تكوين إستثناء التقسيم ل AnyConnect FlexVPN باستخدام ISE

المحتويات

المقدمة

يصف هذا المستند إجراء تكوين إستثناء التقسيم باستخدام ISE لاتصال IKEv2 AnyConnect بموجه Cisco IOS® XE.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تجربة تكوين AnyConnect IPsec على موجه
- تكوين محرك خدمات الهوية من Cisco (ISE)
- العميل الآمن من Cisco (CSC)
- بروتوكول RADIUS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

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

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة

الرسم التخطيطي للشبكة

التكوينات

من أجل إكمال التكوين، ضع في الاعتبار هذه الأقسام.

تكوين الموجّه

1. تكوين خادم RADIUS للمصادقة والتخويل المحلي على الجهاز:

```
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. تكوين نقطة موثوق بها لتثبيت شهادة الموجه. بما أن المصادقة المحلية للموجه هي نوع RSA، يتطلب الجهاز أن يقوم الخادم بمصادقة نفسه باستخدام شهادة. يمكنك الرجوع إلى تسجيل الشهادة لـ PKI -1 وتسجيل الشهادة لـ PKI -2 للحصول على مزيد من التفاصيل حول إنشاء الشهادة:

```
crypto pki trustpoint flex
 enrollment terminal
 ip-address none
 subject-name CN=flexserver.cisco.com
```

```
 revocation-check none
 rsakeypair flex1
 hash sha256
```

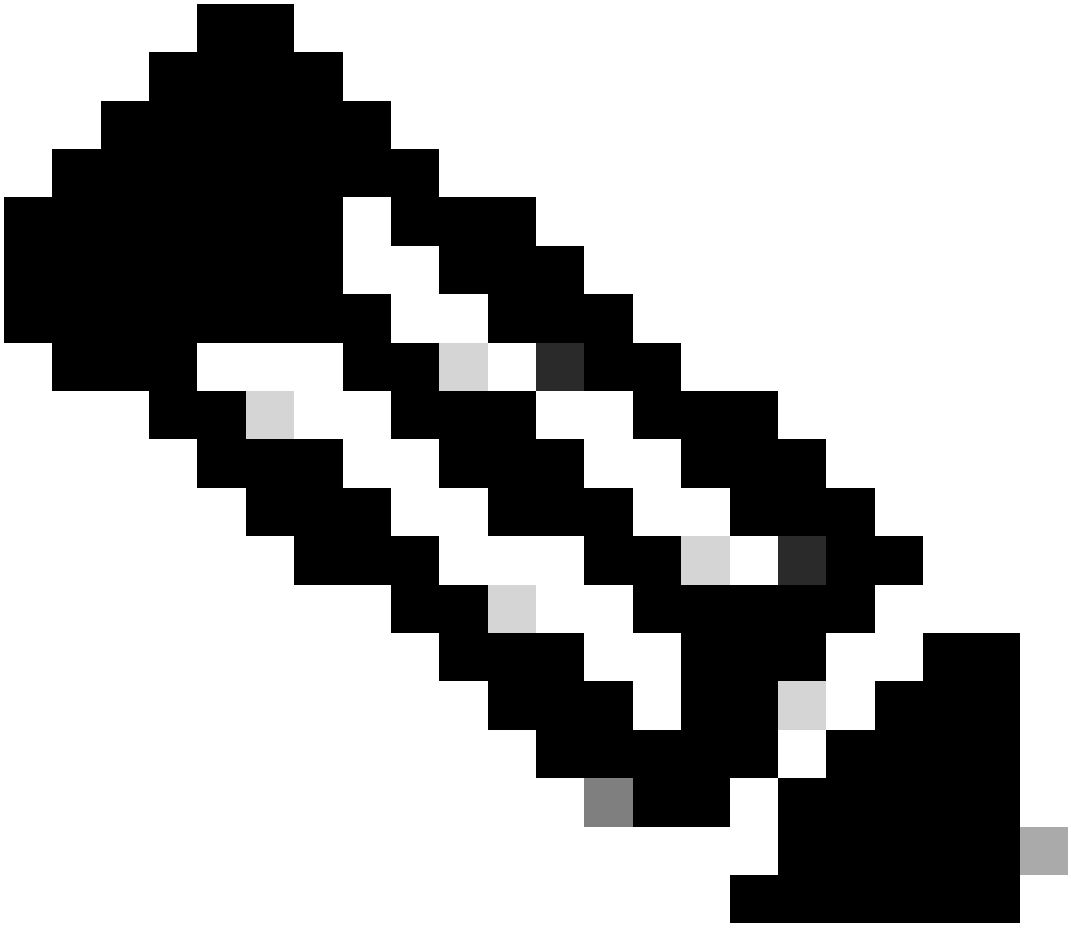
3. حدد تجمع IP المحلي لتعيين العناوين إلى عملاء AnyConnect VPN عند اتصال AnyConnect الناجح:

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

4. قم بإنشاء سياسة ترخيص محلية ل IKEv2:

يتم تطبيق السمات المحددة في هذا النهج مع السمات التي تم دفعها من خادم Radius على المستخدمين

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



ملاحظة: في حالة عدم تكوين نهج تخويل IKEv2 المخصص، يتم إستخدام نهج التخويل الافتراضي الذي يسمى الافتراضي للتخويل. يمكن أيضا دفع السمات المحددة ضمن نهج تخويل IKEv2 عبر خادم RADIUS. تحتاج إلى دفع سمة فصل-إستثناء من خادم RADIUS.

5 (إختياري). إنشاء مقترح ونهج IKEv2 (في حالة عدم تكوينه، يتم إستخدام الافتراضيات الذكية):

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

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

6 (إختياري). تكوين مجموعة التحويل (في حالة عدم تكوينها، يتم إستخدام الافتراضيات الذكية):

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

7. قم بتكوين واجهة إسترجاع باستخدام عنوان IP وهمي. تقوم واجهات الوصول الظاهري باقتراض عنوان IP منه:

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

8. تكوين قالب ظاهري يتم من خلاله نسخ واجهات الوصول الظاهري:

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

9. قم بتحميل ملف تعريف عميل AnyConnect إلى ذاكرة التمهيد للموجه وحدد ملف التعريف كما هو موضح:

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

10. قم بتكوين ملف تعريف IKEv2 يحتوي على جميع المعلومات المتعلقة بالاتصال:

```
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
```

ويتم إستخدام هذه العناصر في ملف تعريف IKEv2:

- مطابقة معرف الهوية البعيد للمفتاح *$AnyConnectClient$* - يشير إلى هوية العميل. يستخدم AnyConnect *$AnyConnectClient$* كهوية IKE الافتراضية من النوع key-id. وهو ذلك، يمكن تغيير هذه الهوية يدويا في ملف تعريف AnyConnect لمطابقة إحتياجات النشر.
- المصادقة عن بعد - يشير إلى أنه يجب إستخدام بروتوكول EAP لمصادقة العميل.
- المصادقة المحلية - تذكر أنه يجب إستخدام الشهادات للمصادقة المحلية.
- AAA Authentication EAP - أثناء مصادقة EAP، يتم إستخدام FlexVPN_AUTH لخادم RADIUS.
- قائمة EAP الخاصة بمجموعة تفويض AAA - أثناء التخويل، تستخدم قائمة الشبكة a-EAP-author-GRP مع سياسة التخويل ikev2-auth-policy.
- AAA تخويل المستعمل تخزينا مؤقتا- تمكين تخويل مضمون من المستخدم.
- القالب الظاهري 100 - يحدد أي القالب الظاهري سيتم نسخه.
- AnyConnect Profile acvpn - يتم تطبيق ملف تعريف العميل المحدد في الخطوة 9. هنا على ملف تعريف IKEv2 هذا.

11. تكوين ملف تعريف IPsec:

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

12. إضافة ملف تعريف IPsec إلى القالب الظاهري:

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

13. قم بتعطيل بحث الشهادة المستند إلى HTTP-URL وخادم HTTP على الموجه:

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

14. قم بتكوين سياسة SSL وحدد IP WAN الخاص بالموجه كعنوان محلي لتنزيل ملف التعريف:

```
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
```

قصاصة من ملف تعريف عميل AnyConnect (ملف تعريف XML):

قبل Cisco IOS XE 16.9.1، لا تتوفر تنزيلات ملف التعريف التلقائية من وحدة الاستقبال والبث. بعد 16.9.1، من الممكن تنزيل ملف التعريف من وحدة الاستقبال والبث.

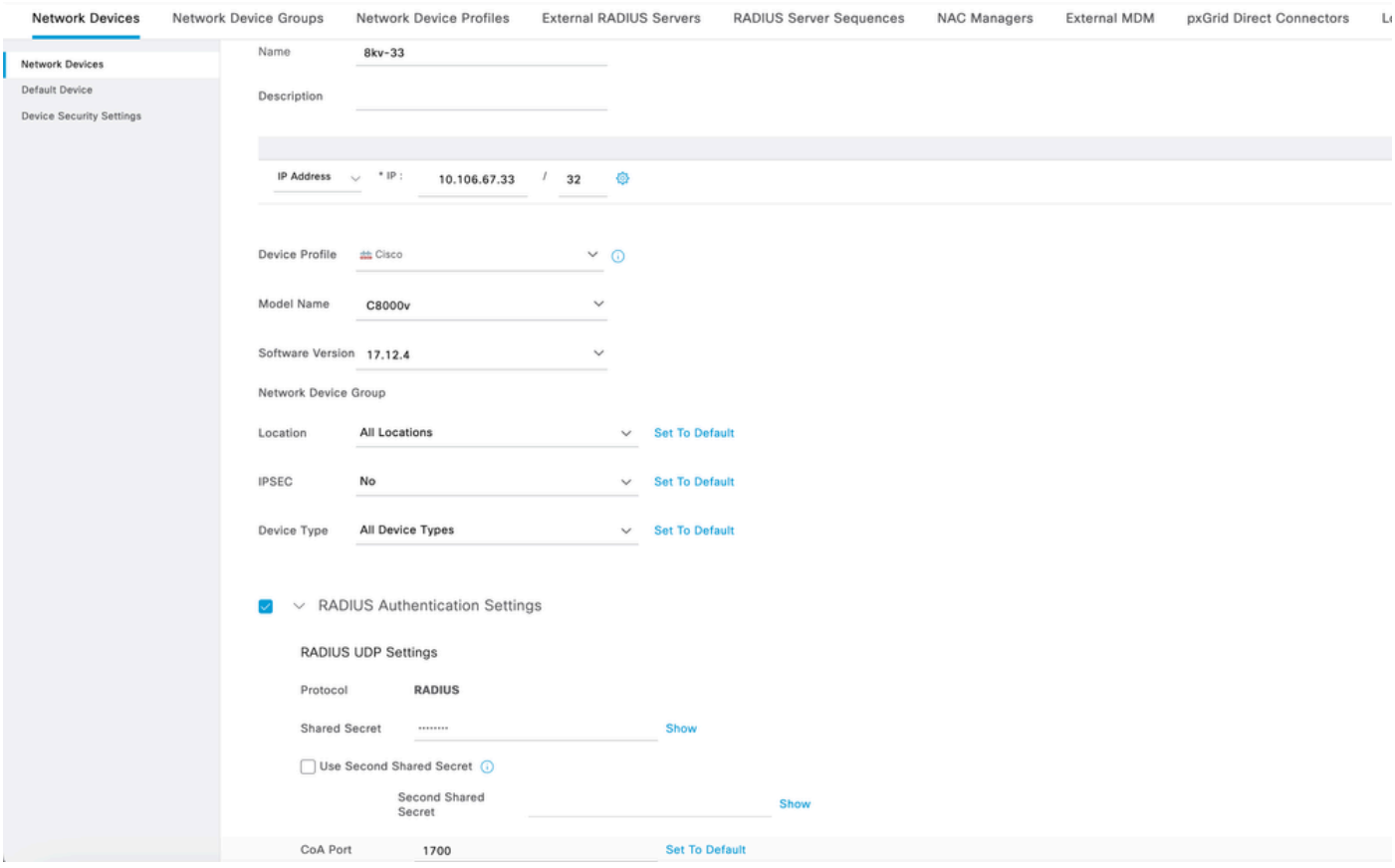
<#root>

```
<?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>
```

تكوين محرك خدمات الهوية (ISE)

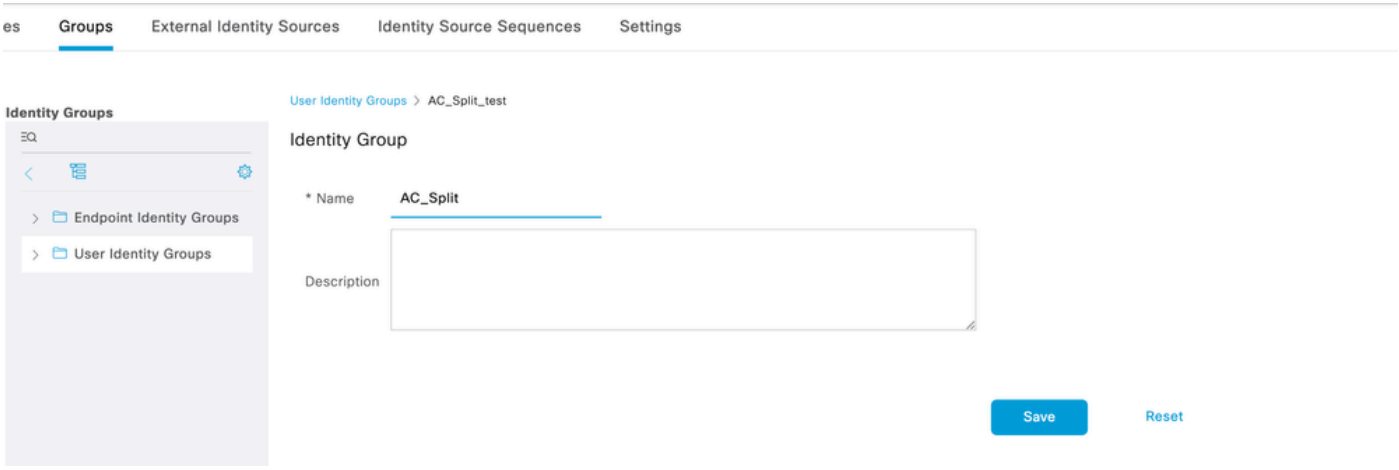
1. سجل الموجه كجهاز شبكة صالح على ISE وقم بتكوين المفتاح السري المشترك ل RADIUS. لذا، انتقل إلى إدارة > موارد الشبكة > أجهزة الشبكة. انقر فوق إضافة لتكوين الموجه كعميل AAA:



إضافة جهاز شبكة

2. إنشاء مجموعات الهوية:

قم بتعريف مجموعات الهوية لإقران المستخدمين بخصائص مماثلة والذين يتقاسمون أذون مماثلة. يتم إستخدام هذه العناصر في الخطوات التالية. انتقل إلى إدارة > إدارة الهوية > مجموعات > مجموعات هوية المستخدم، ثم انقر فوق إضافة:



إنشاء مجموعة هوية

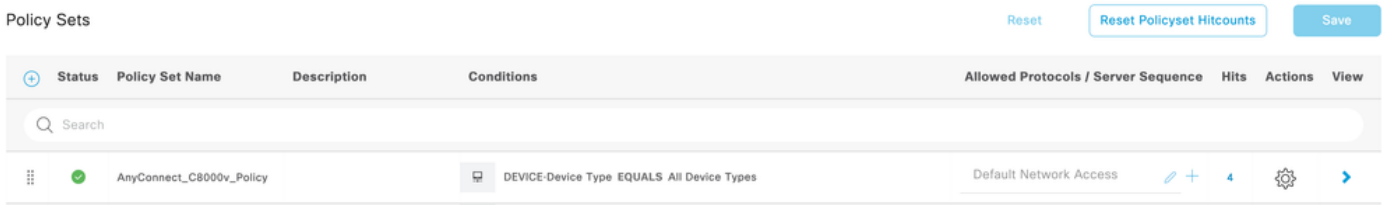
3. إقران المستخدمين بمجموعات الهوية:

إقران المستخدمين بمجموعة الهوية الصحيحة. انتقل إلى إدارة > إدارة الهوية > الهويات > المستخدمين.

إضافة مستخدم إلى مجموعة الهوية

4. إنشاء مجموعة سياسات:

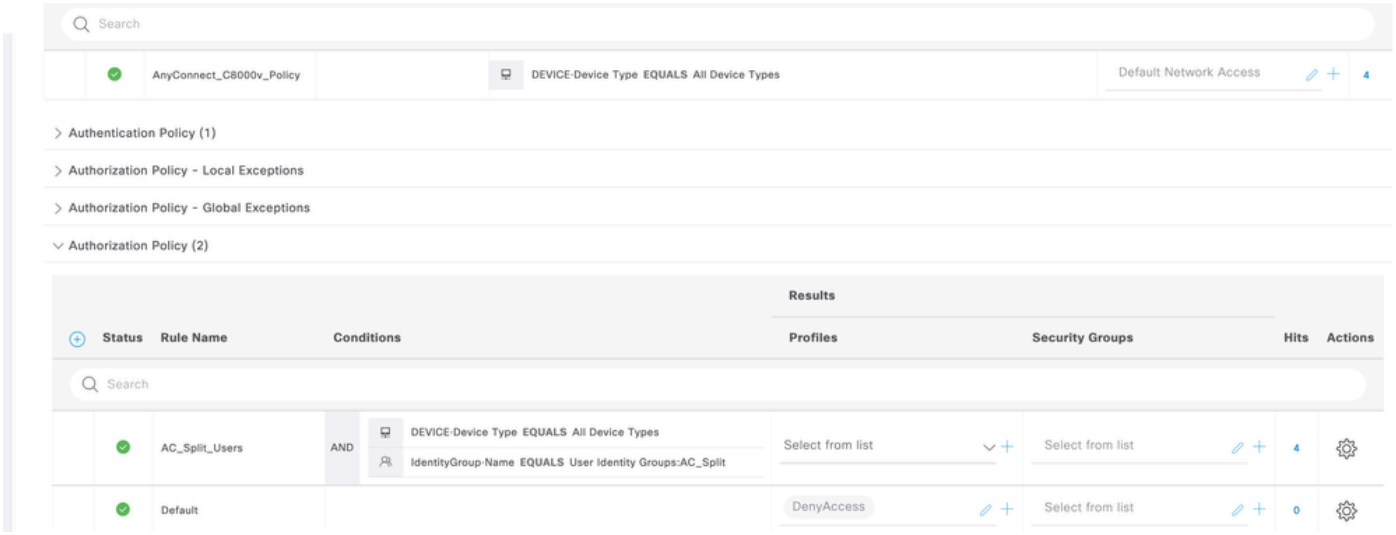
قم بتحديد مجموعة سياسات جديدة وتحديد الشروط التي تطابق السياسة. في هذا المثال، يتم السماح بجميع أنواع الأجهزة تحت الشروط. للقيام بذلك، انتقل إلى النهج>مجموعات النهج:



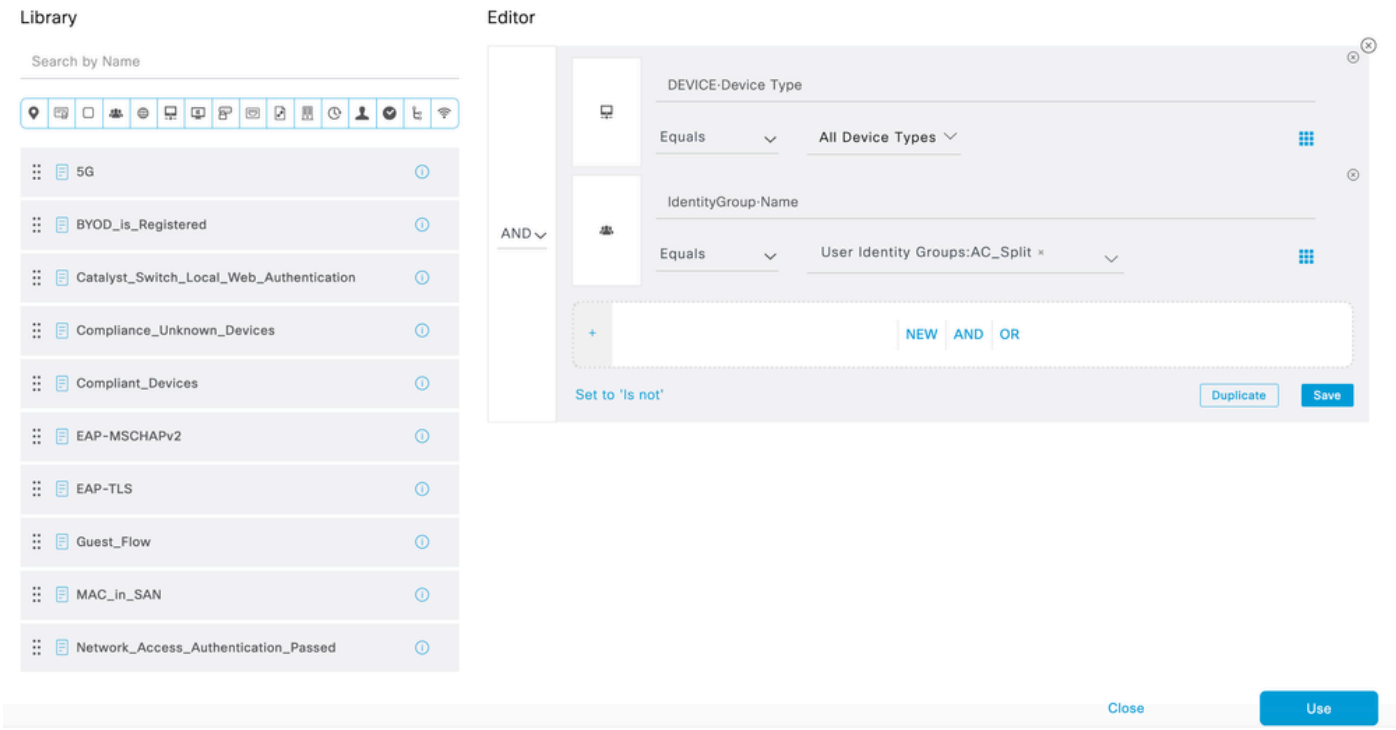
إنشاء مجموعة نهج

5. إنشاء سياسة تخويل:

قم بتحديد نهج تخويل جديد بالشروط المطلوبة لمطابقة النهج. تأكد من تضمين مجموعات الهوية التي تم إنشاؤها في الخطوة 2 كشرط.



إنشاء سياسة التخويل

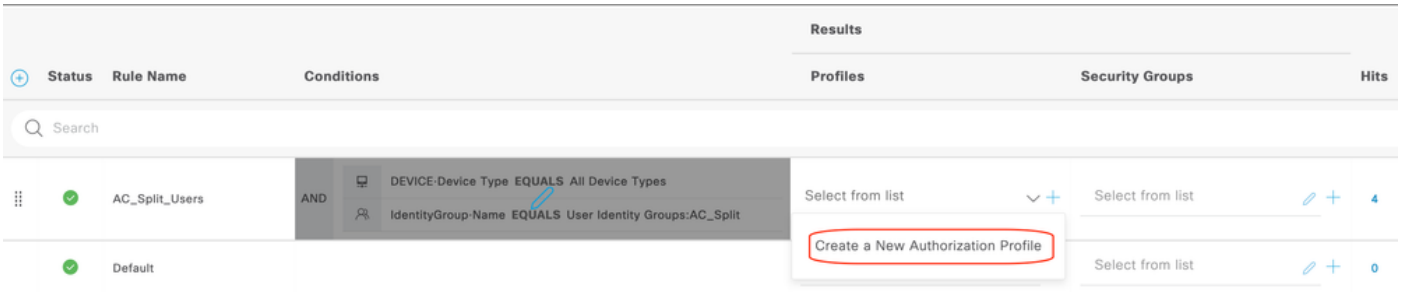


إختيار شروط في نهج التخويل

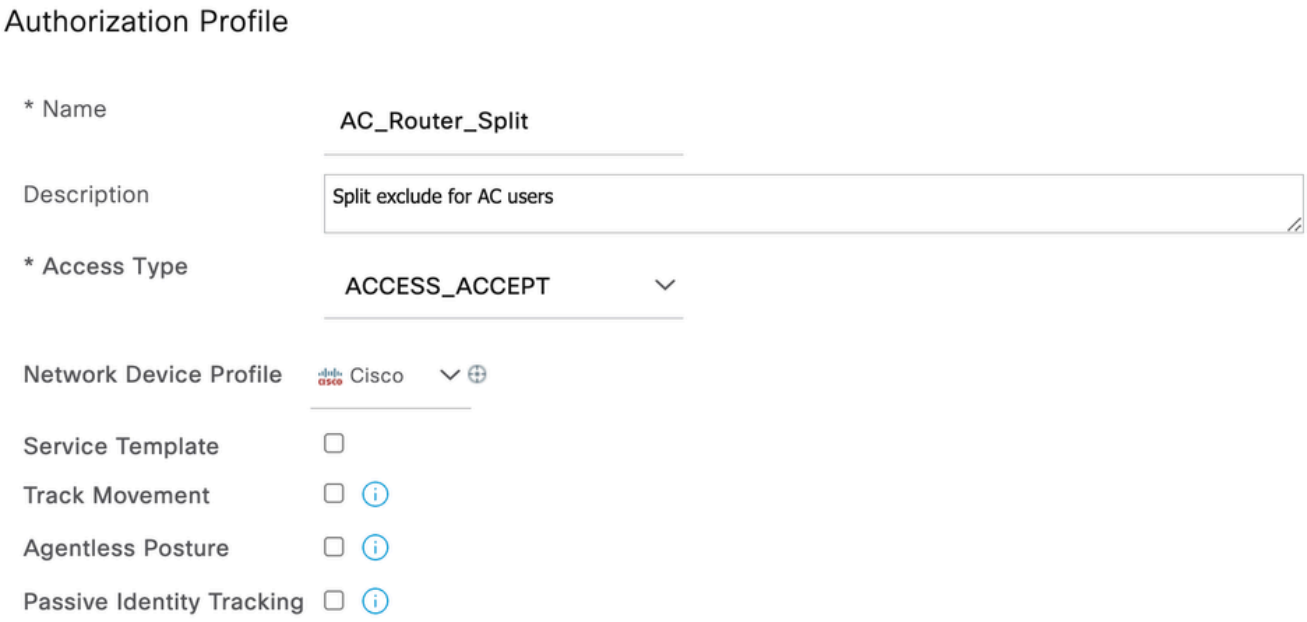
6. إنشاء ملف تعريف تخويل:

يتضمن ملف تعريف التخويل الإجراءات التي يتم إتخاذها عند مطابقة سياسة التخويل.
إنشاء ملف تعريف تخويل جديد يتضمن السمات التالية:

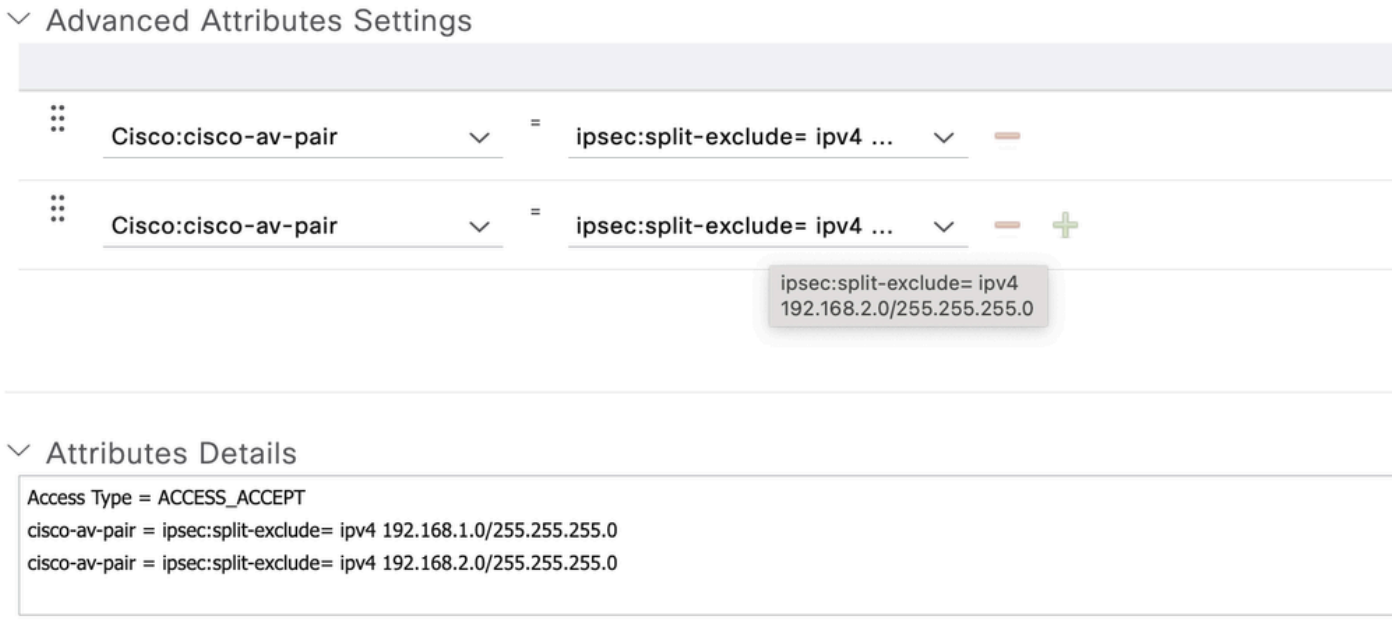
نوع الوصول = ACCESS_ACCEPT
Cisco-av-pair = ipsSec:split-exclude= IPv4 <ip_network>/<subnet_mask>



إنشاء ملف تعريف تخويل جديد

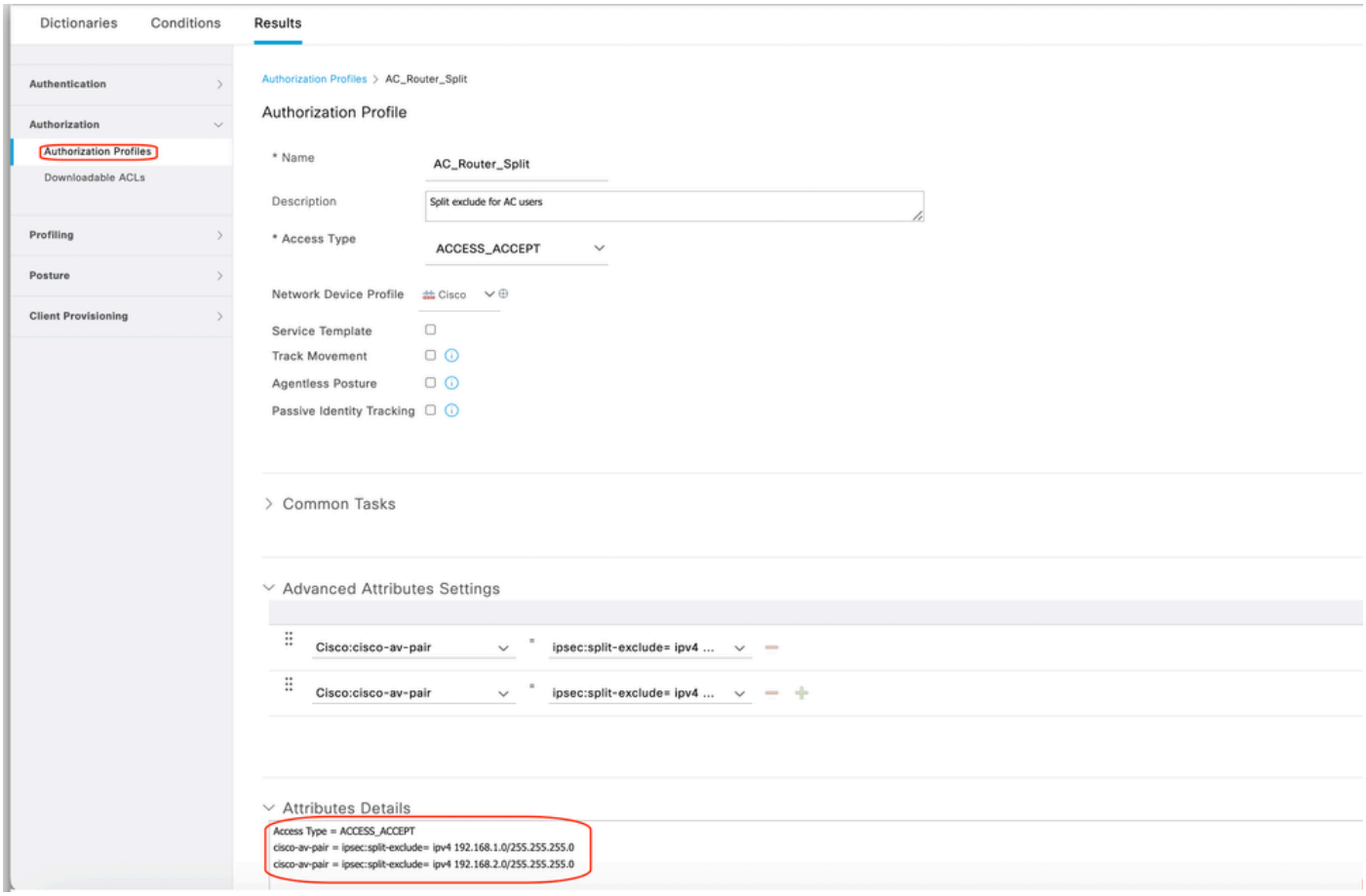


تكوين ملف تعريف التخويل



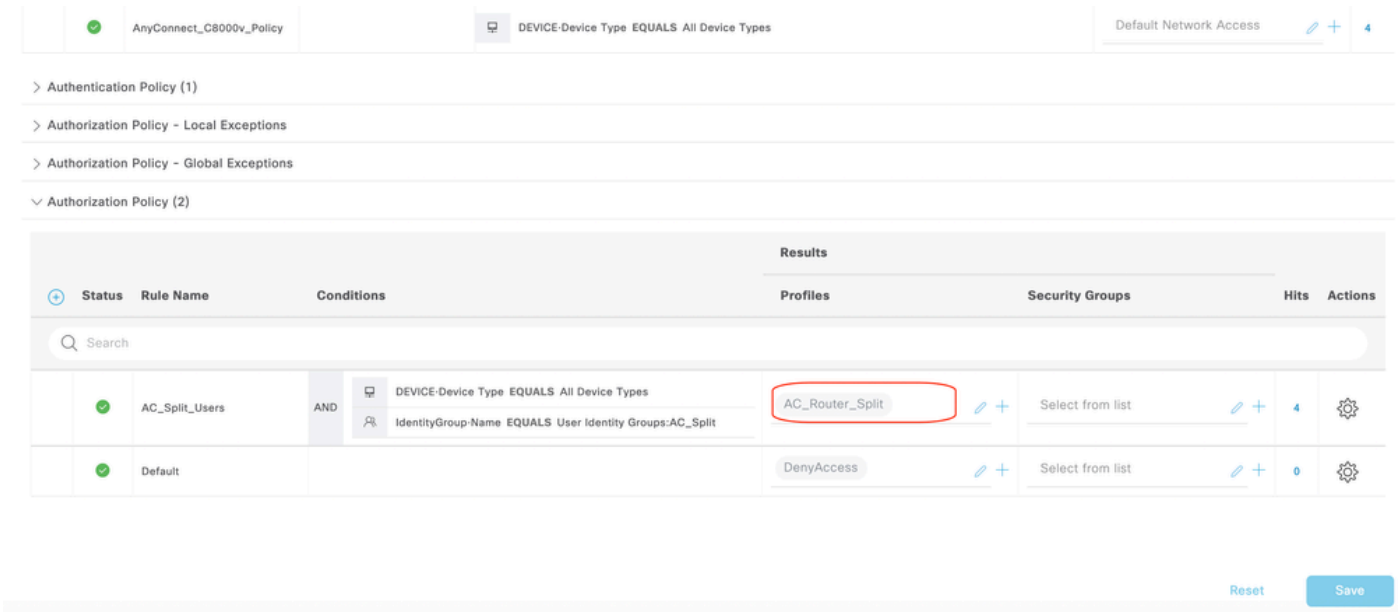
تكوين السمات في ملف تعريف التخويل

7. مراجعة تكوين ملف تعريف التخويل.



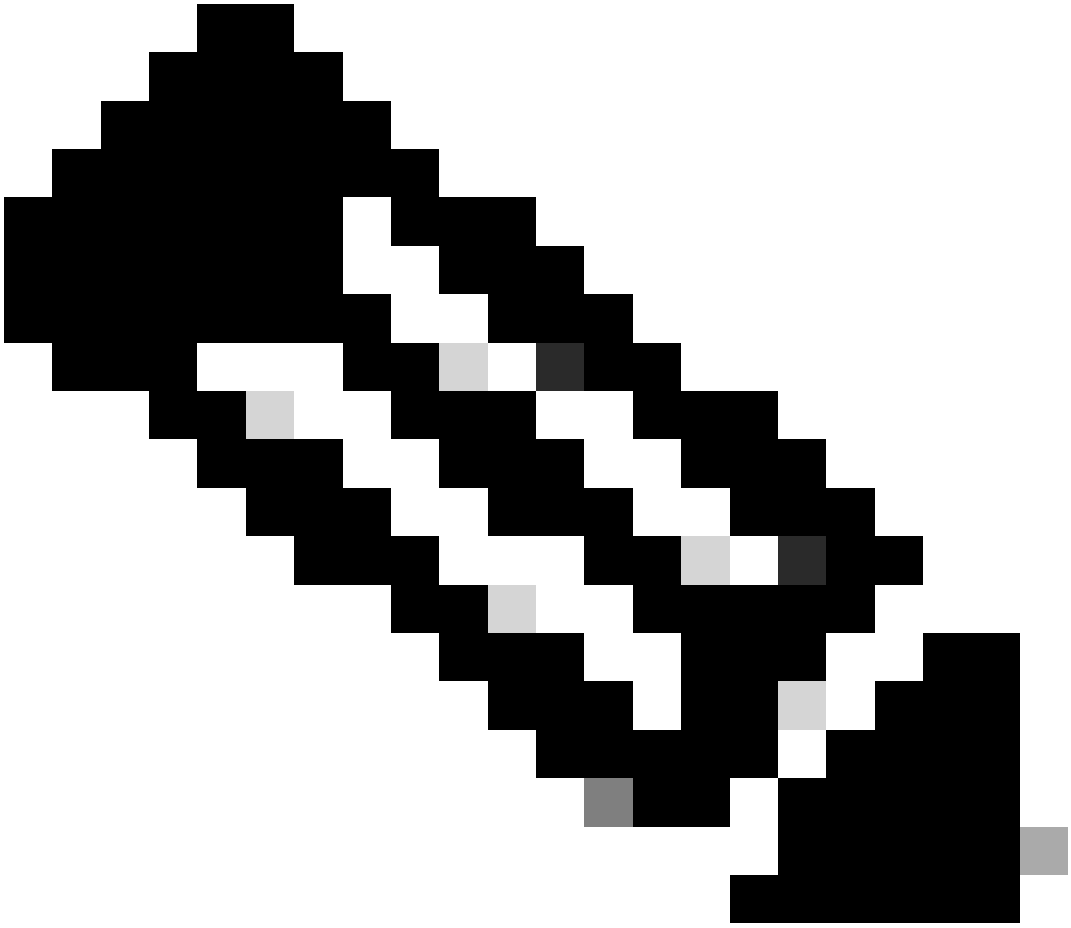
مراجعة تكوين ملف تعريف التخويل

8. هذا هو نهج التخويل في تكوين مجموعة النهج بعد تحديد ملفات التعريف المطلوبة:



التكوين النهائي لنهج التخويل

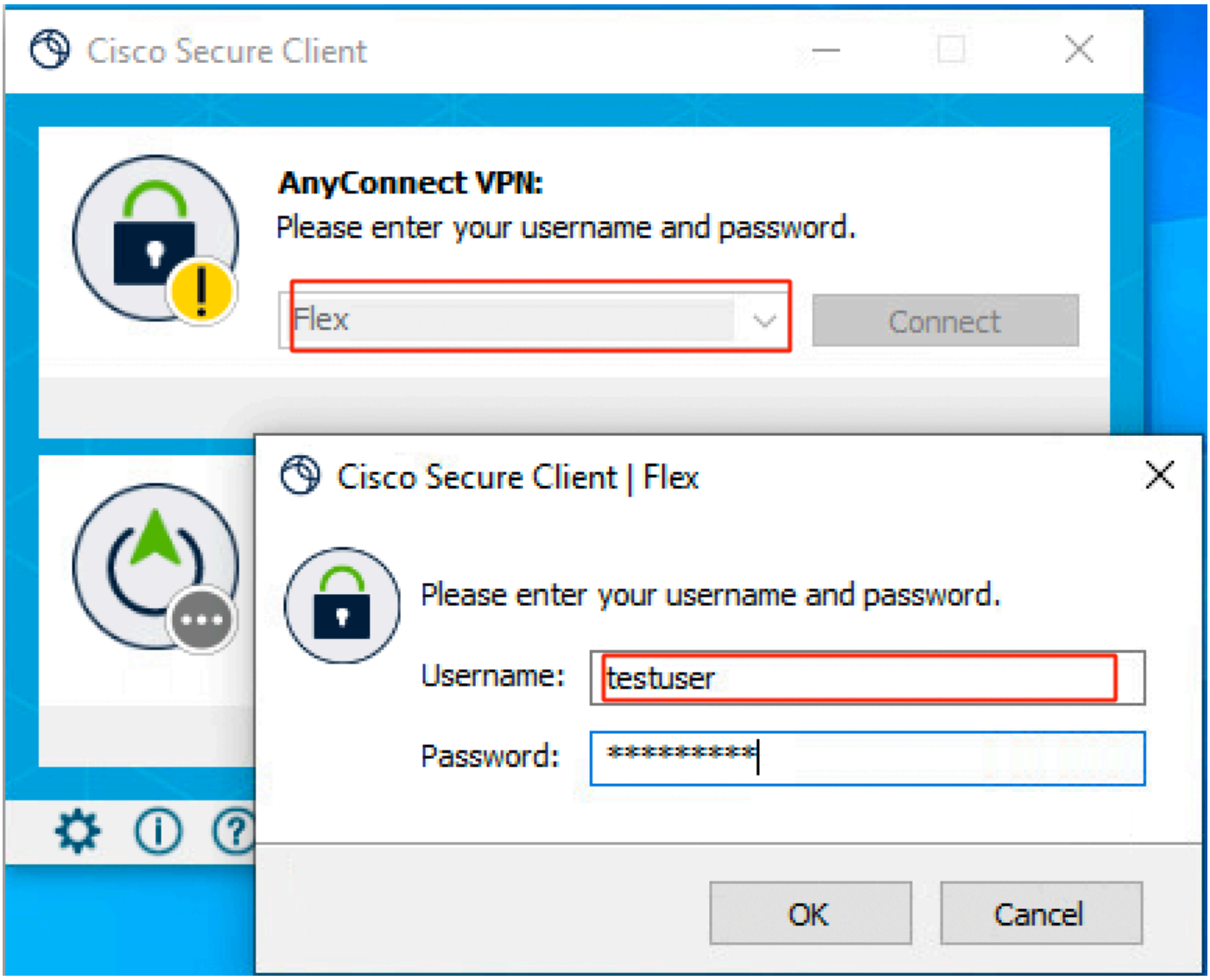
مع مثال التكوين هذا، يمكنك إستبعاد الشبكات من المرور عبر شبكة VPN من خلال تكوين ISE القائم على مجموعة الهوية التي ينتمي إليها المستخدم.



ملاحظة: يمكن دفع شبكة فرعية واحدة فقط لاستثناء النفق إلى جهاز الكمبيوتر العميل عند إستخدام وحدة الاستقبال والبث الخاصة ب Cisco IOS XE لاتصال RA VPN. وقد تم معالجة هذا الأمر بواسطة معرف تصحيح الأخطاء من Cisco CSCwj38106 ويمكن دفع شبكات فرعية متعددة ذات فصل-إستثناء من 17.12.4. ارجع إلى الخط للحصول على مزيد من التفاصيل حول الإصدارات الثابتة.

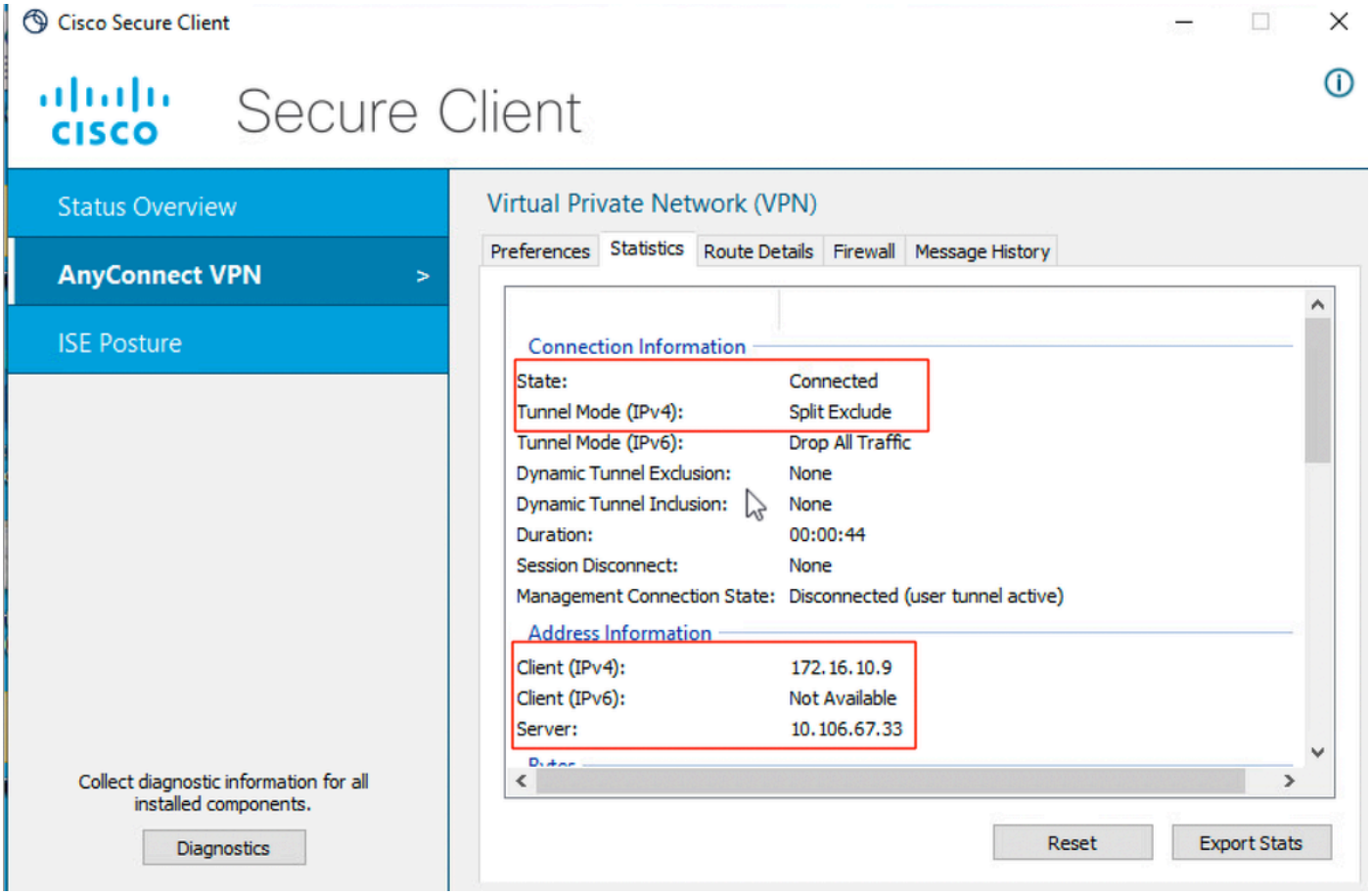
التحقق من الصحة

1. لاختبار المصادقة، قم بالاتصال بالطراز C8000V من كمبيوتر المستخدم من خلال AnyConnect وأدخل بيانات الاعتماد.



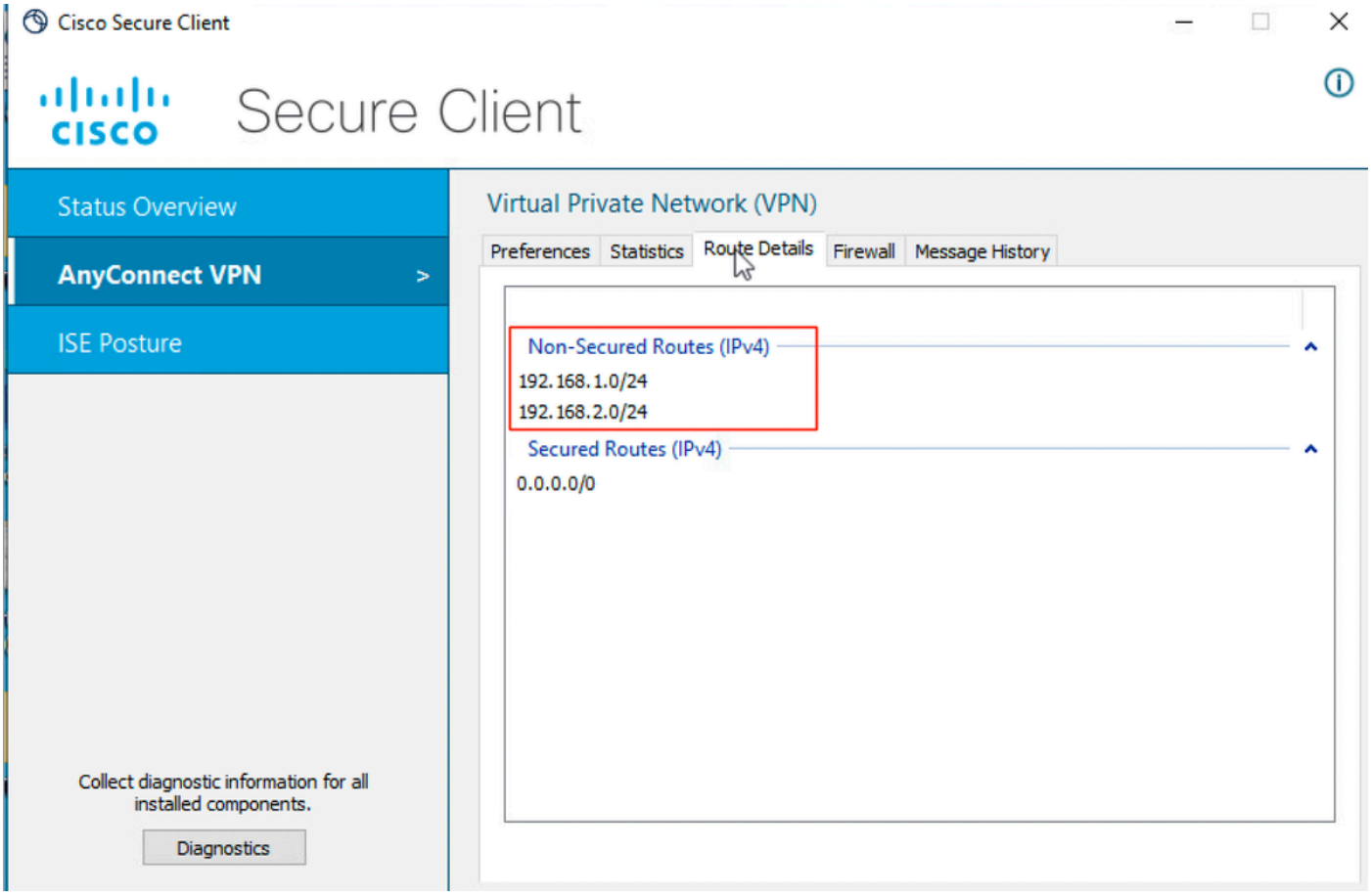
تسجيل الدخول إلى AnyConnect

2. بمجرد تأسيس الاتصال، انقر فوق أيقونة العتاد (الزاوية اليسرى السفلى) وانتقل إلى AnyConnect VPN > Statistics. تأكيد إستبعاد وضع النفق المرار تقسيمه.



التحقق من صحة الإحصائيات

انتقل إلى AnyConnect VPN > تفاصيل المسار وتأكد من أن المعلومات المعروضة تتوافق مع المسارات الآمنة والمسارات غير الآمنة.



التحقق من صحة تفاصيل المسار

كما يمكنك التحقق من تفاصيل الاتصال على وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (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.

استكشاف الأخطاء وإصلاحها

على موجه Cisco:

1. أستخدم تصحيح أخطاء IKEv2 و IPsec للتحقق من التفاوض بين وحدة الاستقبال والبث والعميل.

```
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. أستخدم أخطاء المصادقة والتفويض والمحاسبة (AAA) للتحقق من تعيين السمات المحلية و/أو البعيدة.

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

على ISE:

أستخدم سجلات RADIUS المباشرة بالتنقل إلى العمليات > سجلات البث المباشر.

سيناريو العمل

هذا هو تصحيح أخطاء الاتصال الناجح:

<#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#
```

المراجع

- تكوين وحدة الاستقبال والبث FlexVPN للوصول عن بعد لـ IKEv2 باستخدام قاعدة بيانات المستخدم المحلي
- تكوين AnyConnect FlexVPN باستخدام مصادقة EAP و DUO
- تكوين الوصول عن بعد إلى AnyConnect IKEv2 باستخدام EAP-MD5

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).