

Configurar a exclusão dividida para AnyConnect FlexVPN usando ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração do roteador](#)

[Configuração do Identity Services Engine \(ISE\)](#)

[Verificar](#)

[Troubleshooting](#)

[Referências](#)

Introdução

Este documento descreve o procedimento para configurar o split-exclude usando ISE para conexão AnyConnect IKEv2 com um roteador Cisco IOS® XE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Experiência com a configuração do AnyConnect IPsec em um roteador
- Configuração do Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocolo RADIUS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Diagrama de Rede

Configurações

Para concluir a configuração, leve em consideração estas seções.

Configuração do roteador

1. Configure um servidor RADIUS para autenticação e autorização local no 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 um ponto confiável para instalar o certificado do roteador. Como a autenticação local do roteador é do tipo RSA, o dispositivo requer que o servidor autentique-se usando um certificado. Você pode consultar [Registro de Certificado para um PKI -1](#) e [Registro de Certificado para um PKI -2](#) para obter mais detalhes sobre a criação do certificado:

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

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

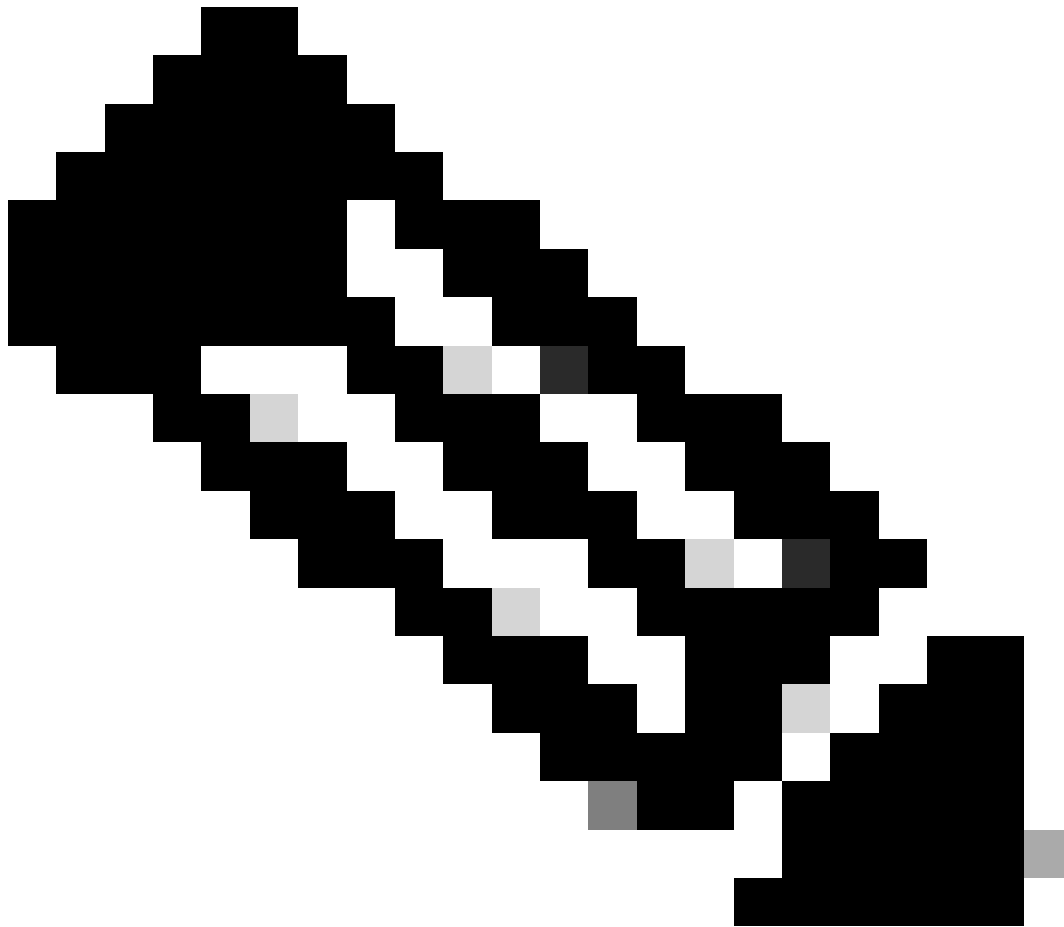
3. Defina um pool IP local para atribuir endereços a clientes AnyConnect VPN em uma conexão bem-sucedida do AnyConnect:

```
ip local pool ACP00L 172.16.10.5 172.16.10.30
```

4. Crie uma política de autorização local IKEv2:

Os atributos definidos nesta política, juntamente com os atributos enviados do servidor Radius, são aplicados aos usuários

```
crypto ikev2 authorization policy ikev2-auth-policy
pool ACP00L
dns 8.8.8.8
```



Note: Se a política de autorização IKEv2 personalizada não estiver configurada, a política de autorização padrão chamada padrão será usada para autorização. Os atributos especificados na política de autorização IKEv2 também podem ser enviados por meio do servidor RADIUS. Você precisa enviar o atributo split-exclude do servidor RADIUS.

5 (Opcional). Crie uma proposta e uma política IKEv2 (se não estiverem configuradas, serão usados padrões inteligentes):

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

```
crypto ikev2 policy IKEv2-po1
  proposal IKEv2-prop1
```

6 (Opcional). Configure o conjunto de transformação (se não estiver configurado, os padrões inteligentes serão usados):

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

7. Configure uma interface de loopback com algum endereço IP fictício. As interfaces de acesso virtual pegam emprestado o endereço IP:

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

8. Configure um Modelo virtual a partir do qual as interfaces de acesso virtual são clonadas:

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

9. Carregue o perfil do cliente AnyConnect para o flash de inicialização do roteador e defina o perfil conforme indicado:

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

10. Configure um perfil IKEv2 que contenha todas as informações relacionadas à conexão:

```
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
```

Eles são usados no perfil IKEv2:

- match identity remote key-id `*$AnyConnectClient$*` - Refere-se à identidade do cliente. O AnyConnect usa `*$AnyConnectClient$*` como sua identidade IKE padrão do tipo key-id. No entanto, essa identidade pode ser alterada manualmente no perfil do AnyConnect para corresponder às necessidades de implantação.
- authentication remote - Menciona que o protocolo EAP deve ser usado para a autenticação do cliente.
- authentication local - Menciona que os certificados devem ser usados para autenticação local.
- aaa authentication eap - Durante a autenticação EAP, o servidor RADIUS FlexVPN_auth é usado.
- aaa authorization group eap list - Durante a autorização, a lista de rede a-eap-author-grp usada com a política de autorização ikev2-auth-policy.
- aaa authorization user eap cached- Ativa a autorização implícita do usuário.
- virtual-template 100 - Define o modelo virtual a ser clonado.
- anyconnect profile acvpn - O perfil de cliente definido na Etapa 9. é aplicado aqui a este perfil IKEv2.

11. Configure o perfil IPsec:

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

12. Adicione o perfil IPsec ao molde virtual:

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

13. Desative a pesquisa de certificado baseada em URL HTTP e o servidor HTTP no roteador:

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

14. Configure a política SSL e especifique o IP WAN do roteador como o endereço local para fazer download do 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
```

Trecho do Perfil do cliente AnyConnect (Perfil XML):

Antes do Cisco IOS XE 16.9.1, os downloads automáticos de perfil do headend não estavam disponíveis. Após 16.9.1, é possível fazer o download do perfil do 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>  
<PPPEExclusion UserControllable="false">Disable  
<PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>  
</PPPEExclusion>  
<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>

Configuração do Identity Services Engine (ISE)

1. Registre o roteador como um dispositivo de rede válido no ISE e configure a chave secreta compartilhada para o RADIUS. Para isso, navegue para Administração > Recursos de rede > Dispositivos de rede. Clique em Adicionar para configurar o roteador como um cliente AAA:

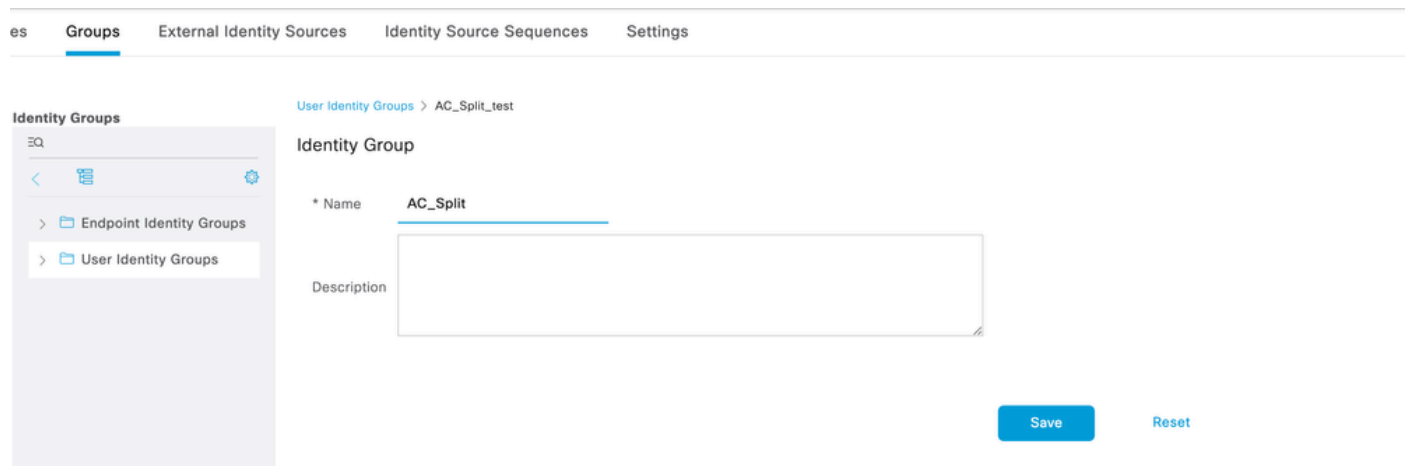
The screenshot shows the 'Network Devices' configuration page in Cisco ISE. The left sidebar has 'Network Devices' selected. The main area shows configuration for a device named '8kv-33'. Fields include: Name (8kv-33), Description, IP Address (10.106.67.33 / 32), Device Profile (Cisco), Model Name (C8000v), Software Version (17.12.4), Network Device Group, Location (All Locations), IPSEC (No), Device Type (All Device Types), and CoA Port (1700). The 'RADIUS Authentication Settings' section is expanded, showing 'RADIUS UDP Settings' with Protocol set to 'RADIUS', a Shared Secret field, and an option to 'Use Second Shared Secret'.

Adicionar dispositivo de rede

2. Criar grupos de identidade:

Defina grupos de identidade para associar usuários com características semelhantes e que compartilhem permissões semelhantes. Eles são usados nas próximas etapas. Navegue até

Administração > Gerenciamento de identidades > Grupos > Grupos de identidades de usuário, e clique em Adicionar:



Criar grupo de identidade

3. Associar usuários a grupos de identidade:

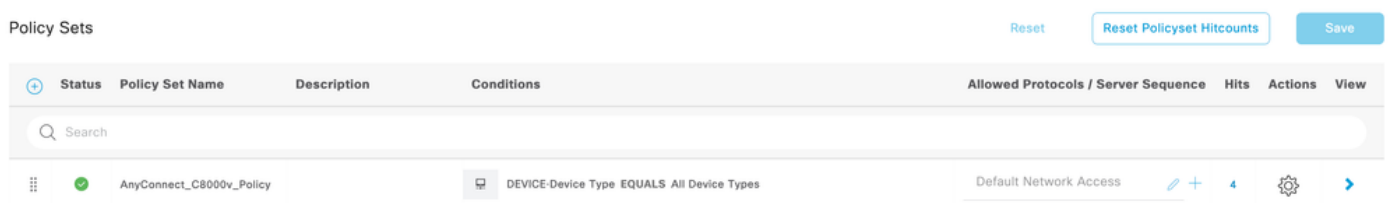
Associe usuários ao grupo de identidade correto. Navegue até Administração > Gerenciamento de identidades > Identidades > Usuários.



Adicionar usuário ao grupo de identidade

4. Criar Conjunto de Políticas:

Defina um novo conjunto de políticas e as condições que correspondem à política. Neste exemplo, todos os tipos de dispositivos são permitidos sob as condições. Para fazer isso, navegue até Política>Conjuntos de políticas:



Criar Conjunto de Políticas

5. Criar uma Política de Autorização:

Defina uma nova Diretiva de Autorização com as condições necessárias para atender à diretiva. Certifique-se de incluir os grupos de identidade criados na etapa 2 como uma condição.

Q Search

✓

AnyConnect_C8000v_Policy

🖨

DEVICE-Device Type EQUALS All Device Types

Default Network Access

✎

+

4

➤ Authentication Policy (1)

➤ Authorization Policy - Local Exceptions

➤ Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

					Results				
⊕	Status	Rule Name	Conditions		Profiles	Security Groups		Hits	Actions
Q Search									
	✓	AC_Split_Users	AND	🖨 DEVICE-Device Type EQUALS All Device Types 🔍 IdentityGroup-Name EQUALS User Identity Groups:AC_Split	Select from list ▼ +	Select from list ✎ +	4	⚙	
	✓	Default			DenyAccess ✎ +	Select from list ✎ +	0	⚙	

Library

Search by Name

- 5G
- BYOD_Is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed

Editor

DEVICE:Device Type

Equals ▼ All Device Types ▼

IdentityGroup-Name

Equals ▼ User Identity Groups:AC_Split ▼

AND ▼

+

NEW AND OR

Set to 'Is not'

Duplicate Save

6. Criar um Perfil de Autorização:

Tipo de acesso = ACCESS_ACCEPT

			Results		
Status	Rule Name	Conditions	Profiles	Security Groups	Hits
Q Search					
AC_Split_Users	AND	DEVICE-Device Type EQUALS All Device Types IdentityGroup-Name EQUALS User Identity Groups:AC_Split	Select from list Create a New Authorization Profile	Select from list Select from list	4 0
Default				Select from list Select from list	

Criar novo perfil de autorização

Authorization Profile

* Name

AC_Router_Split

Description

Split exclude for AC users

* Access Type

ACCESS_ACCEPT

Network Device Profile

Cisco

Service Template

☐

Track Movement

☐

Agentless Posture

☐

Passive Identity Tracking

☐

Configuração do perfil de autorização

Advanced Attributes Settings

Cisco:cisco-av-pair

=

ipsec:split-exclude= ipv4 ...

Cisco:cisco-av-pair

=

ipsec:split-exclude= ipv4 ...

ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0

cisco-av-pair = ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0

Configurar atributos no perfil de autorização

7. Revise a configuração do Perfil de Autorização.

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > AC_Router_Split

Authorization Profile

* Name AC_Router_Split

Description Split exclude for AC users

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

> Common Tasks

> Advanced Attributes Settings

Cisco:cisco-av-pair = ipsec:split-exclude= ipv4 ...

Cisco:cisco-av-pair = ipsec:split-exclude= ipv4 ...

> Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = ipsec:split-exclude= ipv4 192.168.1.0/255.255.255.0

cisco-av-pair = ipsec:split-exclude= ipv4 192.168.2.0/255.255.255.0

Revisar a configuração do perfil de autorização

8. Esta é a política de Autorização na configuração do Conjunto de Políticas após a seleção dos perfis necessários:

AnyConnect_C8000v_Policy

DEVICE-Device Type EQUALS All Device Types

Default Network Access

+

4

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

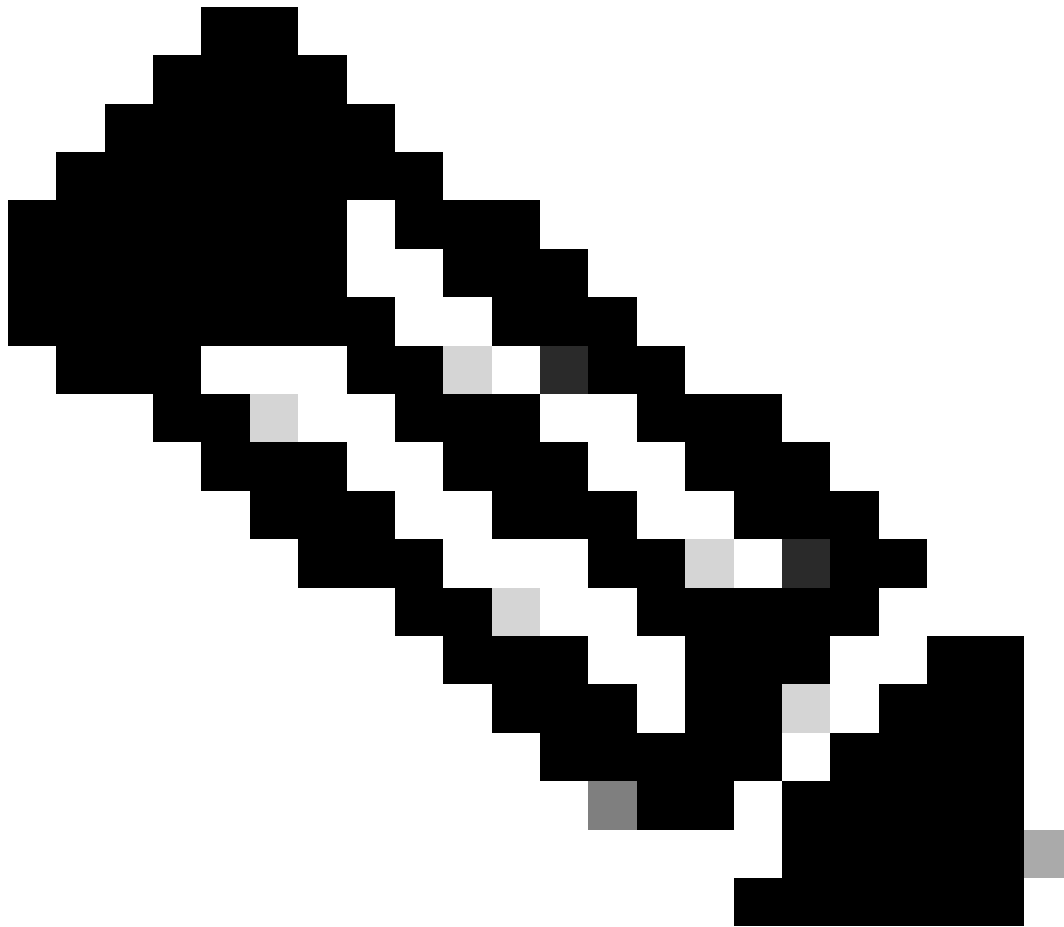
				Results			
+	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search							
	✓	AC_Split_Users	AND DEVICE-Device Type EQUALS All Device Types IdentityGroup-Name EQUALS User Identity Groups:AC_Split	AC_Router_Split +	Select from list +	4	
	✓	Default		DenyAccess +	Select from list +	0	

Reset

Save

Configuração de Política de Autorização Final

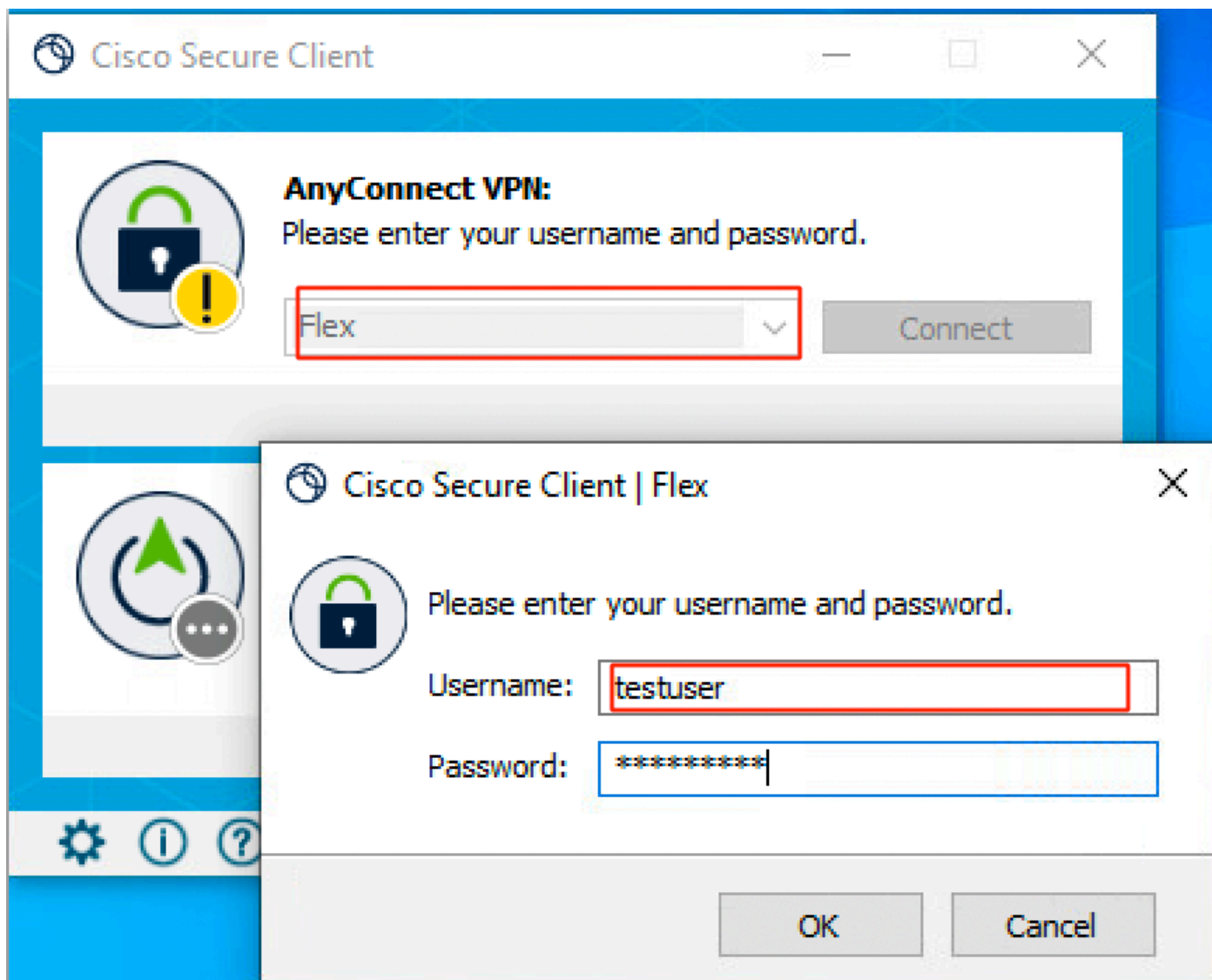
Com este exemplo de configuração, você pode excluir a passagem de redes através de VPN através da configuração do ISE com base no grupo de identidade ao qual o usuário pertence.



Note: Somente uma sub-rede split-exclude pode ser enviada para o PC cliente ao usar o headend do Cisco IOS XE para uma conexão VPN RA. Isso foi solucionado pelo bug da Cisco ID [CSCwj38106](#) e várias sub-redes split-exclude podem ser enviadas de 17.12.4. Consulte o bug para obter mais detalhes sobre versões corrigidas.

Verificar

1. Para testar a autenticação, conecte-se ao C8000V do PC do usuário através do AnyConnect e insira as credenciais.



Faça login no AnyConnect

2. Uma vez estabelecida a conexão, clique no ícone de engrenagem (canto inferior esquerdo) e navegue para AnyConnect VPN > Statistics. Confirme o modo de túnel a ser Split Exclude.

Cisco Secure Client

Secure Client

Status Overview

AnyConnect VPN >

ISE Posture

Collect diagnostic information for all installed components.

Diagnostics

Virtual Private Network (VPN)

Preferences Statistics **Route Details** Firewall Message History

Connection Information

State:	Connected
Tunnel Mode (IPv4):	Split Exclude
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:44
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

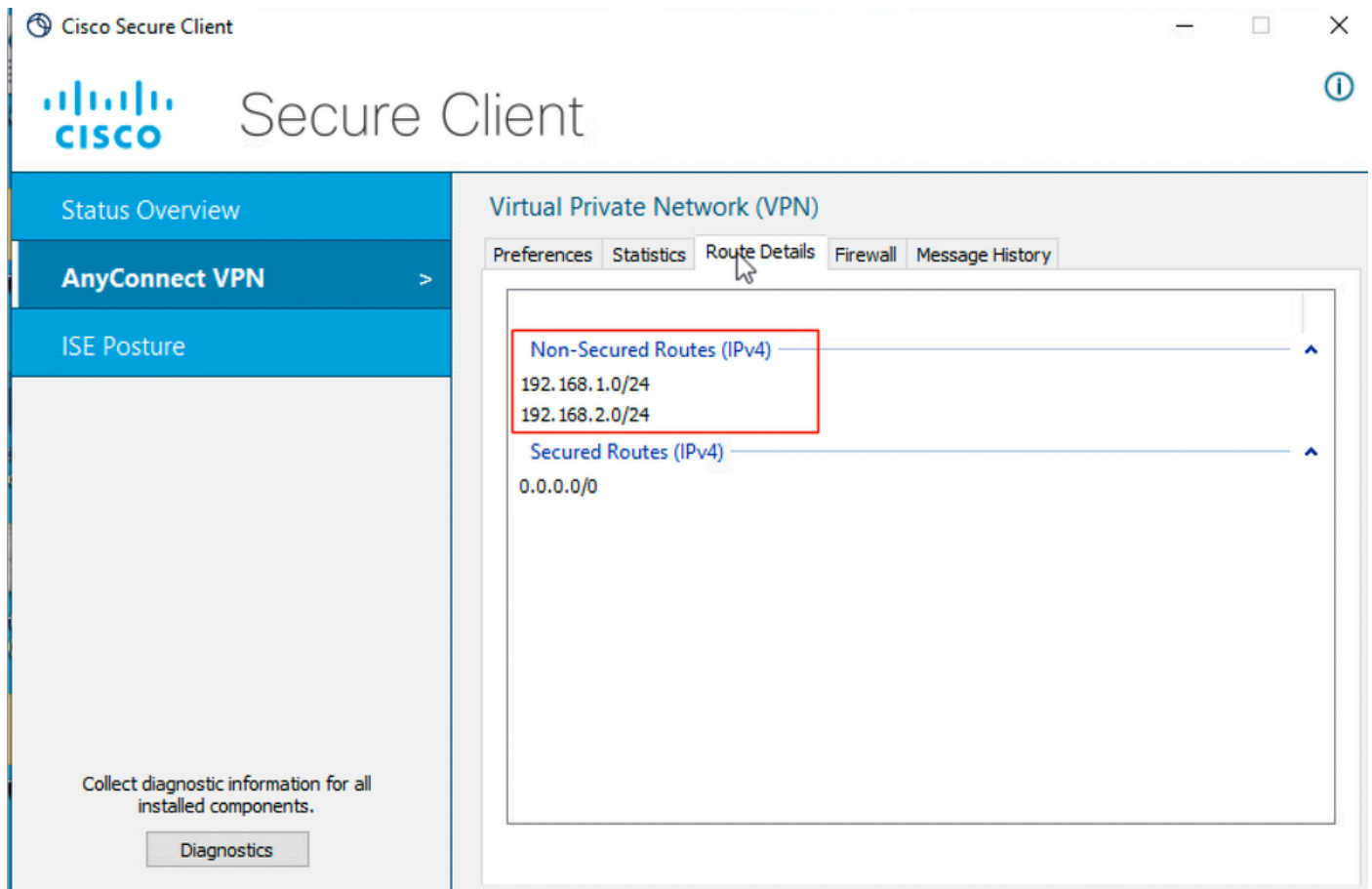
Address Information

Client (IPv4):	172.16.10.9
Client (IPv6):	Not Available
Server:	10.106.67.33

Reset Export Stats

Validar as estatísticas

Navegue até AnyConnect VPN > Route details e confirme se as informações exibidas correspondem às rotas seguras e não seguras.



Validar os detalhes da rota

Você também pode verificar os detalhes da conexão no headend da VPN:

1. IKEv2 parameters

<#root>

8kv#

show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvr/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 fvrfr: (none) ivrfr: (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.

Troubleshooting

No roteador Cisco:

1. Use as depurações de IKEv2 e IPsec para verificar a negociação entre o headend e o 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. Use depurações AAA para verificar a atribuição de atributos locais e/ou remotos.

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

No ISE:

Use os logs ao vivo RADIUS navegando até Operations > Livelogs.

Cenário de trabalho

Esta é a depuração da conexão bem-sucedida:

<#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=L2L40A6A4321Z02L40A6A325BZH1194CC58
*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 [2L40A6A4321Z02L4]
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 [1Z02L40A6A325BZH]
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#

```

Referências

- [Configurar o headend do FlexVPN para acesso remoto IKEv2 usando o banco de dados de usuário local](#)
- [Configurar o AnyConnect Flexvpn com autenticação EAP e DUO](#)
- [Configurar o acesso remoto do AnyConnect IKEv2 com EAP-MD5](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.