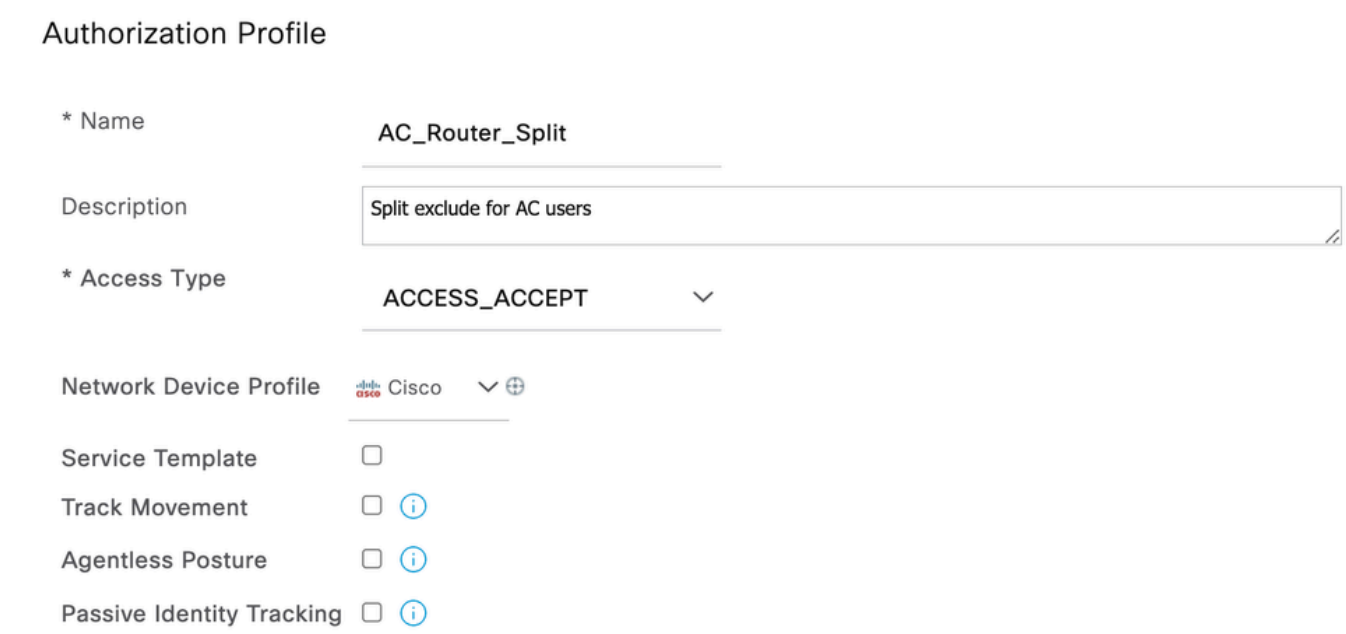
6. Cree un perfil de autorización:

El perfil de autorización incluye las acciones que se llevan a cabo cuando coincide la directiva de autorización. Cree un nuevo perfil de autorización que incluya los siguientes atributos:

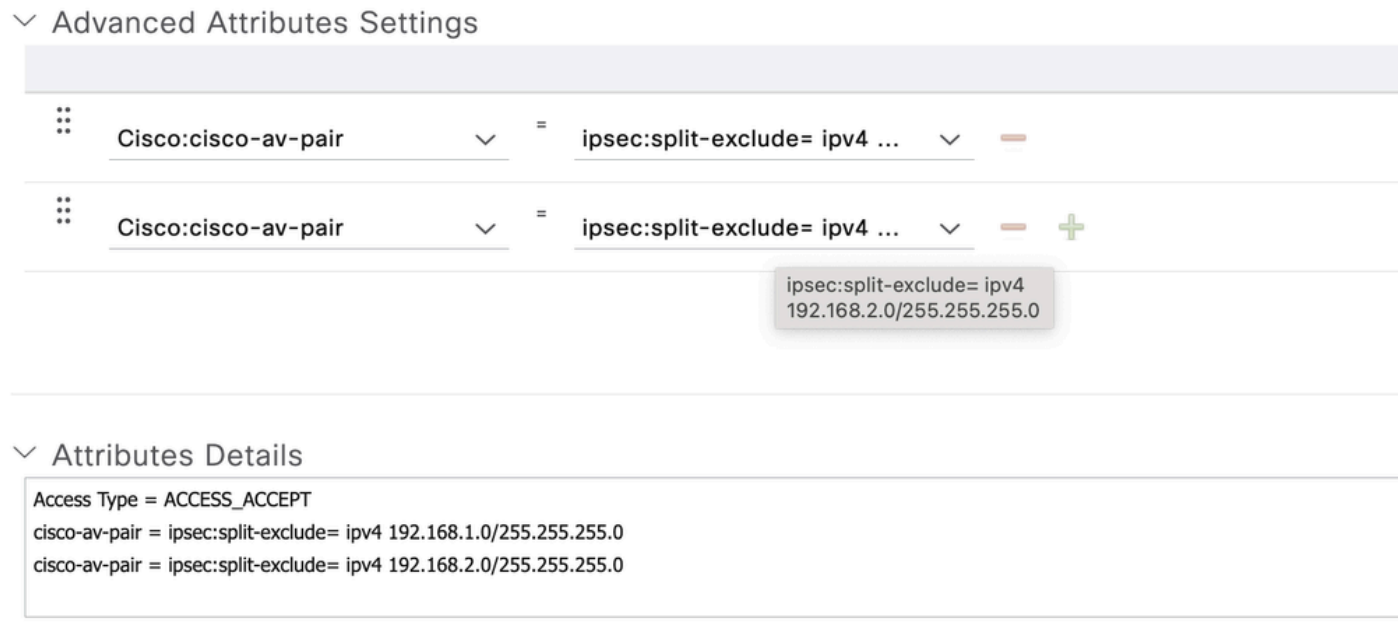
Tipo de acceso = ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <ip_network>/<subnet_mask>



Crear nuevo perfil de autorización

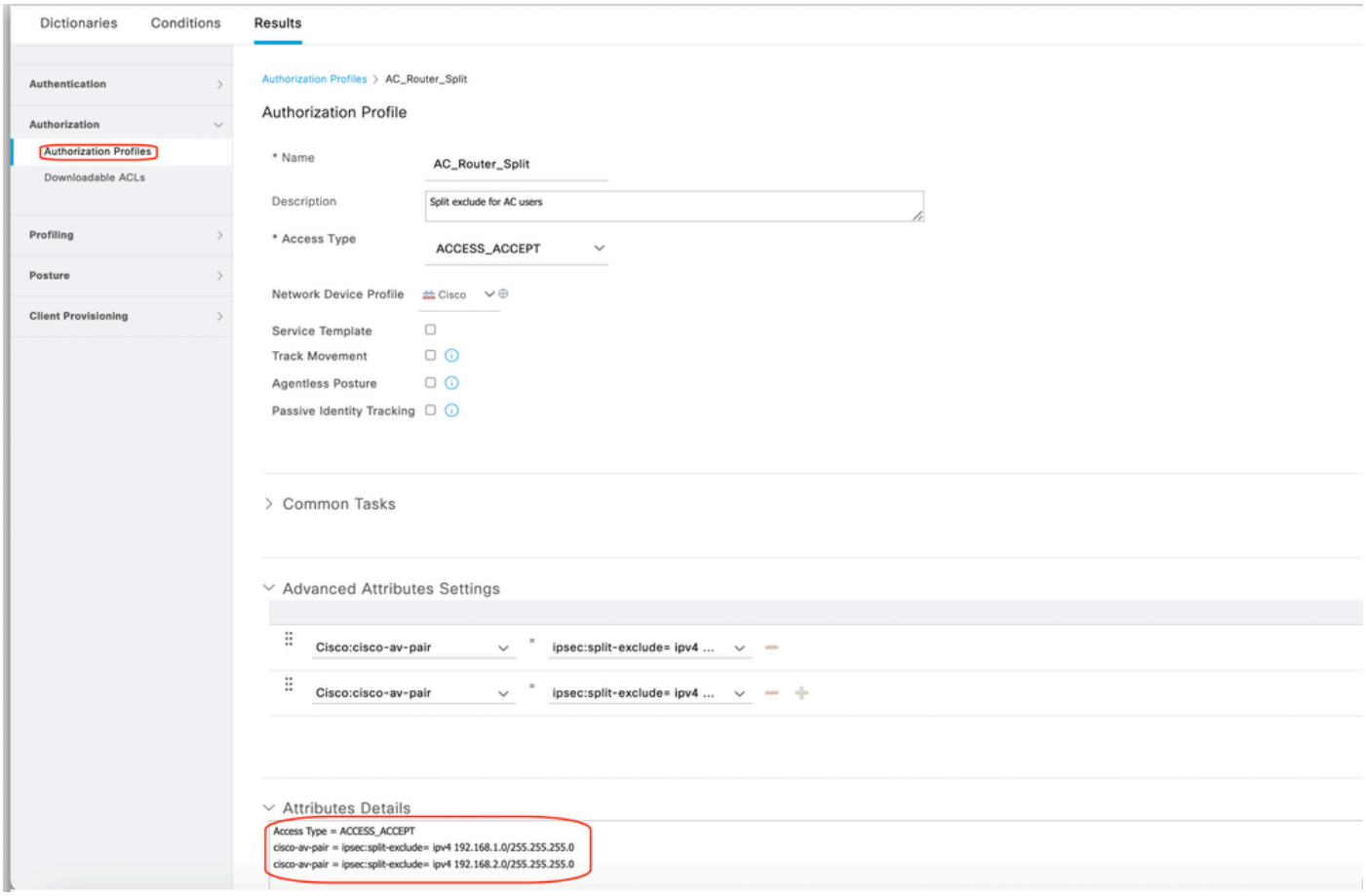


Configuración del perfil de autorización



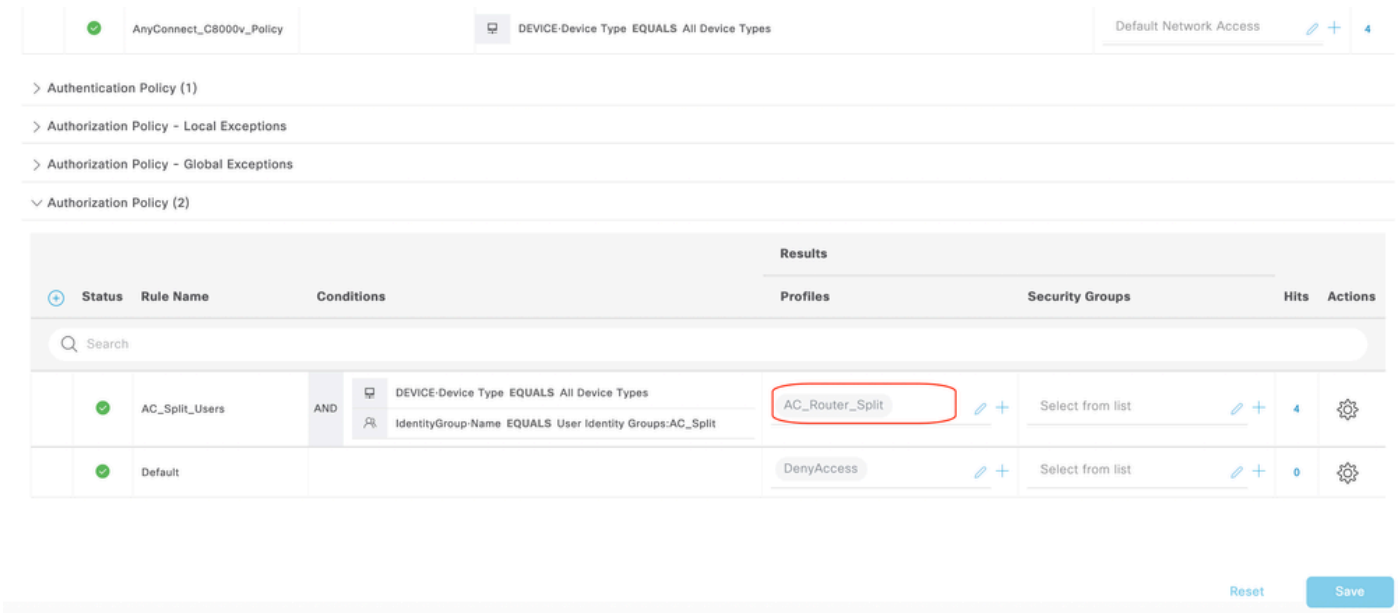
Configurar atributos en el perfil de autorización

7. Revise la configuración del perfil de autorización.



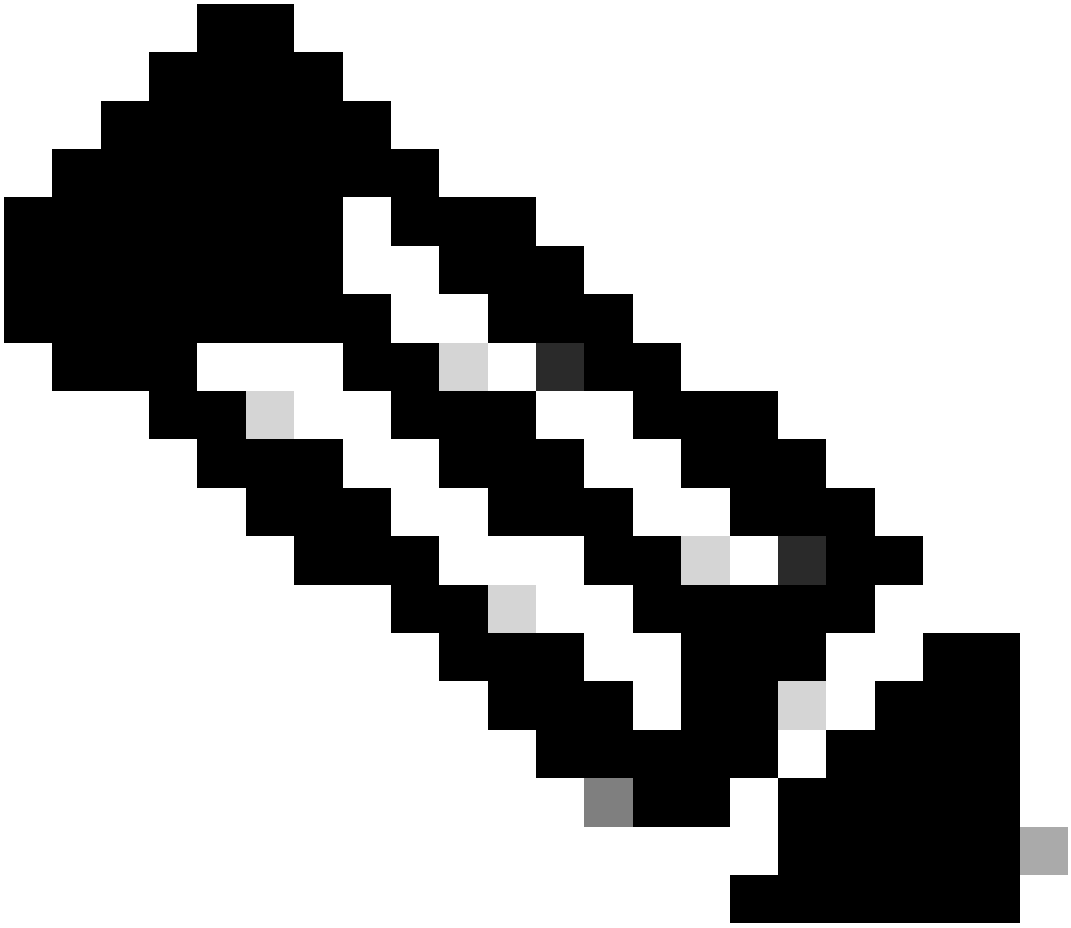
Revisar la configuración del perfil de autorización

8. Esta es la política de autorización en la configuración del conjunto de políticas después de seleccionar los perfiles necesarios:



Configuración final de la política de autorización

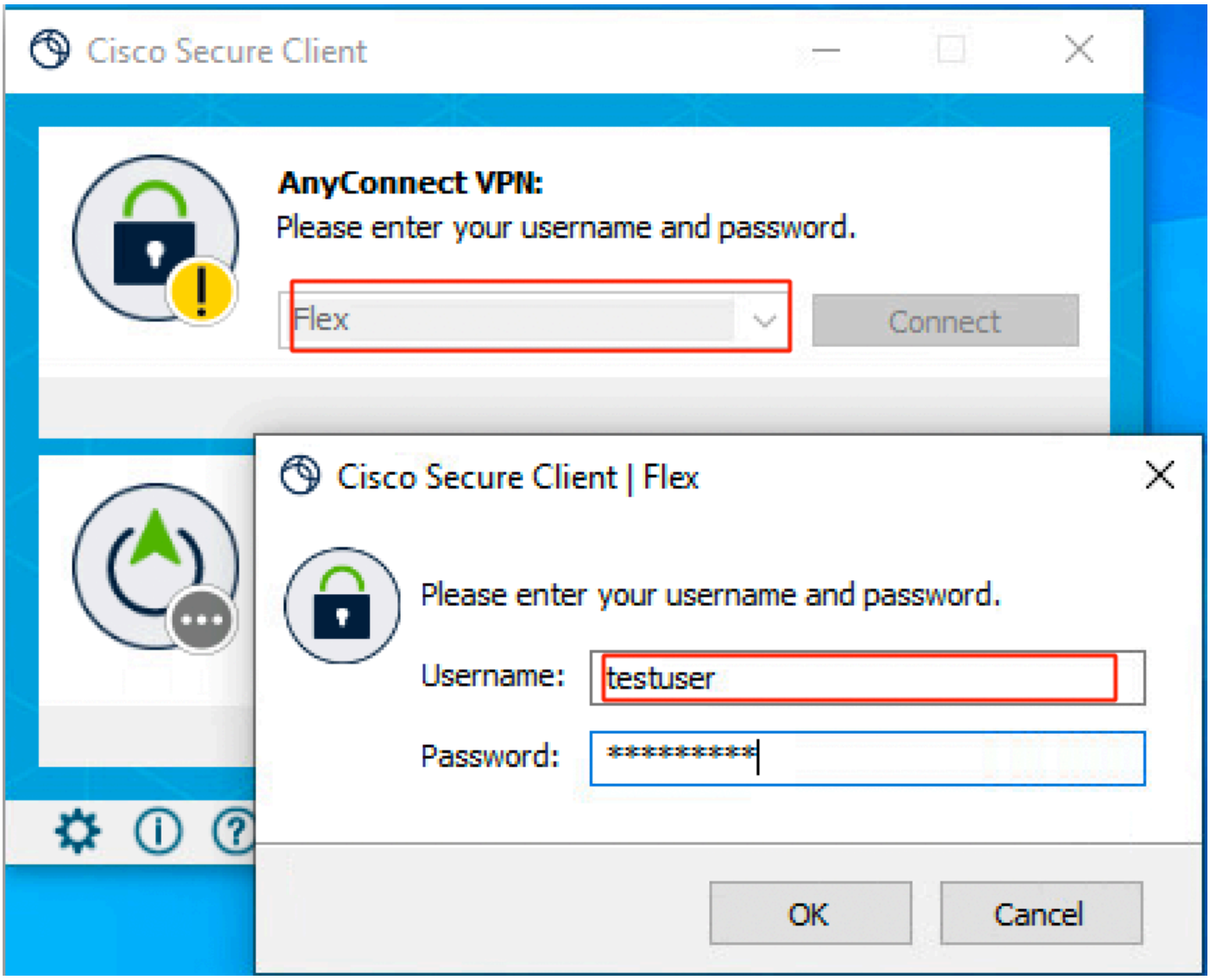
Con este ejemplo de configuración, puede excluir redes para que no pasen a través de VPN a través de la configuración de ISE en función del grupo de identidad al que pertenece el usuario.



Nota: Sólo se puede enviar una subred de exclusión dividida al equipo cliente cuando se usa la cabecera Cisco IOS XE para una conexión VPN de RA. Esto se ha solucionado con el Id. de error de Cisco CSCwj38106 y se pueden enviar varias subredes de exclusión dividida desde 17.12.4. Consulte el error para obtener más detalles sobre las versiones fijas.

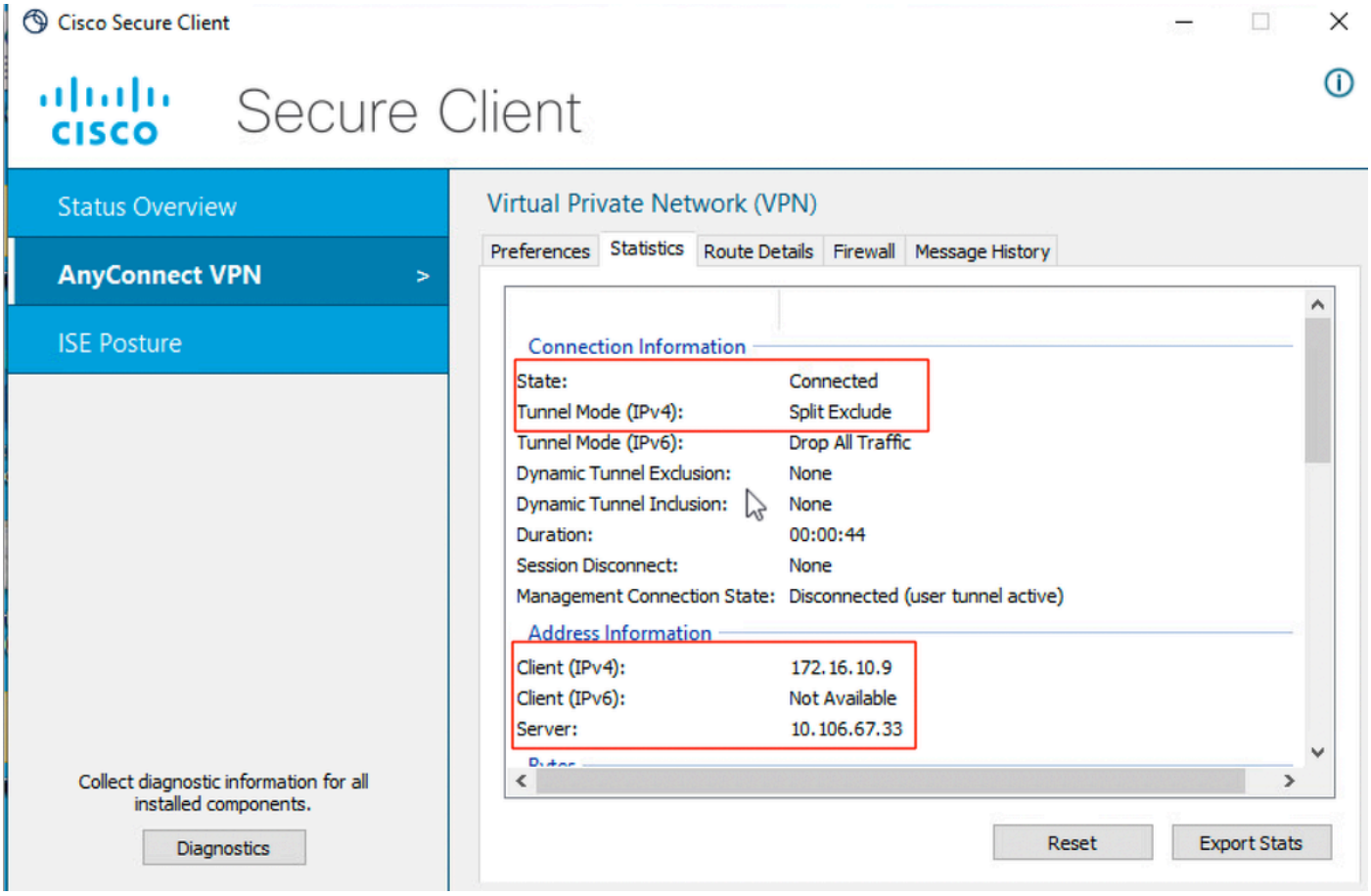
Verificación

1. Para probar la autenticación, conéctese al C8000V desde el equipo del usuario a través de AnyConnect e ingrese las credenciales.



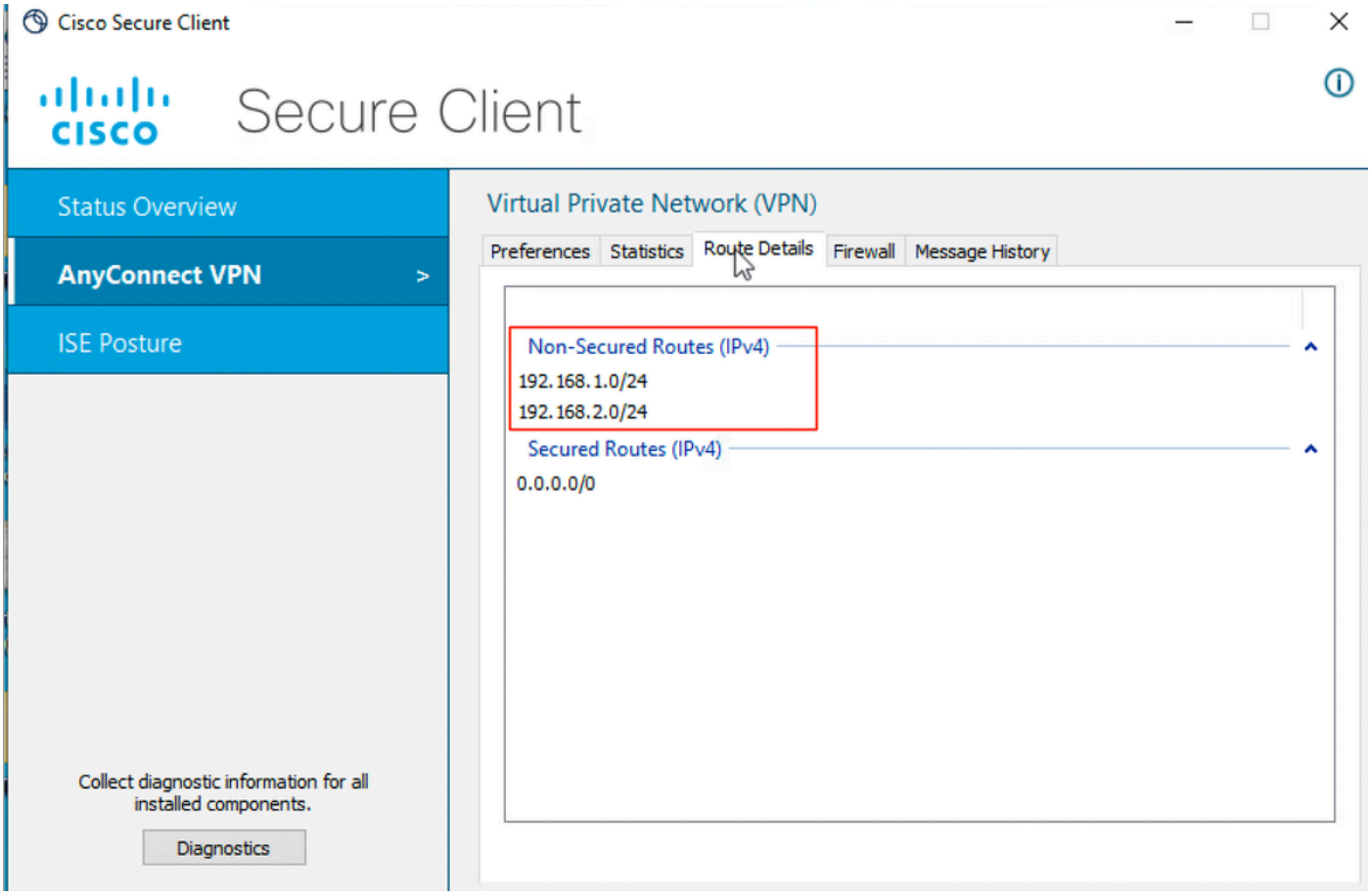
Inicio de sesión en AnyConnect

2. Una vez establecida la conexión, haga clic en el icono de engranaje (esquina inferior izquierda) y navegue hasta AnyConnect VPN > Statistics. Confirme que el modo de túnel se debe dividir o excluir.



Validar las estadísticas

Navegue hasta AnyConnect VPN > Route details y confirme que la información mostrada corresponde a las rutas seguras y las rutas no seguras.



Validar los detalles de la ruta

También puede verificar los detalles de conexión en la cabecera de 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.

Troubleshoot

En el router de Cisco:

1. Utilice los debugs IKEv2 e IPsec para verificar la negociación entre el headend y el cliente.

```
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. Utilice los debugs AAA para verificar la asignación de atributos locales y/o remotos.

```
debug aaa authorization
```

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

En ISE:

Utilice los registros en directo de RADIUS navegando hasta Operaciones > Registros en directo.

Escenario de trabajo

Esta es la depuración de la conexión exitosa:

<#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#
```

Referencias

- Configuración del equipo de cabecera FlexVPN para el acceso remoto IKEv2 mediante la base de datos de usuarios locales
- Configuración de AnyConnect Flexvpn con autenticación EAP y DUO
- Configuración del acceso remoto IKEv2 de AnyConnect con EAP-MD5

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).