Configurazione della funzione Split Exclude per AnyConnect FlexVPN con ISE

Sommario

Introduzione

In questo documento viene descritta la procedura per configurare la funzione split-exclude con ISE per la connessione IKEv2 AnyConnect a un router Cisco IOS® XE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Esperienza con la configurazione di AnyConnect IPsec su un router
- Configurazione Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocollo RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 8000V (C800V) - 17.12.04
- Cisco Secure Client - 5.0.2075
- Cisco ISE - 3.2.0
- Windows 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Esempio di rete

Configurazioni

Per completare la configurazione, prendere in considerazione le sezioni seguenti.

Configurazione del router

1. Configurare un server RADIUS per l'autenticazione e l'autorizzazione locale sul 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. Configurare un trust point per installare il certificato del router. Poiché l'autenticazione locale del router è di tipo RSA, il dispositivo richiede che il server si autentichi utilizzando un certificato. È possibile fare riferimento a Registrazione certificato per PKI -1 e Registrazione certificato per PKI -2 per ulteriori dettagli sulla creazione del certificato:

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

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

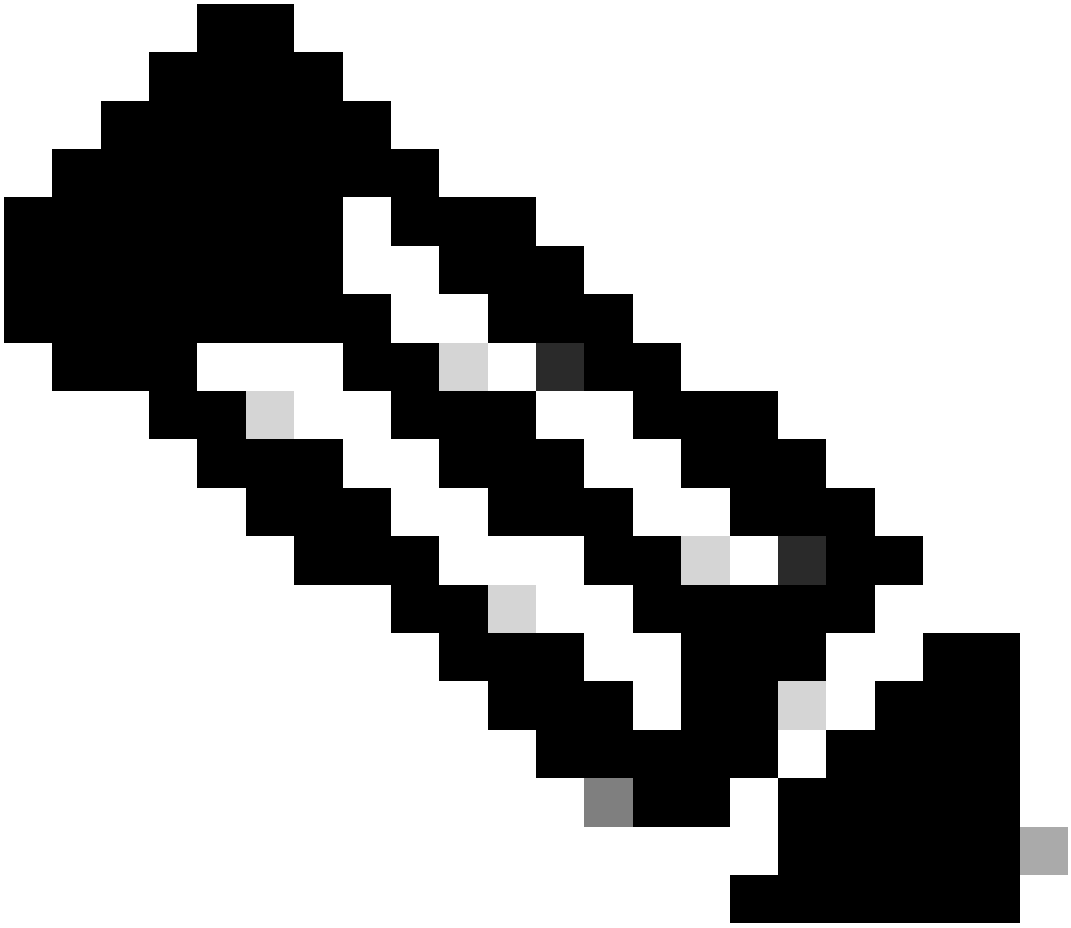
3. Definire un pool locale IP per assegnare gli indirizzi ai client VPN AnyConnect quando la connessione AnyConnect viene stabilita:

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

4. Creare un criterio di autorizzazione locale IKEv2:

Agli utenti vengono applicati gli attributi definiti in questo criterio insieme agli attributi sottoposti a push dal server Radius

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



Nota: Se il criterio di autorizzazione IKEv2 personalizzato non è configurato, per l'autorizzazione verrà utilizzato il criterio di autorizzazione predefinito predefinito. Gli attributi specificati nel criterio di autorizzazione IKEv2 possono inoltre essere sottoposti a push tramite il server RADIUS. Eseguire il push dell'attributo split-exclude dal server RADIUS.

5 (facoltativo). Crea una proposta e un criterio IKEv2 (se non configurati, vengono utilizzati i valori predefiniti intelligenti):

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

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

6 (Facoltativo). Configurare il transform-set (se non è configurato, vengono utilizzati i valori predefiniti intelligenti):

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

7. Configurare un'interfaccia di loopback con un indirizzo IP fittizio. Le interfacce di accesso virtuale prendono in prestito l'indirizzo IP da esso:

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

8. Configurare un modello virtuale da cui vengono clonate le interfacce di accesso virtuale:

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

9. Caricare il profilo del client AnyConnect nella memoria flash del router e definire il profilo come indicato:

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

10. Configurare un profilo IKEv2 contenente tutte le informazioni relative alla connessione:

```
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
```

Questi elementi vengono utilizzati nel profilo IKEv2:

- match identity id-chiave remota *$AnyConnectClient$*: si riferisce all'identità del client. AnyConnect utilizza *$AnyConnectClient$* come identità IKE predefinita di tipo id-chiave. Tuttavia, è possibile modificare manualmente l'identità nel profilo AnyConnect in base alle esigenze di distribuzione.
- autenticazione remota: indica che il protocollo EAP deve essere utilizzato per l'autenticazione del client.
- autenticazione locale: indica che i certificati devono essere utilizzati per l'autenticazione locale.
- aaa authentication eap: durante l'autenticazione EAP, viene utilizzato il server RADIUS FlexVPN_auth.
- aaa authorization group eap list - Durante l'autorizzazione, l'elenco di rete a-eap-author-grp utilizzato con il criterio di autorizzazione ikev2-auth-policy.
- aaa authorization user eap cached: abilita l'autorizzazione utente implicita.
- virtual-template 100: definisce il modello virtuale da duplicare.
- anyconnect profile acvpn: il profilo client definito nel passaggio 9. viene applicato a questo profilo IKEv2.

11. Configurare il profilo IPSec:

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

12. Aggiungere il profilo IPSec al modello virtuale:

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

13. Disabilitare la ricerca del certificato basata su URL HTTP e il server HTTP sul router:

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

14. Configurare il criterio SSL e specificare l'IP WAN del router come indirizzo locale per il download del profilo:

```
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
```

Frammento di codice di AnyConnect Client Profile (profilo XML):

Nelle versioni precedenti a Cisco IOS XE 16.9.1, il download automatico del profilo dall'headend non è disponibile. Dopo 16.9.1, è possibile scaricare il profilo dall'headend.

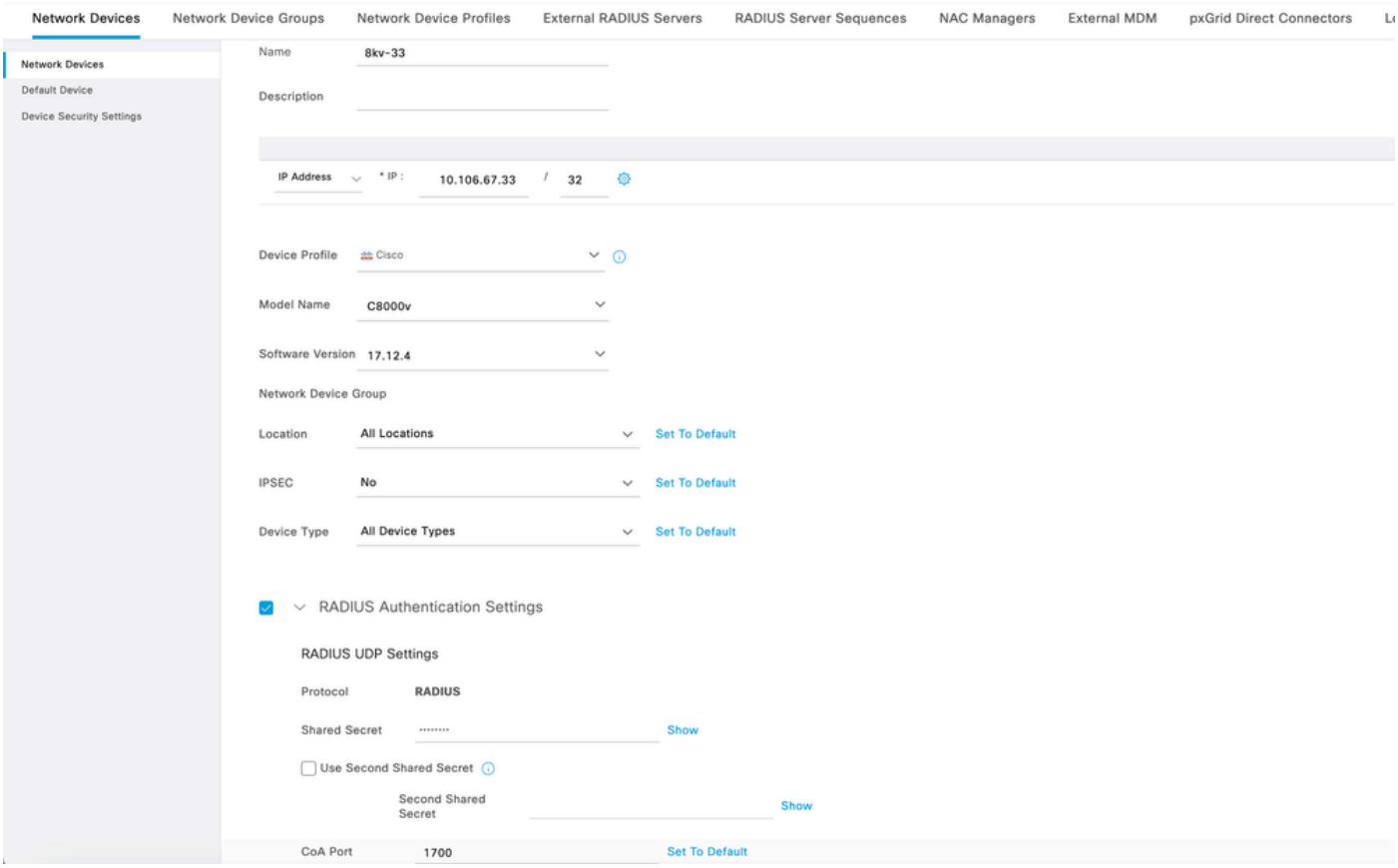
<#root>

```
<?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>
```

Configurazione Identity Services Engine (ISE)

1. Registrare il router come dispositivo di rete valido su ISE e configurare la chiave privata condivisa per RADIUS. A tale scopo, selezionare Amministrazione > Risorse di rete > Dispositivi di rete. Fare clic su Aggiungi per configurare il router come client AAA:

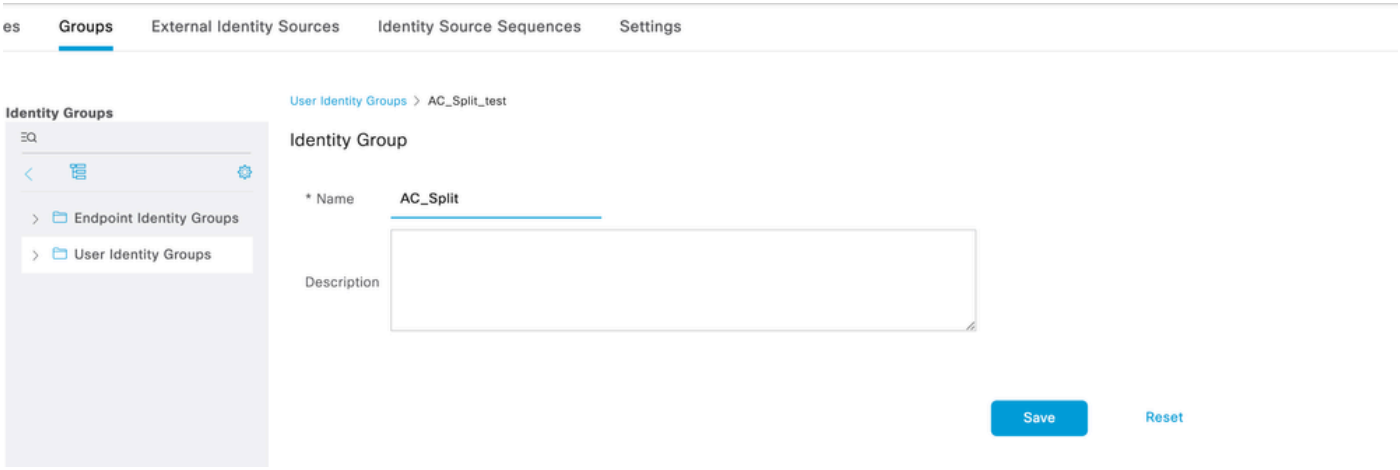


Aggiungi dispositivo di rete

2. Creare gruppi di identità:

Definire i gruppi di identità per associare utenti con caratteristiche simili e che condividono autorizzazioni simili. Queste opzioni verranno utilizzate nei passaggi successivi. Passare a

Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente, quindi fare clic su Aggiungi:



Crea gruppo di identità

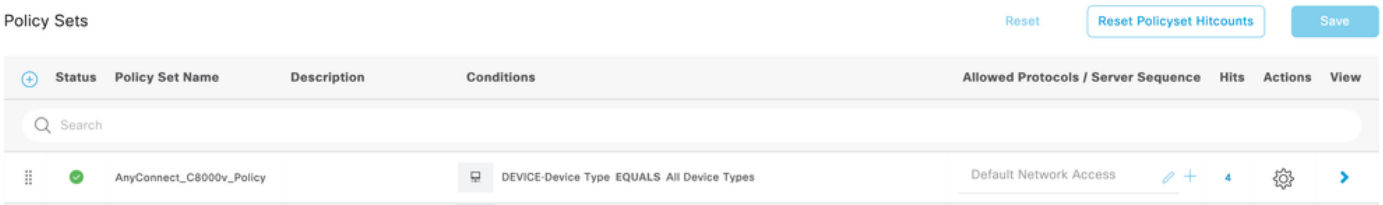
3. Associare gli utenti ai gruppi di identità:

Associare gli utenti al gruppo di identità corretto. Passare ad Amministrazione > Gestione delle identità > Identità > Utenti.

Aggiungi utente a gruppo di identità

4. Crea set di criteri:

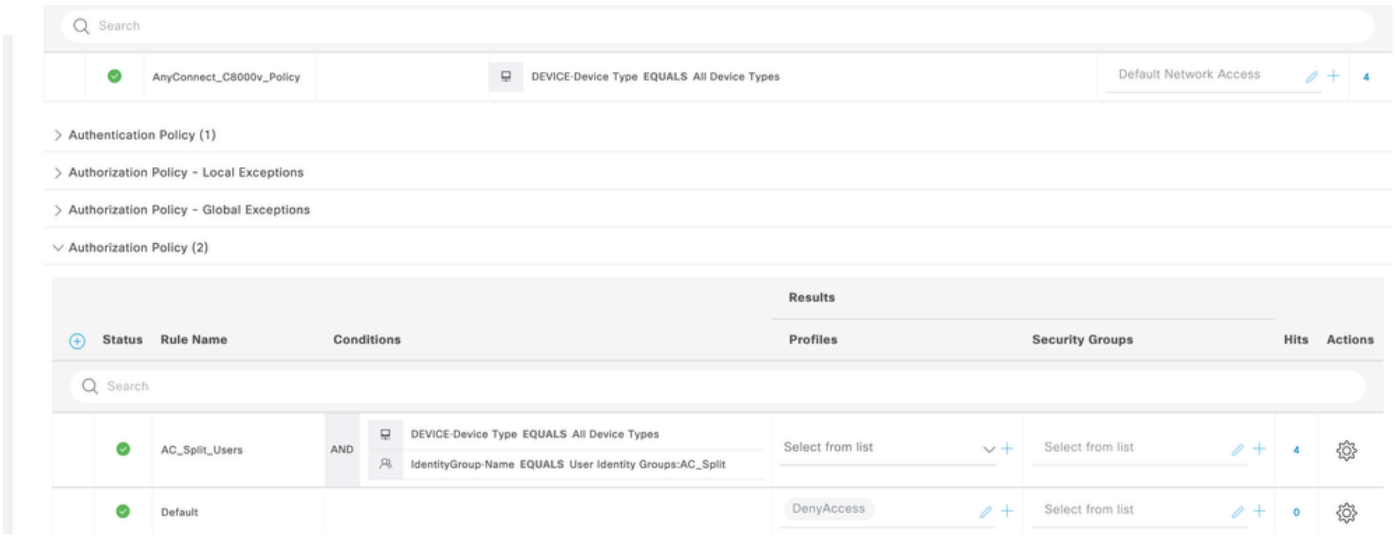
Definire un nuovo set di criteri e definire le condizioni che soddisfano il criterio. In questo esempio, tutti i tipi di dispositivi sono consentiti in queste condizioni. A tale scopo, passare a Criterio>Set di criteri:



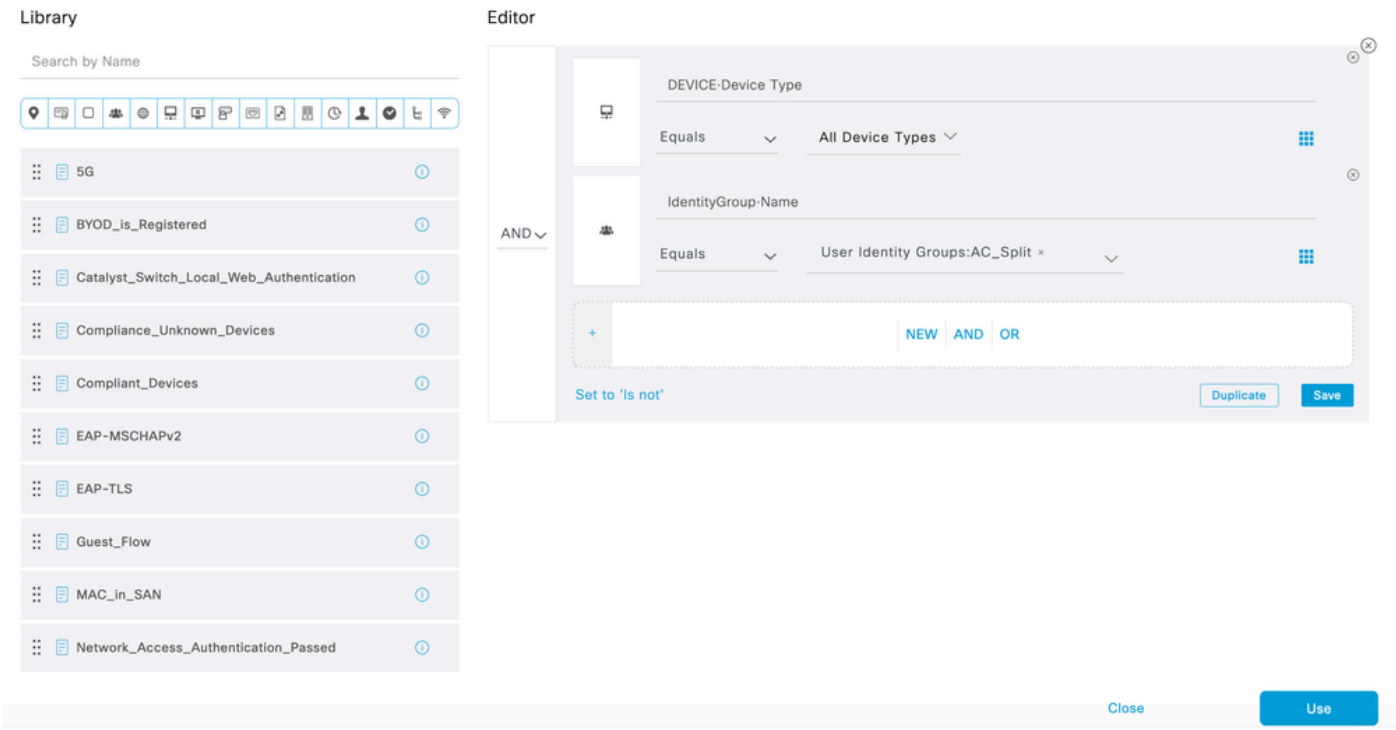
Crea set di criteri

5. Creare un criterio di autorizzazione:

Definire un nuovo criterio di autorizzazione con le condizioni necessarie per soddisfare il criterio. Assicurarsi di includere i gruppi di identità creati nel passaggio 2 come condizione.



Crea criterio di autorizzazione

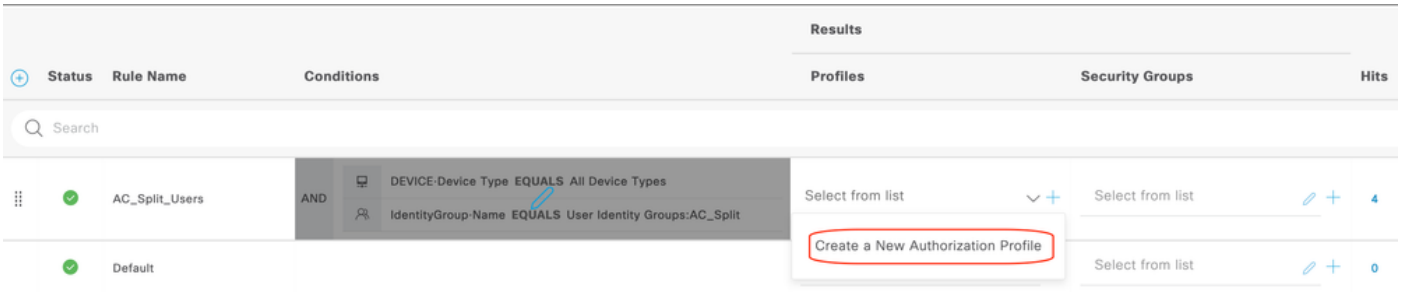


Scegliere le condizioni nei criteri di autorizzazione

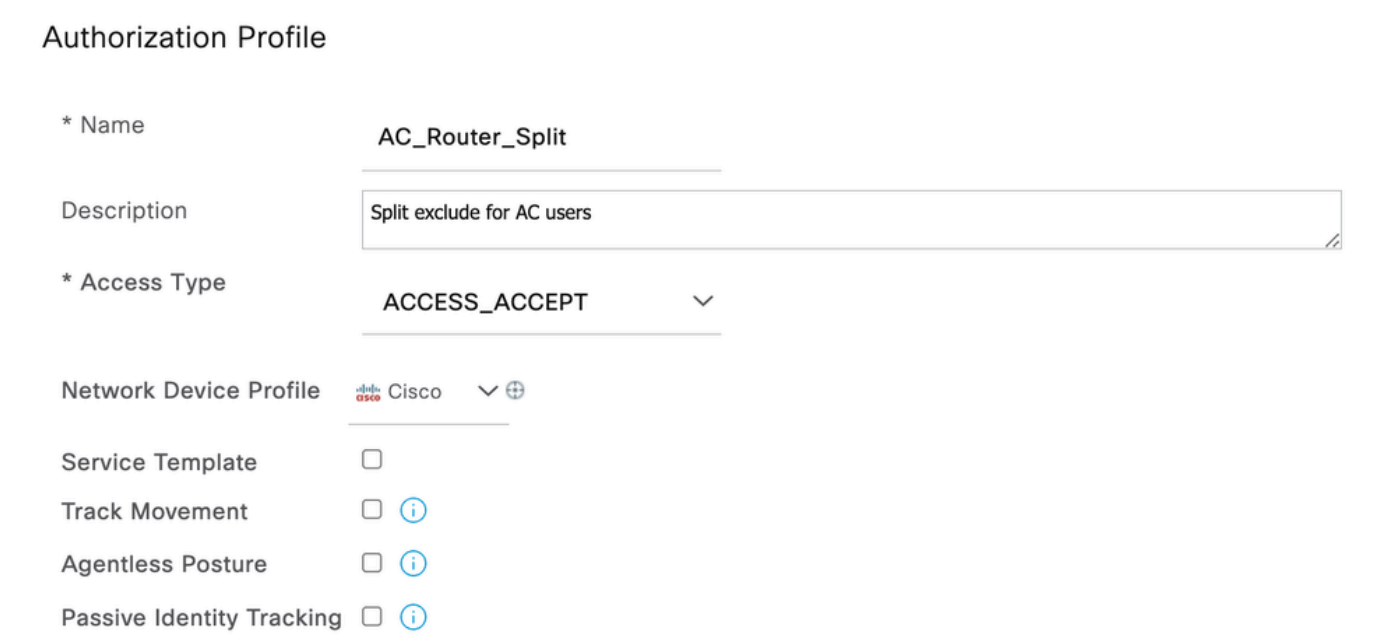
6. Creare un profilo di autorizzazione:

Il profilo di autorizzazione include le azioni eseguite quando viene stabilita una corrispondenza con i criteri di autorizzazione. Creare un nuovo profilo di autorizzazione che includa gli attributi seguenti:

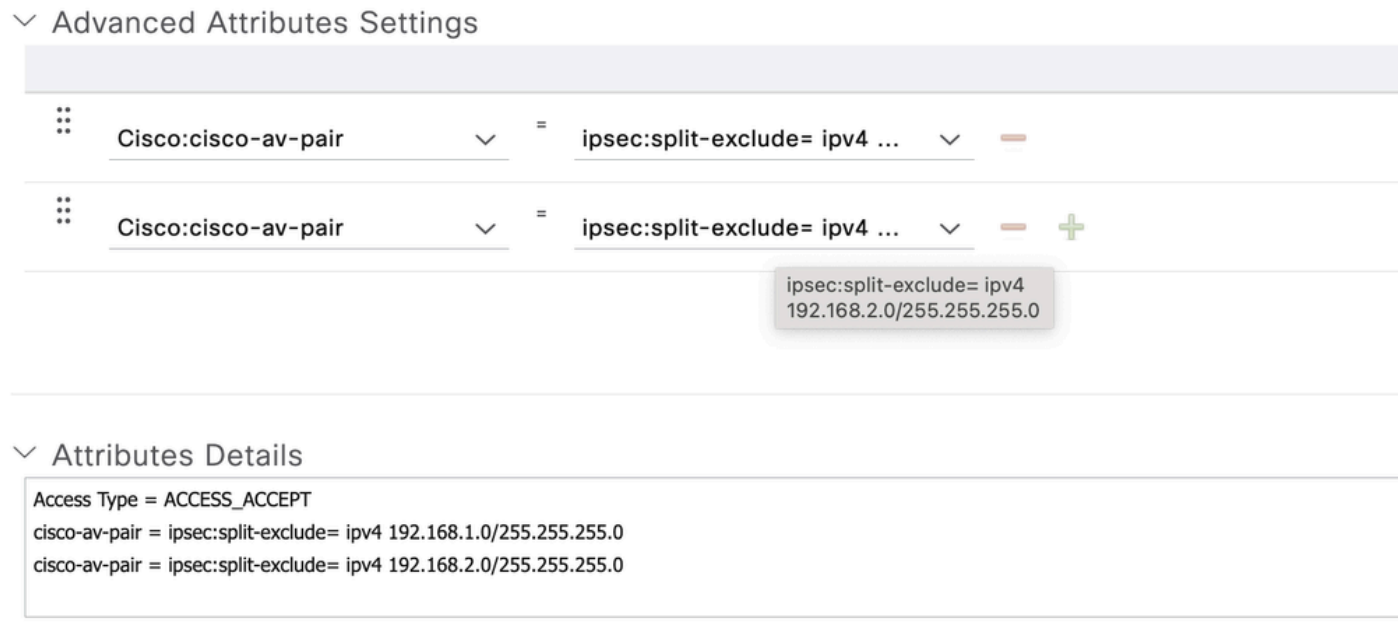
Tipo di accesso = ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <rete_ip>/<subnet_mask>



Crea nuovo profilo di autorizzazione

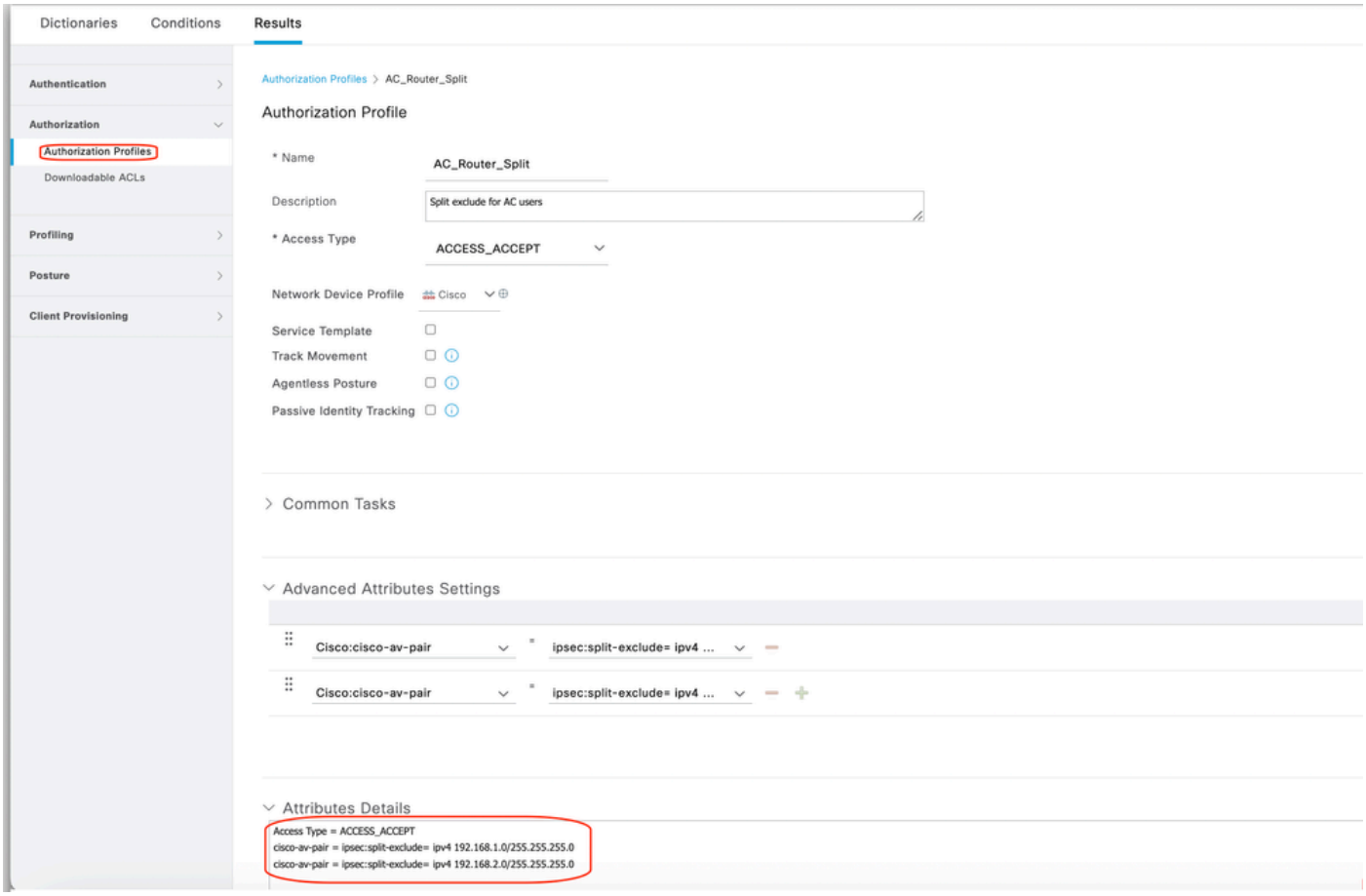


Configurazione profilo di autorizzazione



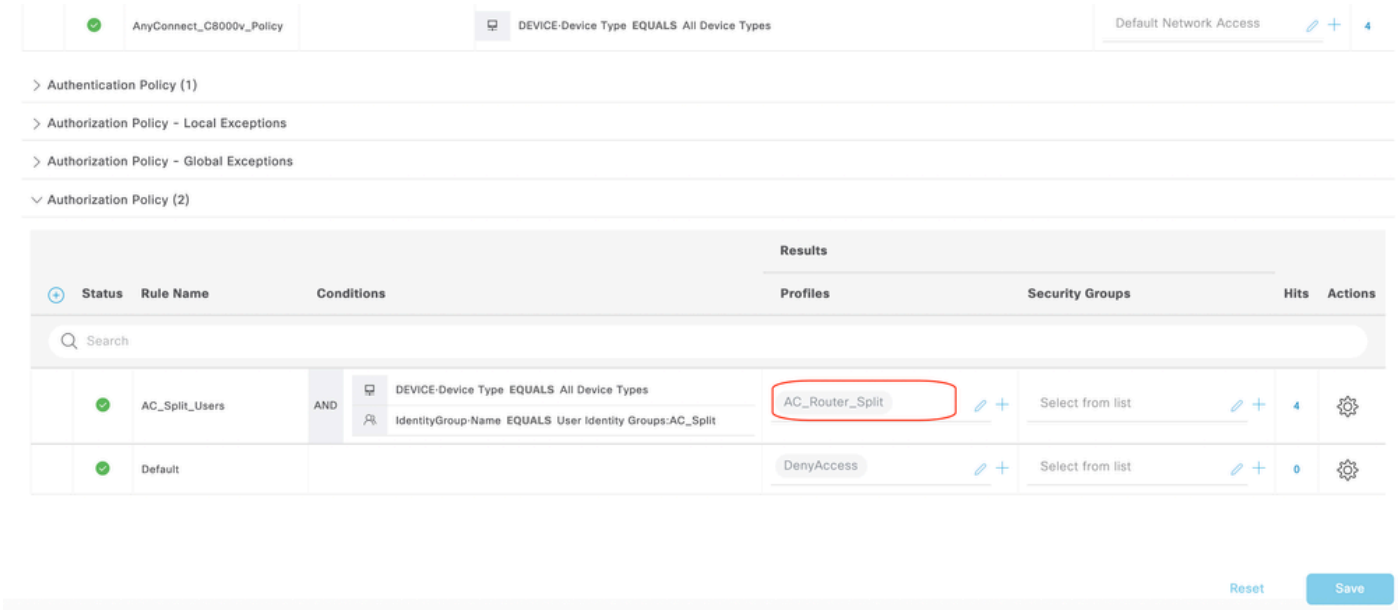
Configura attributi nel profilo di autorizzazione

7. Verificare la configurazione del profilo di autorizzazione.



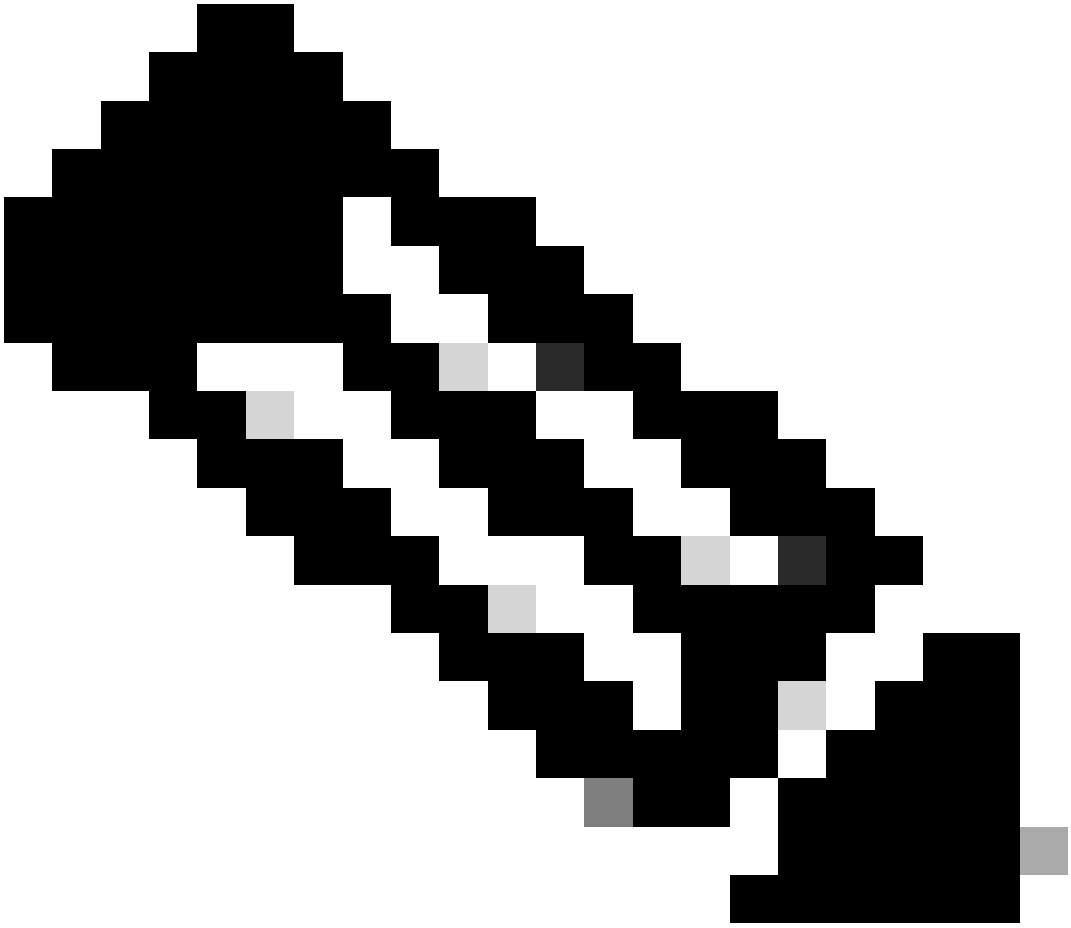
Verifica configurazione profilo di autorizzazione

8. Questo è il criterio di autorizzazione nella configurazione del set di criteri dopo aver selezionato i profili richiesti:



Configurazione finale dei criteri di autorizzazione

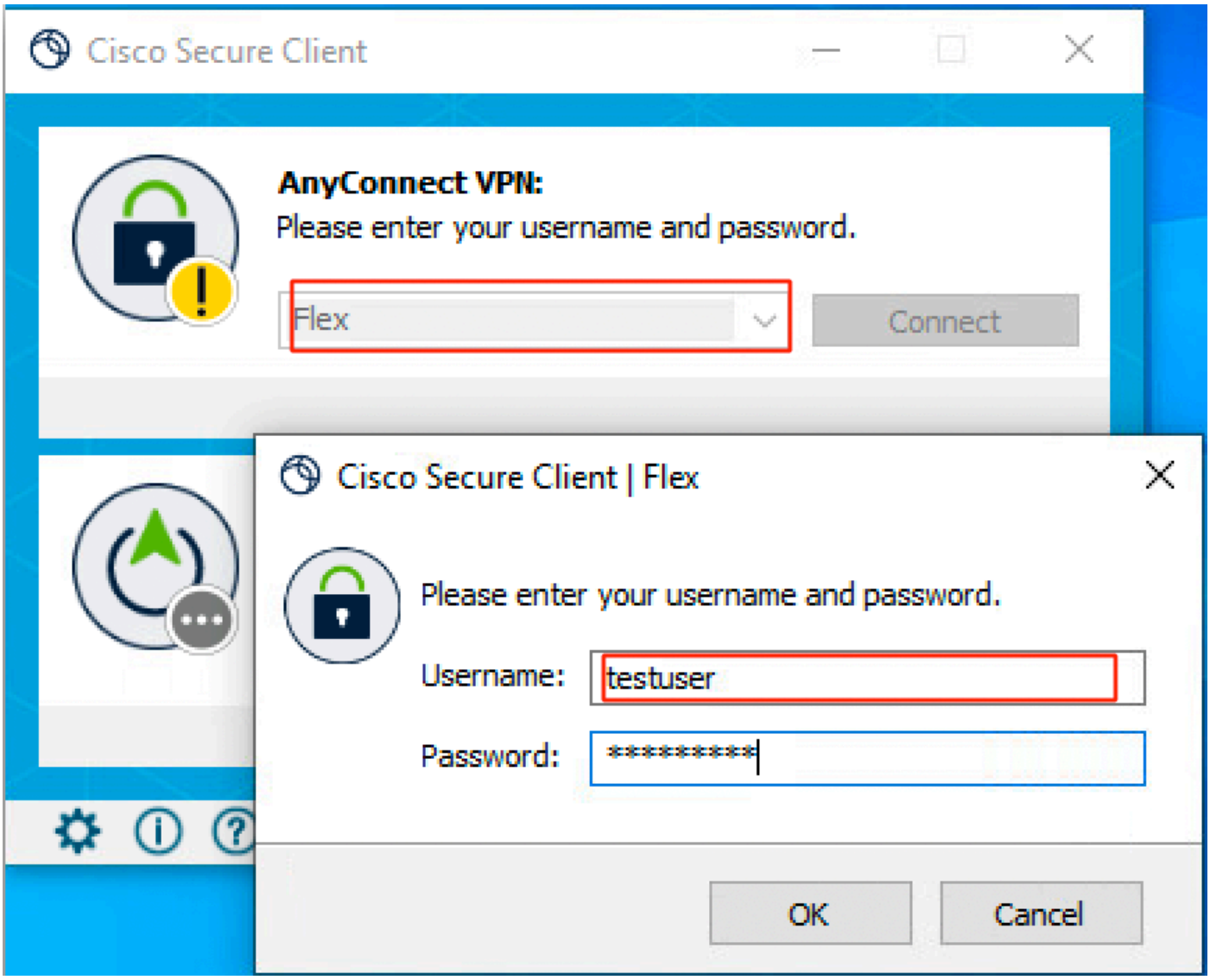
Con questo esempio di configurazione, è possibile escludere le reti dal passaggio attraverso la VPN tramite la configurazione ISE in base al gruppo di identità a cui appartiene l'utente.



Nota: Quando si usa l'headend Cisco IOS XE per una connessione VPN RSA, è possibile eseguire il push di una sola subnet split-exclude nel PC client. Questa condizione è stata risolta dall'ID bug CSCwj38106 e è possibile eseguire il push di più subnet split-exclude a partire dalla versione 17.12.4. Fare riferimento al bug per ulteriori dettagli sulle versioni fisse.

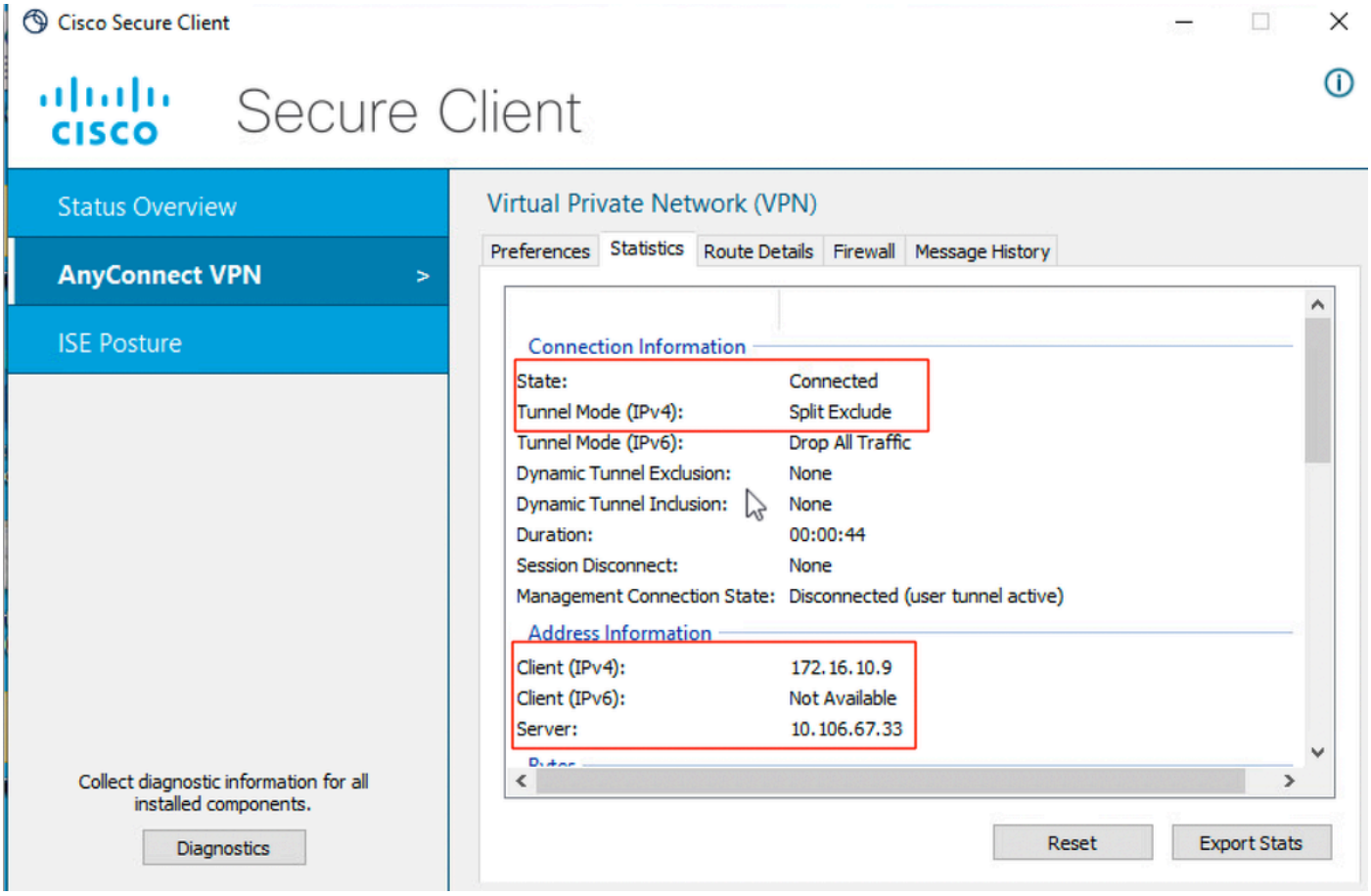
Verifica

1. Per verificare l'autenticazione, connettersi al C8000V dal PC dell'utente tramite AnyConnect e immettere le credenziali.



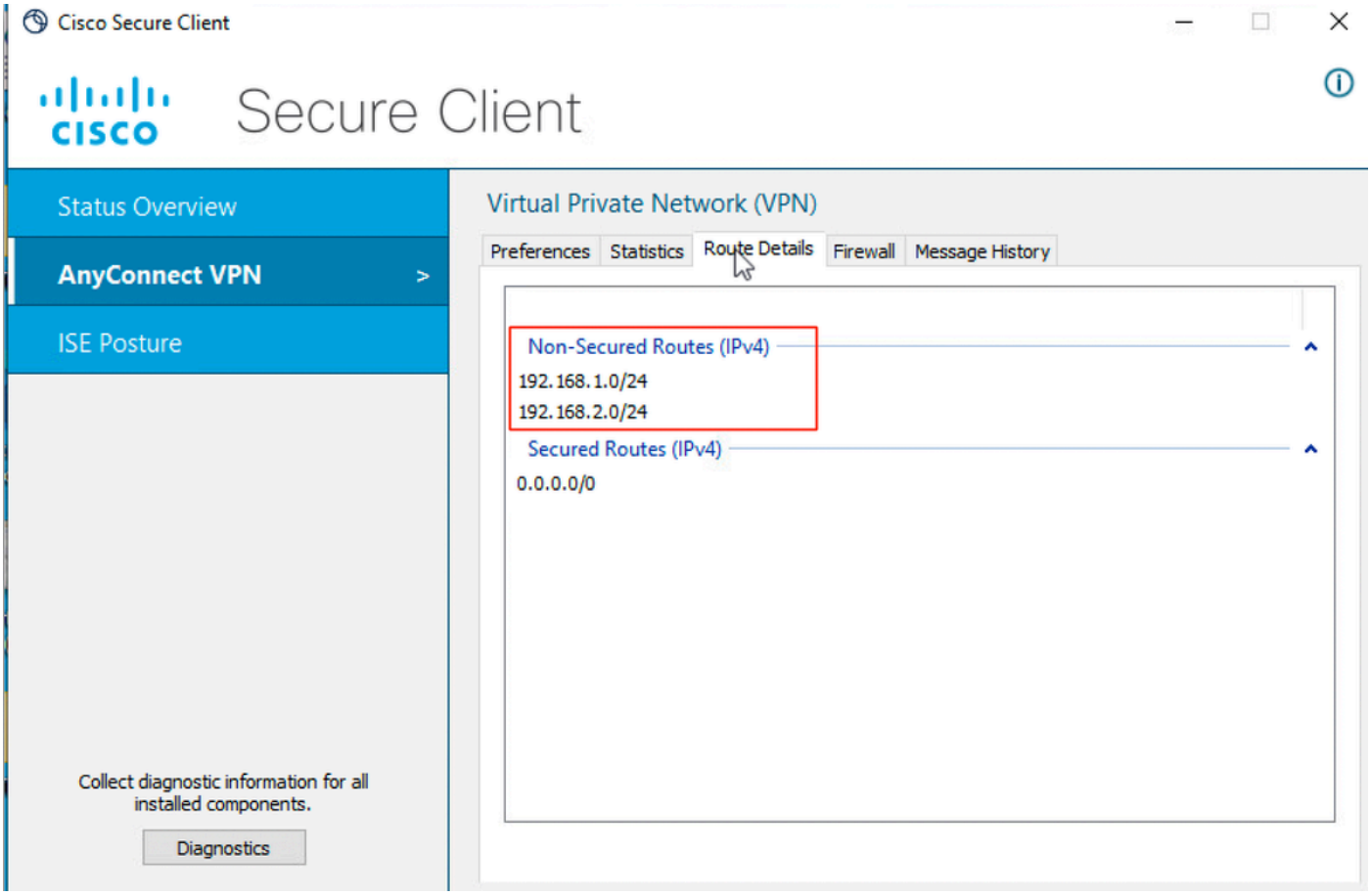
Accedi a AnyConnect

2. Una volta stabilita la connessione, fare clic sull'icona dell'ingranaggio (nell'angolo in basso a sinistra) e selezionare AnyConnect VPN > Statistics. Confermare la modalità tunnel da escludere dalla divisione.



Convalida statistiche

Passare a AnyConnectVPN > Dettagli route e verificare che le informazioni visualizzate corrispondano alle route sicure e a quelle non sicure.



Convalida i dettagli del ciclo di lavorazione

È inoltre possibile verificare i dettagli della connessione sull'headend 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.

Risoluzione dei problemi

Su router Cisco:

1. Utilizzare i debug IKEv2 e IPsec per verificare la negoziazione tra l'headend e il 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. Utilizzare i debug AAA per verificare l'assegnazione degli attributi locali e/o remoti.

```
debug aaa authorization
```

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

ISE:

Utilizzare i log attivi RADIUS selezionando Operazioni > Log attivi.

Scenario di lavoro

Questo è il debug della connessione riuscita:

<#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#
```

Riferimenti

- Configurazione dell'headend FlexVPN per l'accesso remoto IKEv2 tramite il database degli utenti locali
- Configurazione di AnyConnect Flexvpn con autenticazione EAP e DUO
- Configurazione dell'accesso remoto AnyConnect IKEv2 con EAP-MD5

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).