Konfigurieren von Split Exclude für AnyConnect FlexVPN mithilfe der ISE

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zum Konfigurieren von Split-Excluding mithilfe von ISE für IKEv2 AnyConnect-Verbindungen mit einem Cisco IOS® XE-Router beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Anwendererlebnis bei der AnyConnect IPsec-Konfiguration auf einem Router
- Konfiguration der Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- RADIUS-Protokoll

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm

Netzwerkdiagramm

Konfigurationen

Berücksichtigen Sie diese Abschnitte, um die Konfiguration abzuschließen.

Router-Konfiguration

1. Konfigurieren Sie einen RADIUS-Server für die Authentifizierung und lokale Autorisierung auf dem Gerät:

```
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. Konfigurieren Sie einen Vertrauenspunkt, um das Router-Zertifikat zu installieren. Da die lokale Authentifizierung des Routers vom Typ RSA ist, erfordert das Gerät, dass der Server sich selbst mithilfe eines Zertifikats authentifiziert. Weitere Informationen zur Zertifikaterstellung finden Sie unter Zertifikatregistrierung für eine PKI -1 und Zertifikatregistrierung für eine PKI -2:

```
crypto pki trustpoint flex
```

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

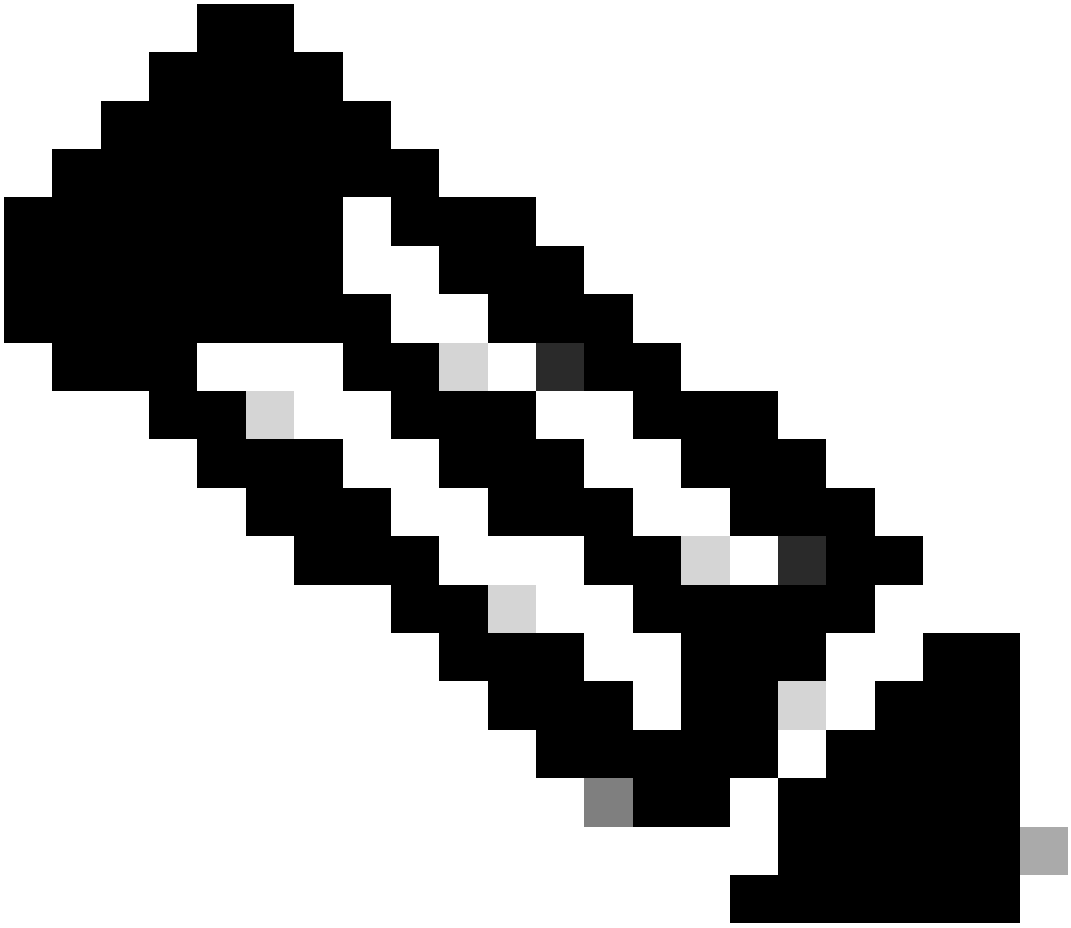
3. Definieren Sie einen lokalen IP-Pool, um AnyConnect VPN-Clients bei erfolgreicher AnyConnect-Verbindung Adressen zuzuweisen:

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

4. Erstellen Sie eine lokale IKEv2-Autorisierungsrichtlinie:

Die in dieser Richtlinie definierten Attribute werden zusammen mit den vom Radius-Server übertragenen Attributen auf die Benutzer angewendet.

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



Anmerkung: Wenn die benutzerdefinierte IKEv2-Autorisierungsrichtlinie nicht konfiguriert ist, wird für die Autorisierung die als Standard bezeichnete Standardautorisierungsrichtlinie verwendet. Die in der IKEv2-Autorisierungsrichtlinie angegebenen Attribute können auch über den RADIUS-Server übertragen werden. Sie müssen das Split-Exclude-Attribut vom RADIUS-Server übertragen.

---

5 (Optional). Erstellen Sie einen IKEv2-Vorschlag und eine IKEv2-Richtlinie (wenn diese nicht konfiguriert sind, werden intelligente Standardeinstellungen verwendet):

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

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

6 (Optional). Konfigurieren Sie den Transformationssatz (falls nicht konfiguriert, werden intelligente Standardeinstellungen verwendet):

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

7. Konfigurieren Sie eine Loopback-Schnittstelle mit einigen Dummy-IP-Adressen. Die Virtual-Access-Schnittstellen leihen sich die IP-Adresse aus:

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

8. Konfigurieren Sie eine virtuelle Vorlage, von der die Schnittstellen für den virtuellen Zugriff geklont werden:

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

9. Laden Sie das AnyConnect-Clientprofil in den Bootflash des Routers hoch, und definieren Sie das Profil wie folgt:

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

10. Konfigurieren Sie ein IKEv2-Profil, das alle verbindungsbezogenen Informationen enthält:

```
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
```

Diese werden im IKEv2-Profil verwendet:

- match identity remote key-id *$AnyConnectClient$* - Bezieht sich auf die Identität des Clients. AnyConnect verwendet *$AnyConnectClient$* als Standard-IKE-Identität vom Typ key-id. Diese Identität kann jedoch im AnyConnect-Profil manuell geändert werden, um Bereitstellungsanforderungen zu erfüllen.
- authentication remote - Gibt an, dass das EAP-Protokoll für die Client-Authentifizierung verwendet werden muss.
- authentication local - Gibt an, dass Zertifikate für die lokale Authentifizierung verwendet werden müssen.
- aaa authentication eap - Bei der EAP-Authentifizierung wird der RADIUS-Server FlexVPN_auth verwendet.
- aaa authorization group eap list - Während der Autorisierung wird die Netzwerkliste a-eap-author-grp mit der Autorisierungsrichtlinie ikev2-auth-policy verwendet.
- aaa authentication user eap cached - Ermöglicht implizite Benutzerautorisierung.
- virtual-template 100 - Definiert, welche virtuelle Vorlage geklont werden soll.
- anyconnect profile acvpn - Das in Schritt 9 definierte Client-Profil wird hier auf dieses IKEv2-Profil angewendet.

11. Konfigurieren Sie das IPsec-Profil:

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

12. Fügen Sie der virtuellen Vorlage das IPsec-Profil hinzu:

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

13. Deaktivieren Sie die HTTP-URL-basierte Zertifikatssuche und den HTTP-Server auf dem Router:

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

14. Konfigurieren Sie die SSL-Richtlinie, und geben Sie die WAN-IP-Adresse des Routers als lokale Adresse für den Download des Profils an:

```
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
```

Ausschnitt des AnyConnect-Clientprofils (XML-Profil):

Vor Cisco IOS XE 16.9.1 ist kein automatischer Profildownload vom Headend möglich. Nach 16.9.1 kann das Profil vom Headend heruntergeladen werden.

<#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

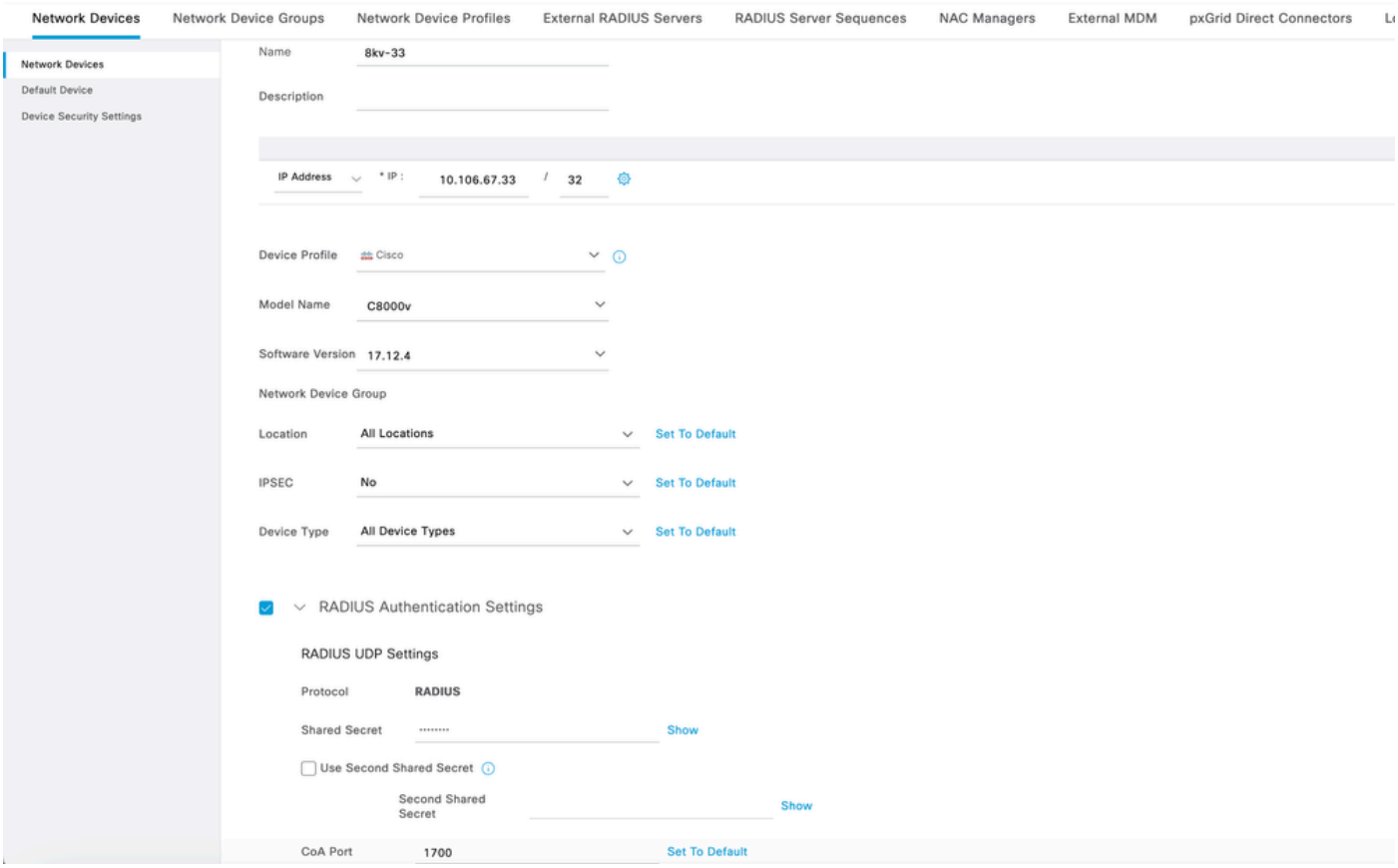
```
</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
```

EAP-MD5

```
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Konfiguration der Identity Services Engine (ISE)

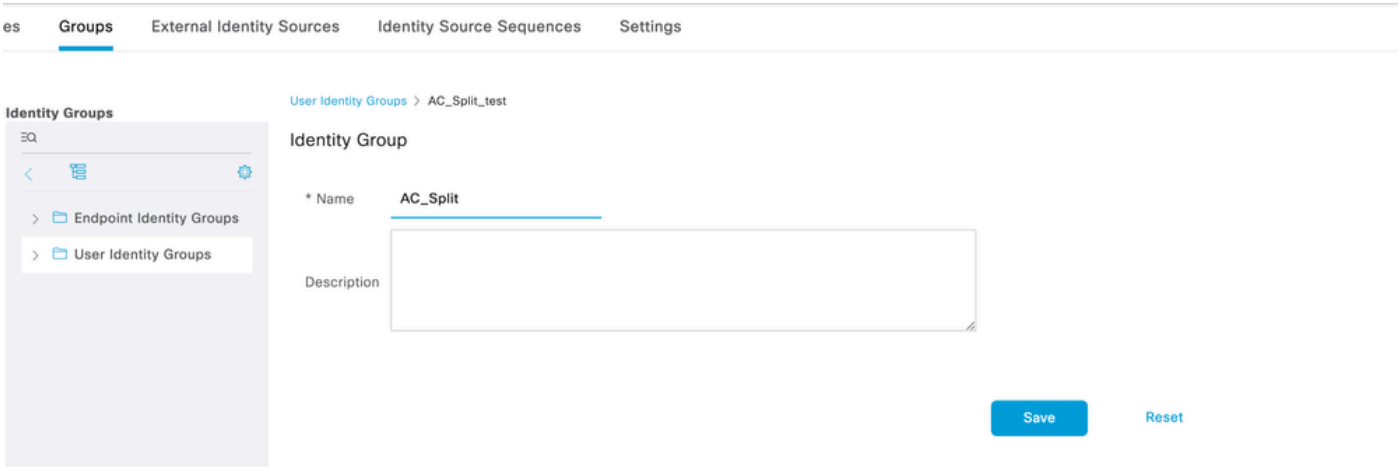
1. Registrieren Sie den Router als gültiges Netzwerkgerät bei der ISE, und konfigurieren Sie den Schlüssel für den gemeinsamen geheimen Schlüssel für RADIUS. Navigieren Sie hierzu zu Administration > Network Resources > Network Devices. Klicken Sie auf Add, um den Router als AAA-Client zu konfigurieren:



Netzwerkgerät hinzufügen

2. Identitätsgruppen erstellen:

Definieren Sie Identitätsgruppen, um Benutzer mit ähnlichen Merkmalen und Berechtigungen zuzuordnen. Diese werden in den nächsten Schritten verwendet. Navigieren Sie zu Administration > Identity Management > Groups > User Identity Groups, und klicken Sie dann auf Hinzufügen:



Identitätsgruppe erstellen

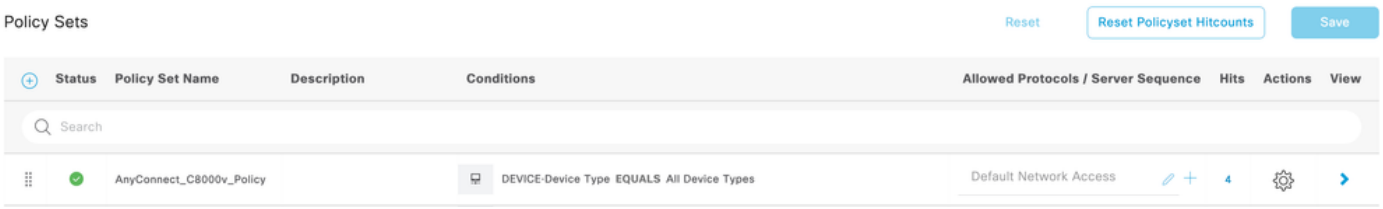
3. Zuordnen von Benutzern zu Identitätsgruppen:

Zuordnen von Benutzern zur richtigen Identitätsgruppe Navigieren Sie zu Administration > Identity Management > Identities > Users.

Benutzer zu Identitätsgruppe hinzufügen

4. Policy Set erstellen:

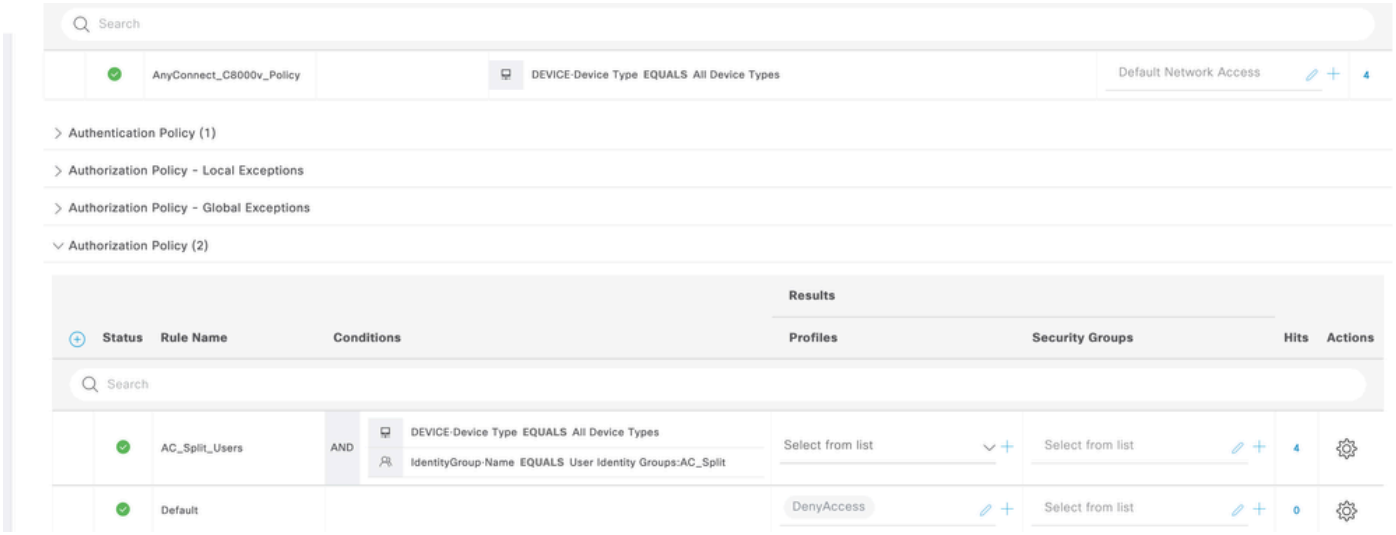
Definieren Sie einen neuen Richtliniensatz und die Bedingungen, die mit der Richtlinie übereinstimmen. In diesem Beispiel sind alle Gerätetypen unter den Bedingungen zulässig. Navigieren Sie dazu zuPolicy>Policy Sets:



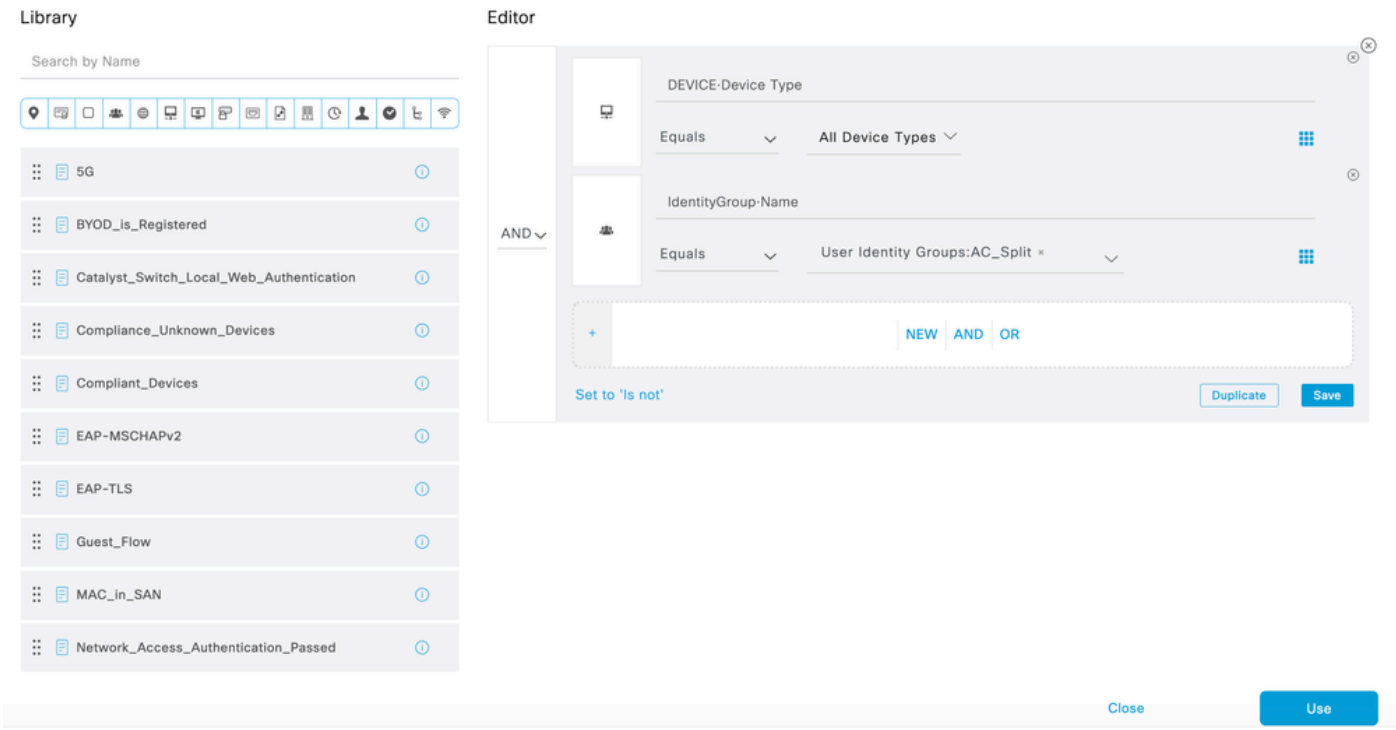
Policy Set erstellen

5. Autorisierungsrichtlinie erstellen:

Definieren Sie eine neue Autorisierungsrichtlinie mit den erforderlichen Bedingungen, die mit der Richtlinie übereinstimmen. Stellen Sie sicher, dass Sie die in Schritt 2 erstellten Identitätsgruppen als Bedingung einschließen.



Autorisierungsrichtlinie erstellen

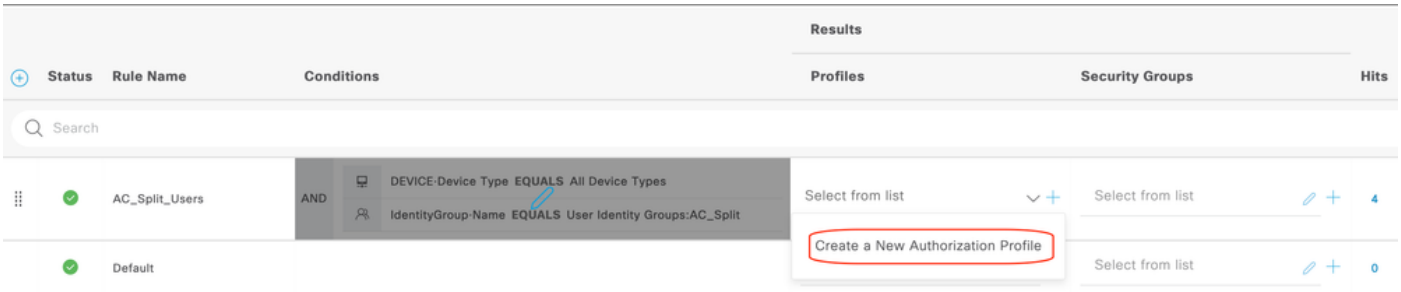


Bedingungen in Autorisierungsrichtlinie auswählen

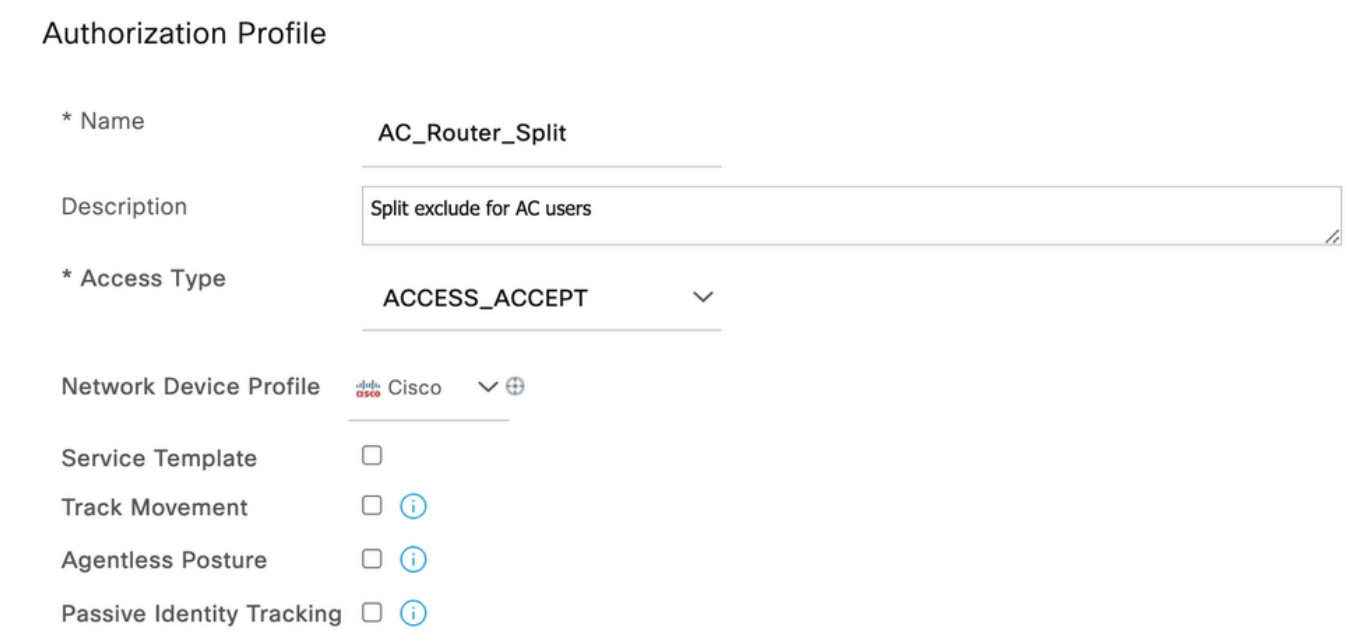
6. Erstellen Sie ein Autorisierungsprofil:

Das Autorisierungsprofil enthält die Aktionen, die beim Abgleich der Autorisierungsrichtlinie ausgeführt werden. Erstellen Sie ein neues Autorisierungsprofil mit den folgenden Attributen:

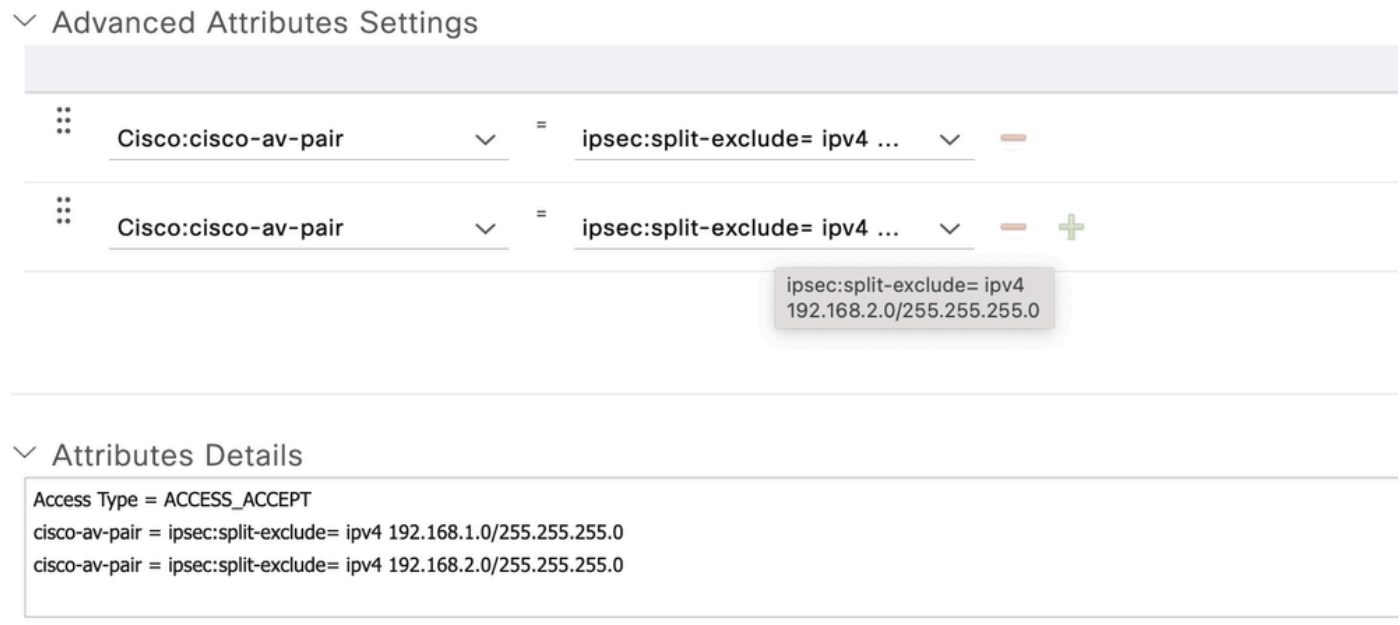
Zugriffstyp = ACCESS_ACCEPT
cisco-av-pair = ipsec:split-exclude= ipv4 <IP-Netzwerk>/<Subnetzmaske>



Neues Autorisierungsprofil erstellen

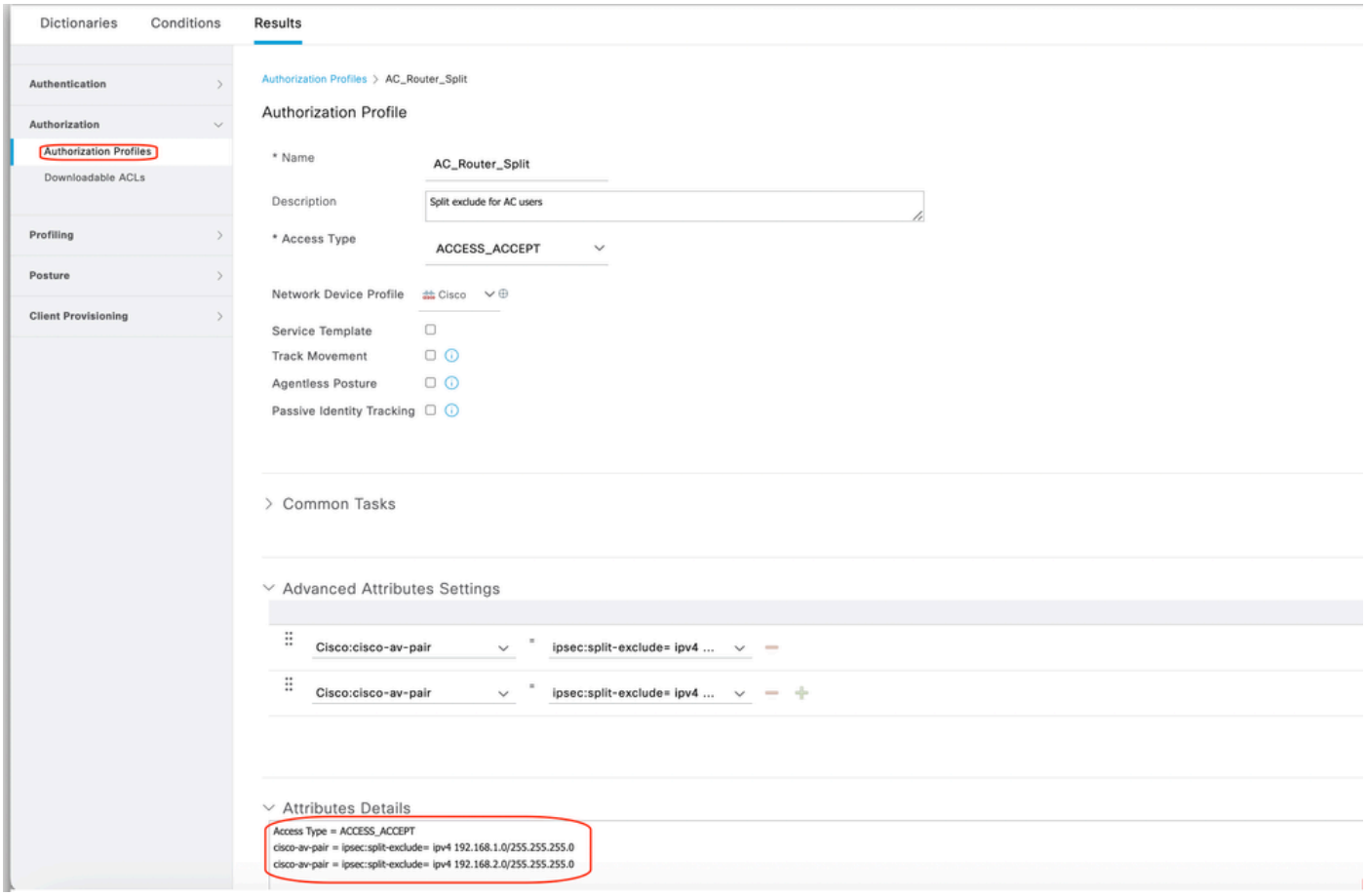


Autorisierungsprofilkonfiguration



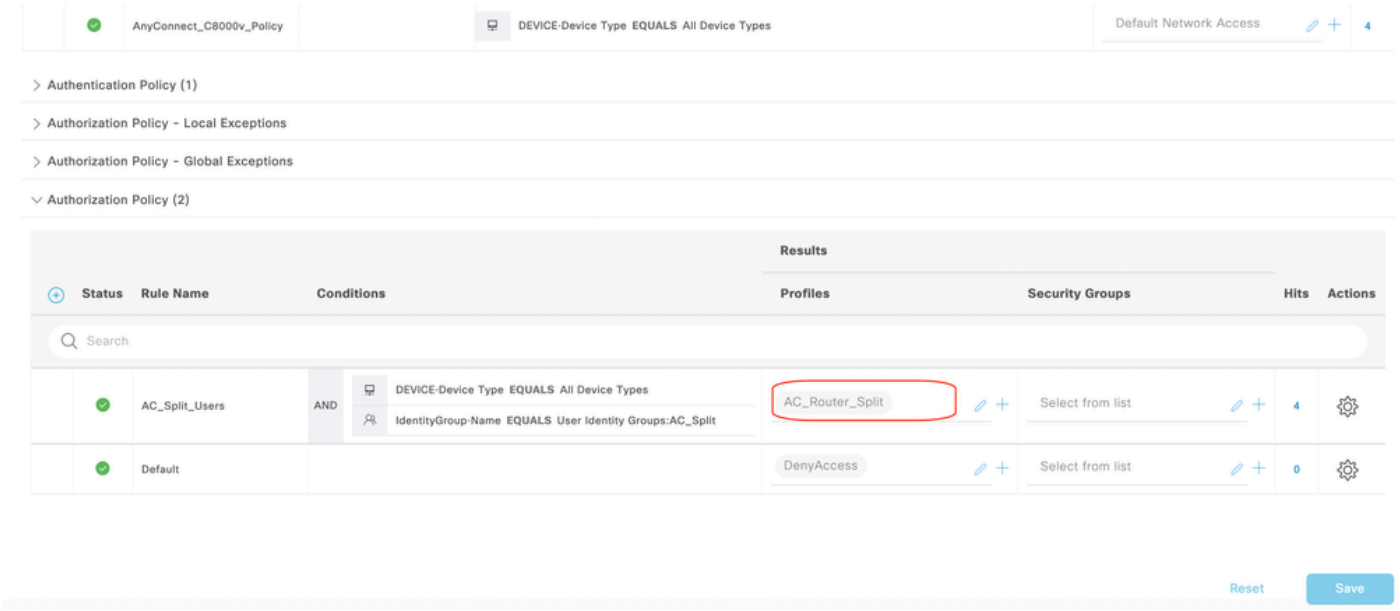
Attribute im Autorisierungsprofil konfigurieren

7. Überprüfen Sie die Autorisierungsprofilkonfiguration.



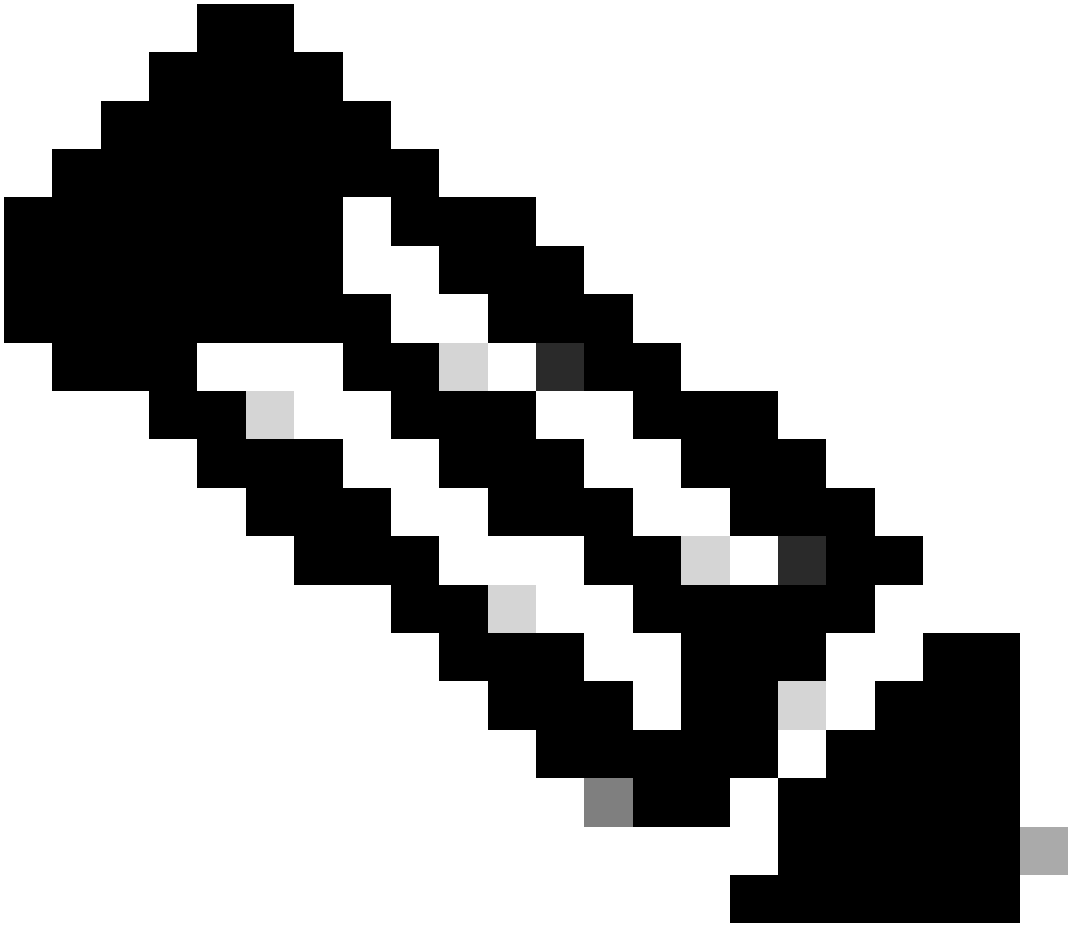
Überprüfen der Autorisierungsprofilkonfiguration

8. Dies ist die Autorisierungsrichtlinie in der Konfiguration des Richtliniensatzes nach Auswahl der erforderlichen Profile:



Abschließende Konfiguration der Autorisierungsrichtlinie

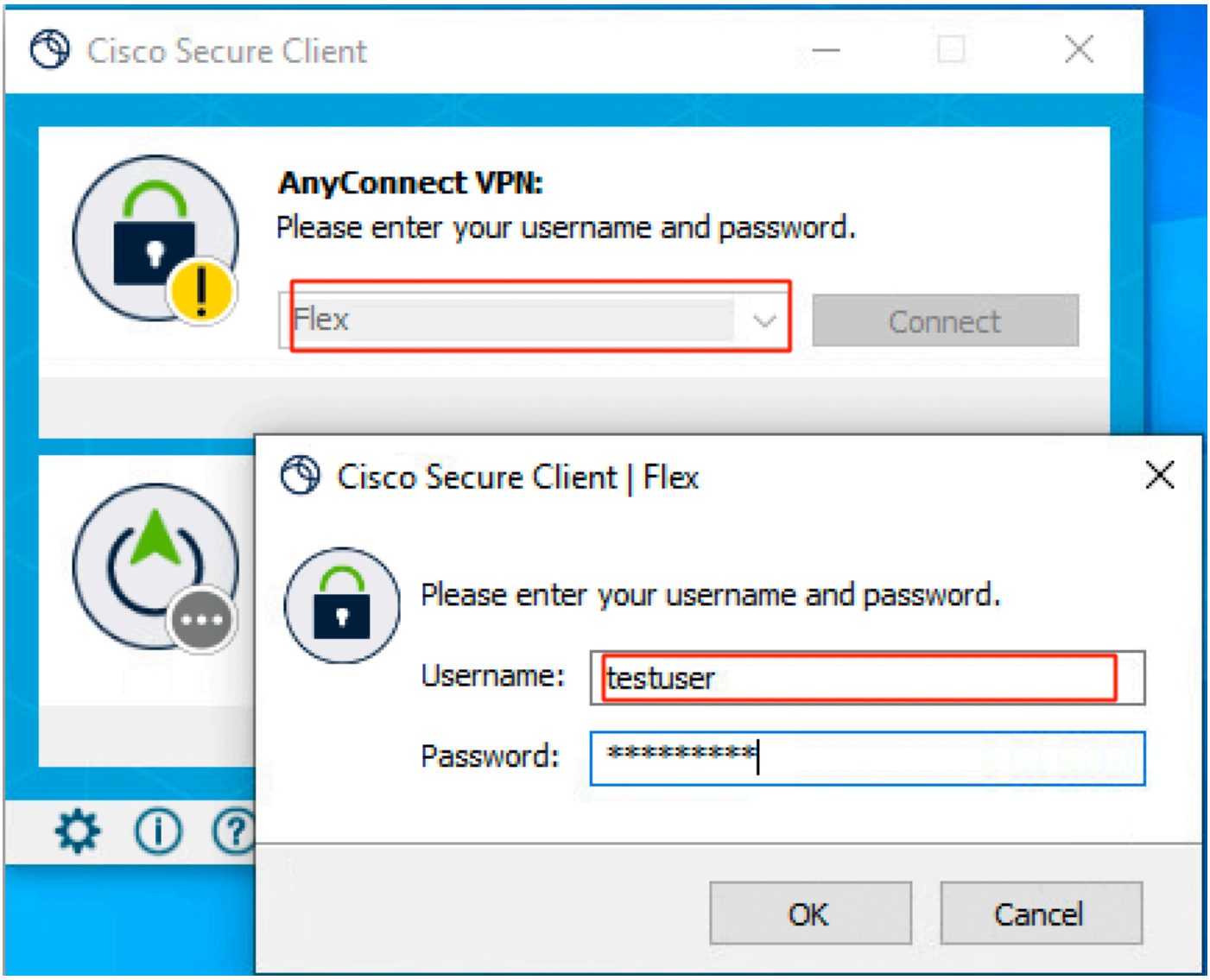
Mit diesem Konfigurationsbeispiel können Sie Netzwerke basierend auf der Identitätsgruppe, zu der der Benutzer gehört, vom Weiterleiten über VPN durch die ISE-Konfiguration ausschließen.



Anmerkung: Bei Verwendung des Cisco IOS XE-Headends für eine RA VPN-Verbindung kann nur ein Split-Exclude-Subnetz auf den Client-PC geschoben werden. Dies wurde durch die Cisco Bug-ID CSCwj38106 behoben, und mehrere Split-Exclude-Subnetze können ab 17.12.4 geschoben werden. Weitere Informationen zu Fixed-Versionen finden Sie im Bug.

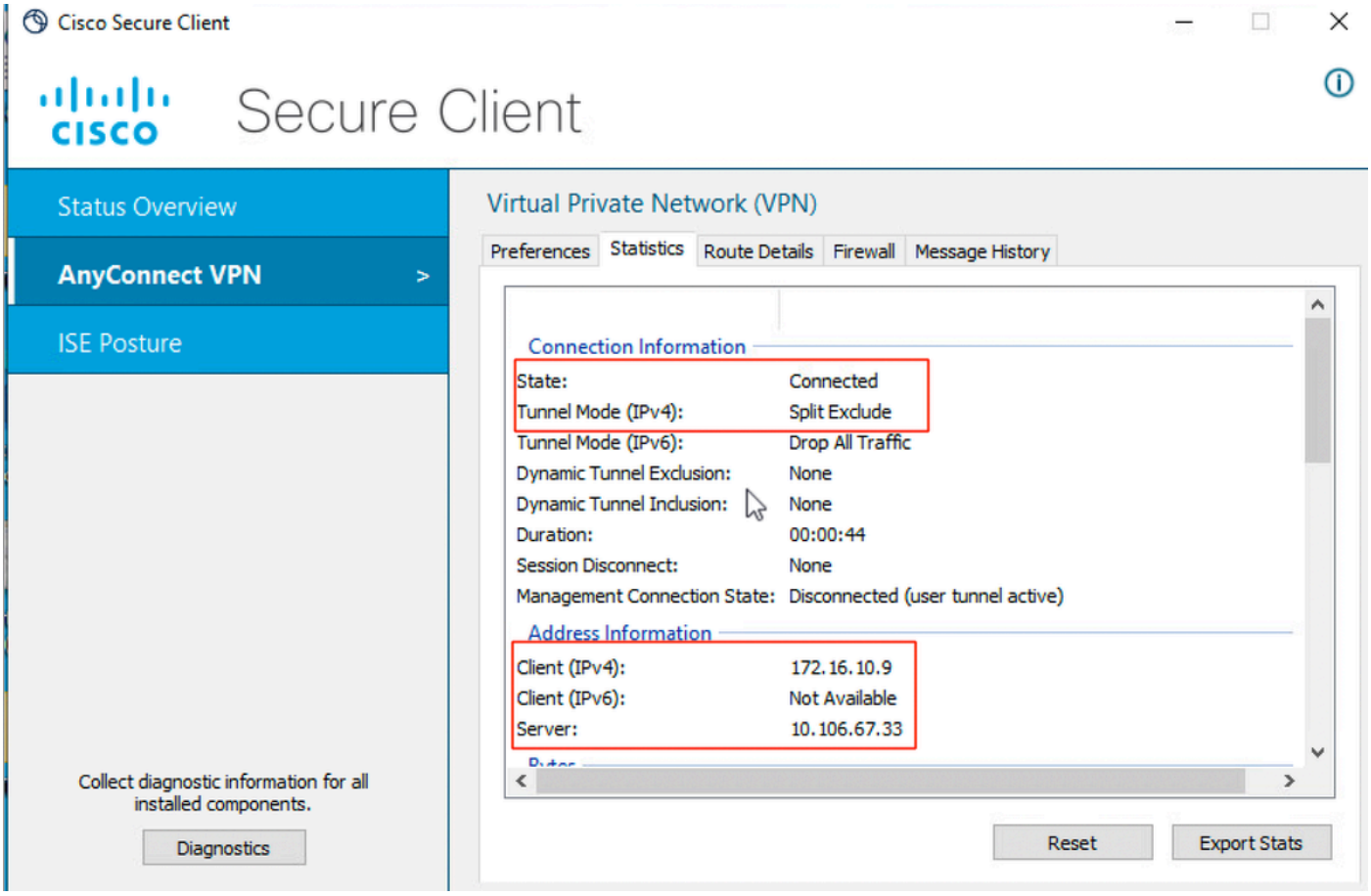
Überprüfung

1. Um die Authentifizierung zu testen, stellen Sie vom PC des Benutzers über AnyConnect eine Verbindung zum C8000V her, und geben Sie die Anmeldeinformationen ein.



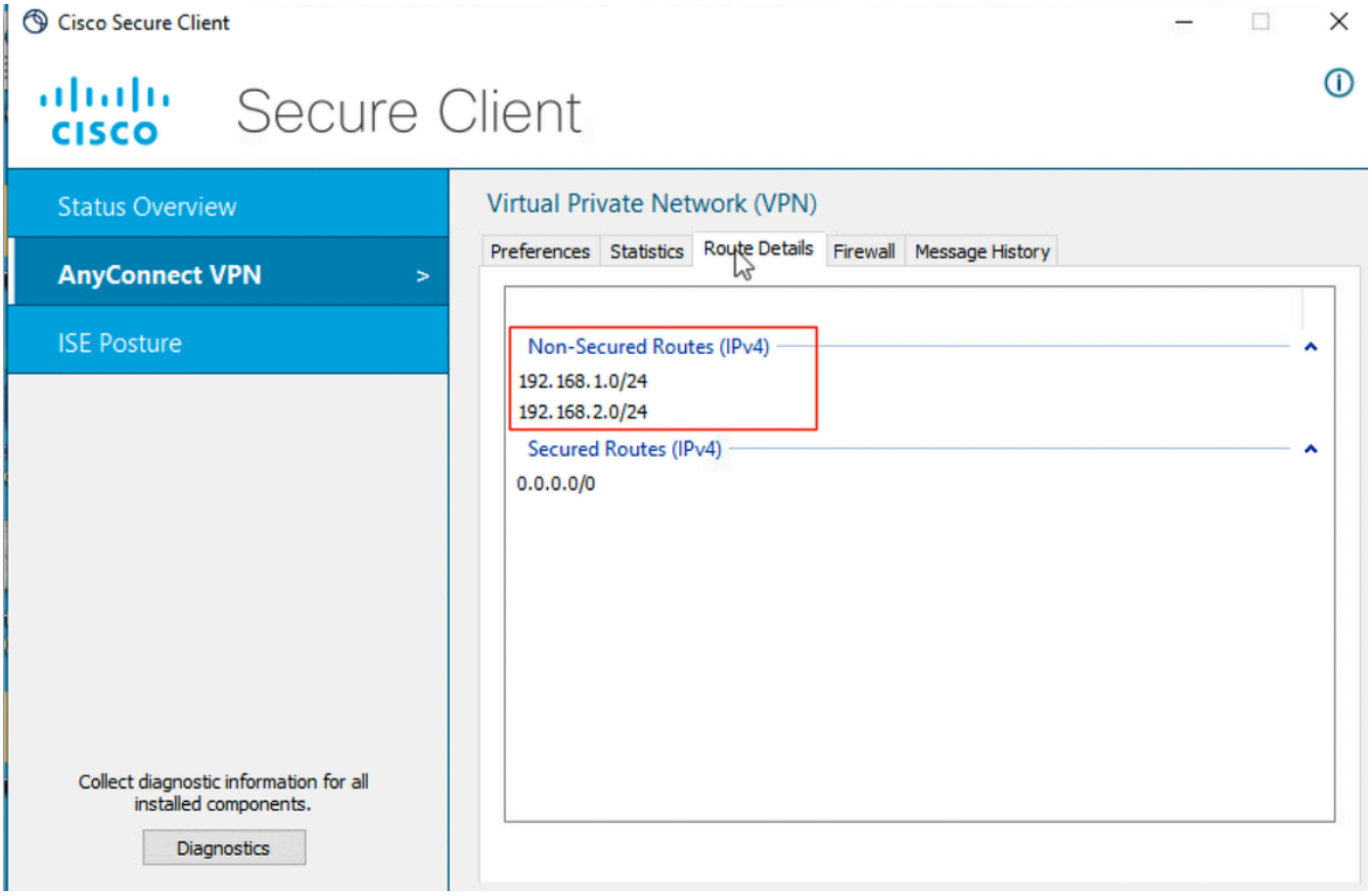
Bei AnyConnect anmelden

2. Sobald die Verbindung hergestellt ist, klicken Sie auf das Zahnradsymbol (linke untere Ecke) und navigieren Sie zu AnyConnectVPN > Statistics. Bestätigen Sie, dass der Tunnelmodus auf "Ausschließen aufteilen" gesetzt ist.



Statistiken überprüfen

Navigieren Sie zu AnyConnectVPN > Route details, und stellen Sie sicher, dass die angezeigten Informationen den sicheren und nicht sicheren Routen entsprechen.



Validierung der Routendetails

Sie können die Verbindungsdetails auch am VPN-Headend überprüfen:

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.

Fehlerbehebung

Auf Cisco Router:

1. Verwenden Sie das IKEv2- und das IPsec-Debugging, um die Aushandlung zwischen dem Headend und dem Client zu überprüfen.

```
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. Verwenden Sie AAA-Debugging-Funktionen, um die Zuweisung von lokalen und/oder Remote-Attributen zu überprüfen.

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

Auf der ISE:

Verwenden Sie die RADIUS-Live-Protokolle, indem Sie zuOperations > Live logs (Operationen > Live-Protokolle) navigieren.

Arbeitsszenario

Dies ist das Debugging der erfolgreichen Verbindung:

<#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#
```

Referenzen

- Konfigurieren des FlexVPN-Headend für IKEv2-Remote-Zugriff mithilfe der lokalen Benutzerdatenbank
- Konfigurieren von AnyConnect FlexVPN mit EAP- und DUO-Authentifizierung
- Konfigurieren von AnyConnect IKEv2-Remote-Zugriff mit EAP-MD5

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.