تكوين FlexVPN باستخدام تكامل ISE

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين FlexVPN باستخدام محرك خدمات الهوية (ISE) من Cisco لتعيين التكوينات للأجهزة بشكل ديناميكي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين محرك خدمات الهوية من Cisco (ISE)
- بروتوكول RADIUS
- الشبكة الخاصة الظاهرية المرنة (FlexVPN)

المكونات المستخدمة

يستند هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco CSR1000V (VXE) - الإصدار 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1

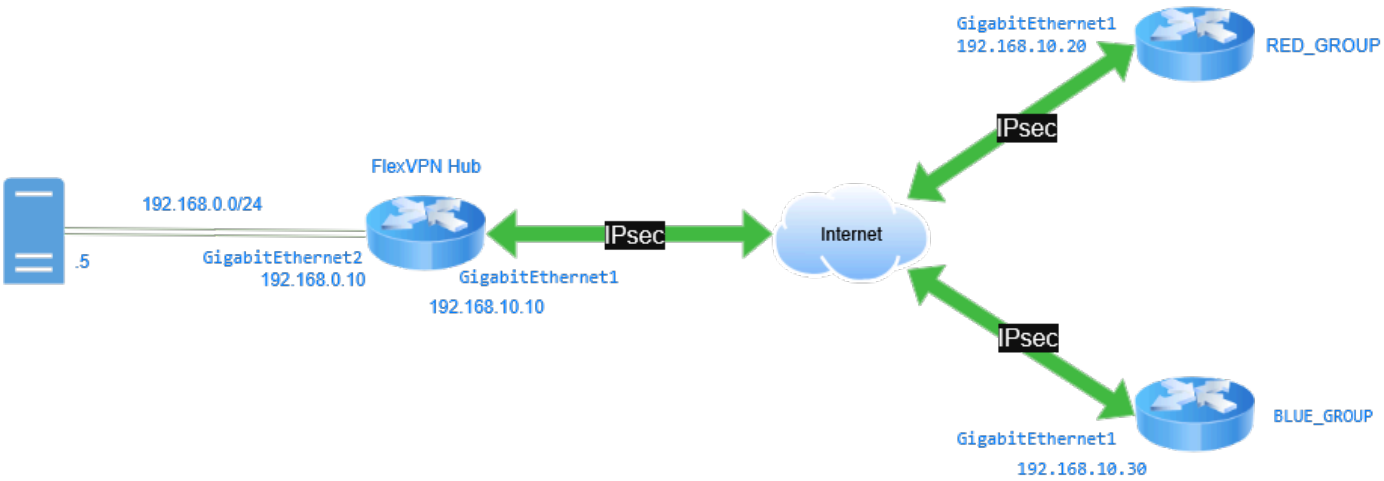
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة

يمكن أن تقوم FlexVPN بإنشاء اتصال بالأسلاك وتخصيص تكوينات معينة تتيح إدارة الاتصالات وحركة مرور البيانات. استنادا إلى المخطط، يوضح هذا كيفية تكامل FlexVPN مع ISE حتى، عند اتصال كلمة ما بالموجه، يتم تعيين معلمات مصدر النفق وتجمع DHCP وفقا للمجموعة أو الفرع الذي ينتمي إليه المتحدث. إنه يستخدم الترخيص لمصادقة الفروع، ثم ISE مع RADIUS كخادم تخويل ومحاسبة.



FlexVPN مع دمج ISE

الخطوة 1: تكوين الموزع

أ. قم بتكوين atrustpointلتخزين شهادة الموجه. يتم إستخدام الشهادات لمصادقة الفروع.

```
crypto pki trustpoint FlexVPNCA
  enrollment url http://10.10.10.10:80
  subject-name cn=FlexvpnServer, o=Cisco, OU=IT_GROUP
  revocation-check crl
```

ب. تكوين **certificate map**. الغرض من certificate map الموجه هو تعريف ومطابقة الشهادات استنادا إلى المعلومات المحددة، في حالة أن الموجه لديه شهادات متعددة مثبتة.

```
crypto pki certificate map CERT_MAP 5
  issuer-name co ca-server.cisco.com
```

ج. تكوين aRADIUS serverللتخويل والمحاسبة على الجهاز:

```
aaa new-model
!
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
```

د. قم بتعريف **RADIUS server group** الأمر باستخدام عنوان IP الخاص به ومنفذ الاتصال والمفاتيح المشترك وواجهة المصدر لحركة مرور RADIUS.

```
radius server ISE25
  address ipv4 192.168.0.5 auth-port 1645 acct-port 1646
  key cisco1234

aaa group server radius ISE
  server name ISE25
  ip radius source-interface g2
```

هـ. قم بتكوين **loopback interfaces**. يتم إستخدام هذه loopback interfaces الوصلة كاتصال مصدر للنفق ويتم تعيينها ديناميكيا وفقا للمجموعة المتصلة.

```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

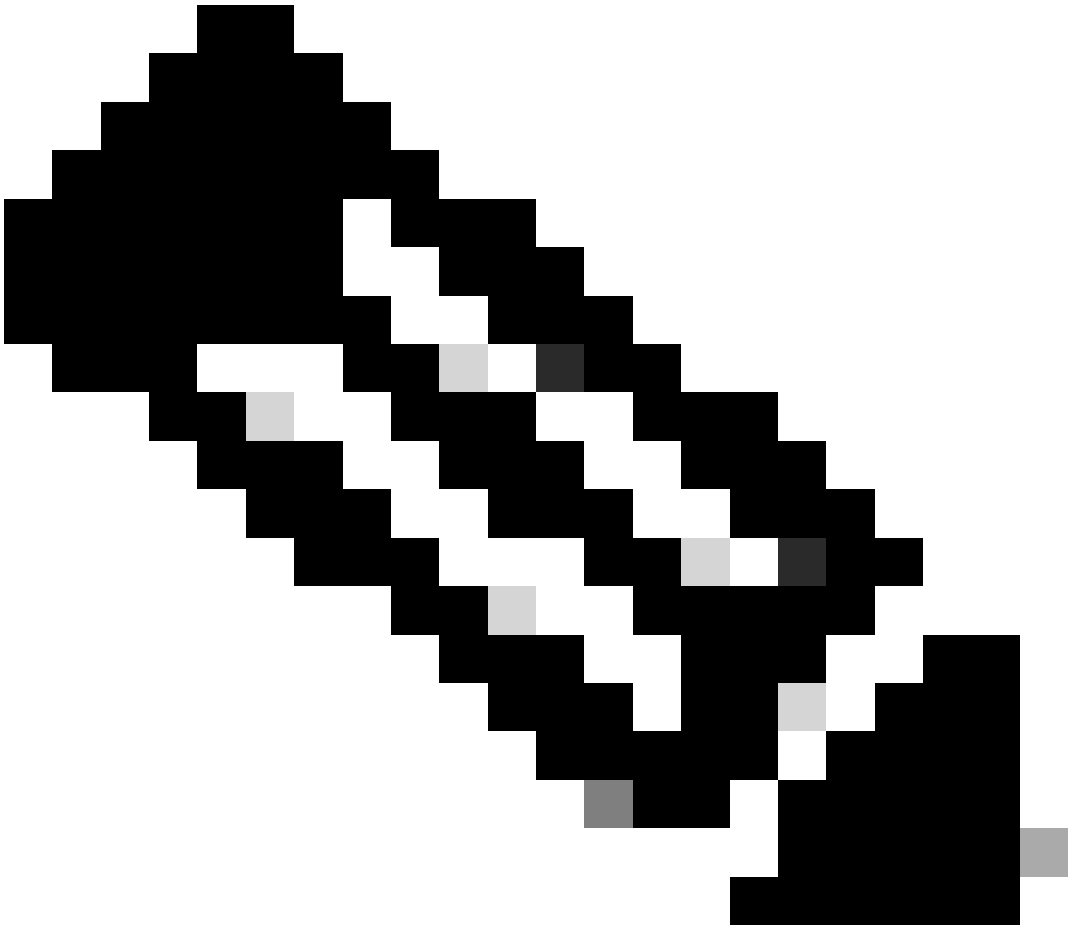
و. قم بتعريف **IP local pool** لكل مجموعة.

```
ip local pool RED_POOL 172.16.10.10 172.16.10.254
ip local pool BLUE_POOL 172.16.0.10 172.16.0.254
```

ز. تكوين EIGRP والإعلان عن شبكات كل مجموعة.

```
router eigrp Flexvpn
address-family ipv4 unicast autonomous-system 10
topology base
exit-af-topology
network 10.100.100.0 0.0.0.255
network 10.10.1.0 0.0.0.255
network 10.200.200.0 0.0.0.255
network 10.10.2.0 0.0.0.255
```

```
network 172.16.0.0
```



ملاحظة: تدعم FlexVPN بروتوكولات التوجيه الديناميكية مثل EIGRP و OSPF و BGP عبر أنفاق شبكة VPN. في هذا الدليل، يتم إستخدام EIGRP.

ج. قم بتكوين **crypto ikev2 name mangler**. يتم إستخدام IKEv2 name mangler الأمر لاستخلاص اسم المستخدم لتفويض IKEv2. وفي هذه الحالة، يتم تكوينها لاستخدام معلومات Organization-Unit من الشهادات الموجودة على الفرع كاسم مستخدم للتخويل.

```
crypto ikev2 name-mangler NM
dn organization-unit
```

ط. قم بتكوين **IKEv2 profile**. تتم الإشارة إلى certificate map، AAA server groupو name mangler، في ملف تعريف IKEv2.

يتم تكوين المصادقة المحلية والمصادقة عن بعد على النحو RSA-SIGالتالي في هذا السيناريو المحدد.

يجب إنشاء حساب مستخدم محلي على RADIUS server أساس اسم مستخدم يتطابق مع قيمةorganization-unitCisco1234وكلمة المرور (كما هو محدد في التكوين أدناه).

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint FlexVPNCA
dpd 10 2 periodic
aaa authorization group cert list FLEX name-mangler NM password Cisco1234
aaa accounting cert FLEX
virtual-template 1 mode auto
```

ي. قم بتكوينIPsec profileومرجع IKEv2 profile.

```
crypto ipsec profile IPSEC_FlexPROFILE
set ikev2-profile Flex_PROFILE
```

ك. إنشاء virtual-template. يتم إستخدامه لإنشاء virtual-access interface وارتباط IPsec profile الذي تم إنشاؤه.

ثبتت ال **virtual-template** مع ام من عنوان، بما أن هذا يكون عينت ب ال RADIUS server.

```
interface Virtual-Template2 type tunnel
no ip address
tunnel source GigabitEthernet1
tunnel destination dynamic
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

قم بتكوين إثنينloopbacksلمحاكاة شبكة داخلية.

```
interface Loopback1010
ip address 10.10.1.10 255.255.255.255
!
interface Loopback1020
ip address 10.10.2.10 255.255.255.255
```

الخطوة 2: التكوين الذي تم التحدث به

أ. تكوينtrustpointلتخزين شهادة الموجه الذي تم التحدث عنه.

```
crypto pki trustpoint FlexVPNSpoke
 enrollment url http://10.10.10.10:80
 subject-name cn=FlexVPNSpoke, o=Cisco, OU=RED_GROUP
 revocation-check crl
```

ب. تكوينcertificate map. الغرض من certificate map الموجه هو تعريف ومطابقة الشهادات استنادا إلى المعلومات المحددة، في حالة أن الموجه لديه شهادات متعددة مثبتة.

```
crypto pki certificate map CERT_MAP 5
issuer-name co ca-server.cisco.com
```

c. تكوين شبكة التخويل المحلية ل AAA.

يتم إستخدام أمر شبكة تفويض المصادقة والتفويض والمحاسبة (AAA) لتفويض طلبات الوصول المتعلقة بخدمات الشبكة. ويتضمن التحقق مما إذا كان لدى المستخدم إذن للوصول إلى الخدمة المطلوبة بعد التصديق.

```
aaa new-model
aaa authorization network FLEX local
```

د. قم بتكوينIKEv2 profile. تتم الإشارة إلى certificate map تخويل المصادقة والتفويض والمحاسبة (AAA) المحلي في IKEv2 profile.

يتم تكوين المصادقة المحلية والبعيدة على هيئة **RSA-SIG**.

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint FlexVPNSpoke
dpd 10 2 on-demand
aaa authorization group cert list FLEX default
```

هـ. قم بتكوينIPsec profileومرجع IKEv2 profile.

```
crypto ipsec profile IPSEC_FlexPROFILE
set ikev2-profile Flex_PROFILE
```

و. قم بتكوينtunnel interface. تم تكوين tunnel interface لتلقي عنوان IP للنفق من الصرة استنادا إلى نتائج التخويل.

```
interface Tunnel0
ip address negotiated
tunnel source GigabitEthernet1
tunnel destination 192.168.10.10
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

ز. قم بتكوين EIGRP، والإعلان عن الشبكة المحلية للكلام tunnel interface.

```
router eigrp 10
network 10.20.1.0 0.0.0.255
network 172.16.0.0
```

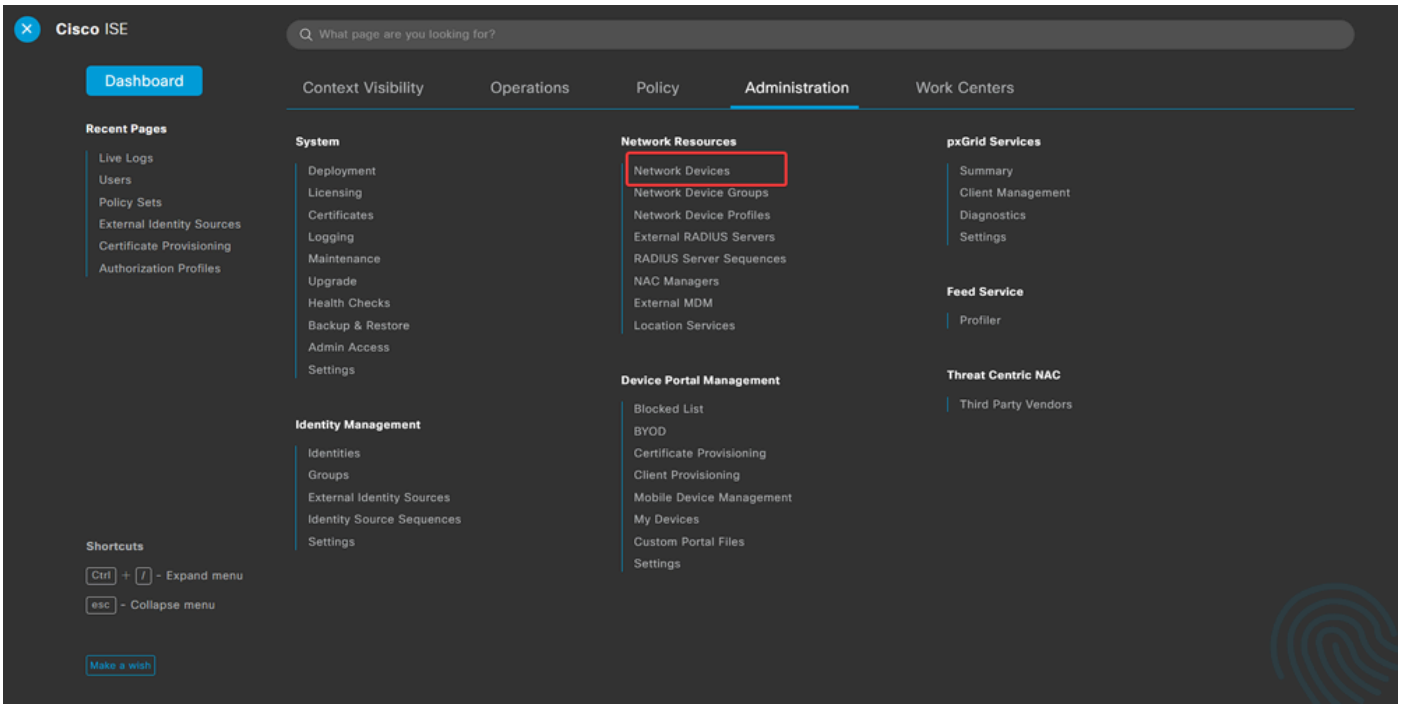
تكوين aloopbackلمحاكاة شبكة داخلية.

```
interface Loopback2010
ip address 10.20.1.10 255.255.255.255
```

الخطوة 3: تكوين ISE

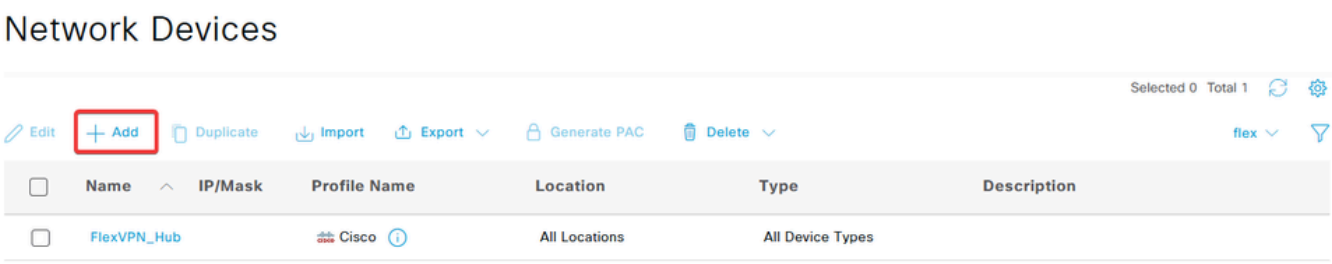
الخطوة 3.1: إنشاء مستخدمين ومجموعات وإضافة جهاز شبكة

أ. قم بتسجيل الدخول إلى خادم ISE وانتقل إلى **Administration > Network Resources > Network Devices**.



أجهزة شبكة موارد الإدارة

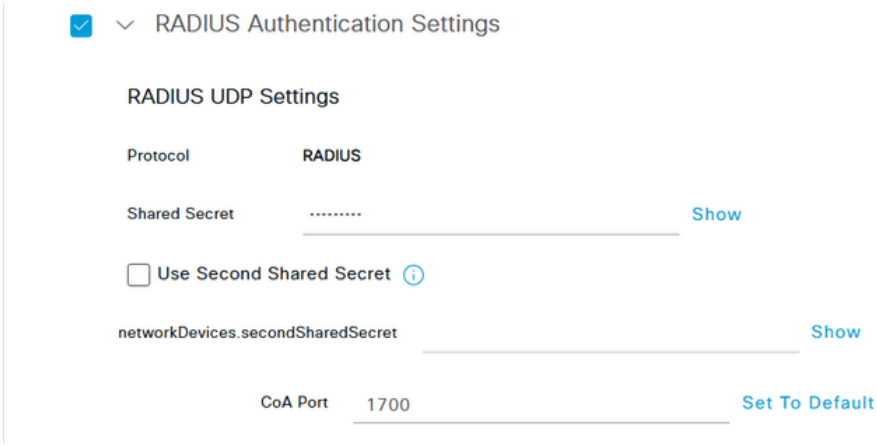
ب. انقر **Add** لتكوين موزع FlexVPN كعميل AAA.



إضافة موجه FlexVPN كعميل AAA

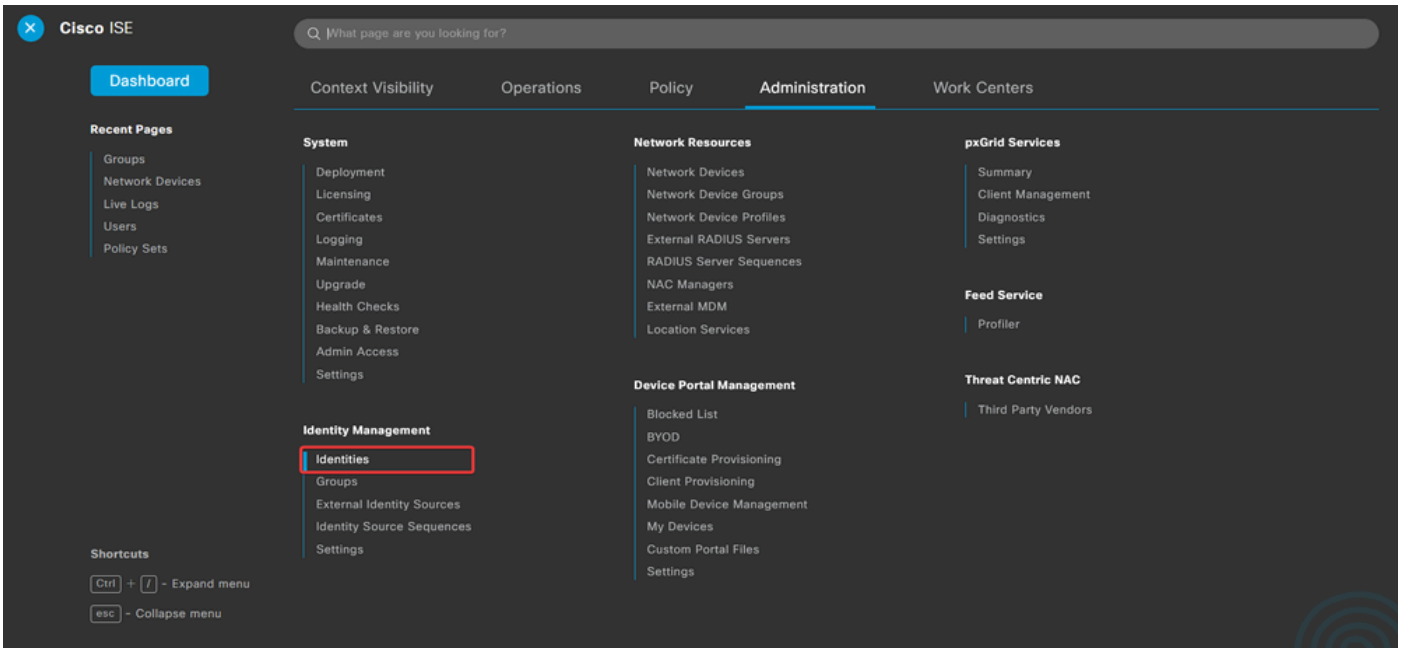
c. أدخل اسم جهاز الشبكة وحقل عنوان IP ثم **RADIUS Authentication Settings** حدد خانة الاختيار وأضف كلمة المرور السرية المشتركة **Shared Secret**. يجب أن تكون هي نفسها التي تم إستخدامها عند إنشاء مجموعة خادم RADIUS على لوحة وصل FlexVPN. انقر.Save

عنوان IP لجهاز الشبكة



المفتاح المشترك لجهاز الشبكة

د. انتقل إلى **Administration > Identity Management > Identities.**

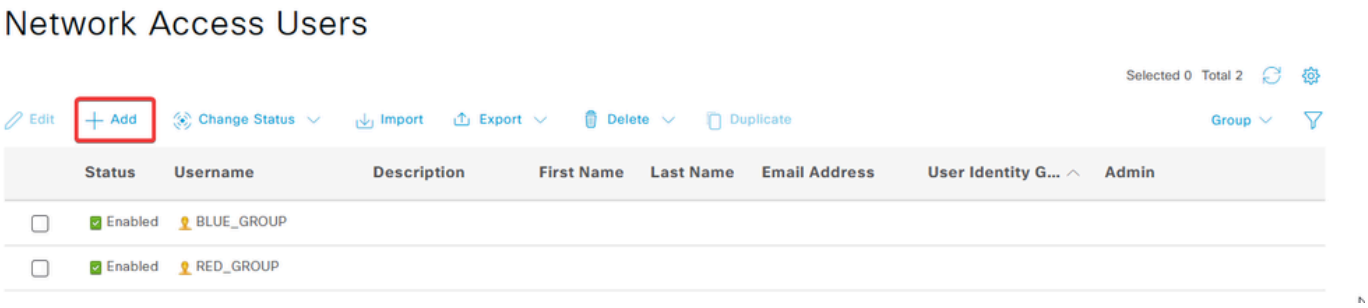


الإدارة - تعريف الإدارة - معرفات الإدارة

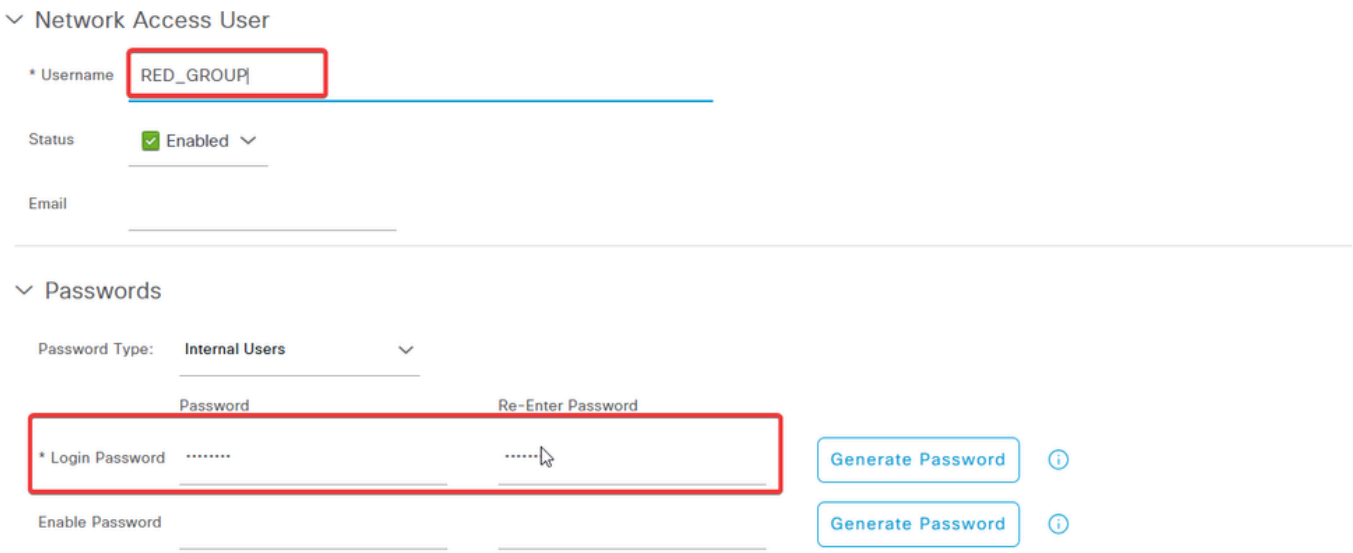
هـ. انقرAddلإنشاء مستخدم جديد في قاعدة البيانات المحلية للخادم.

أدخلUsernameو **Login Password**. اسم المستخدم هو نفس الاسم الذي تحتوي عليه الشهادات على قيمة المؤسسة-الوحدة في الشهادة ويجب أن تكون كلمة مرور تسجيل الدخول هي نفسها التي تم تحديدها في ملف تعريف IKev2.

انقر.**Save**



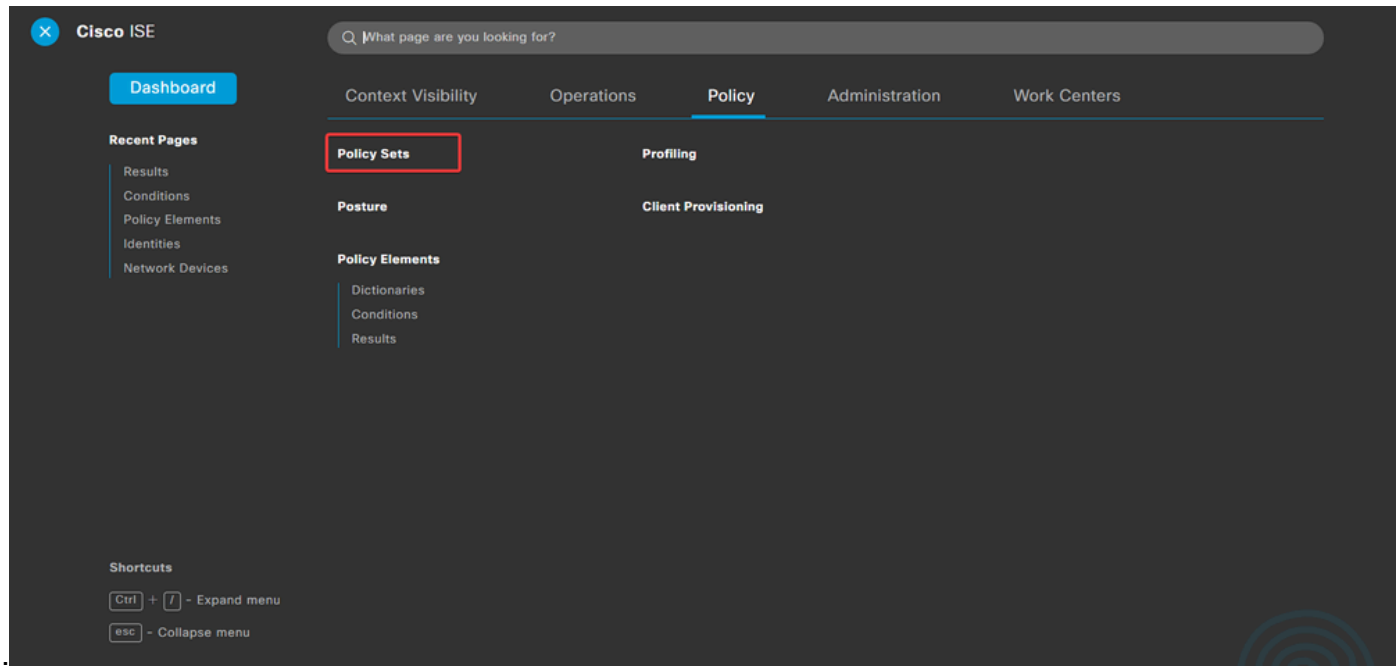
الإدارة - تعريف الإدارة - معرفات الإدارة



تم إنشاء المجموعة بنفس قيمة الوحدة التنظيمية

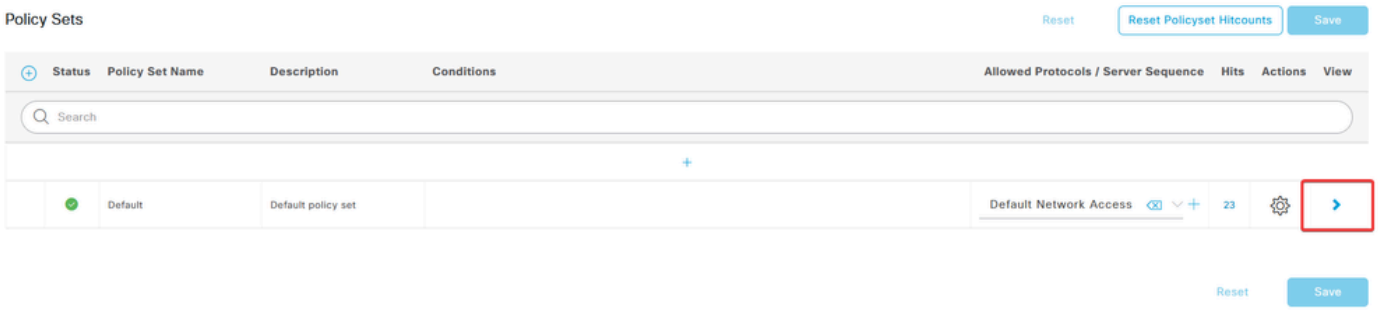
الخطوة 3.2: تكوين مجموعة النهج

أ. انتقل إلى **Policy** > **Policy Sets.**



مجموعات السياسات

ب. حدد نهج التخويل الافتراضي بالنقر فوق السهم الموجود على الجانب الأيمن من الشاشة:



تحرير النهج الافتراضي

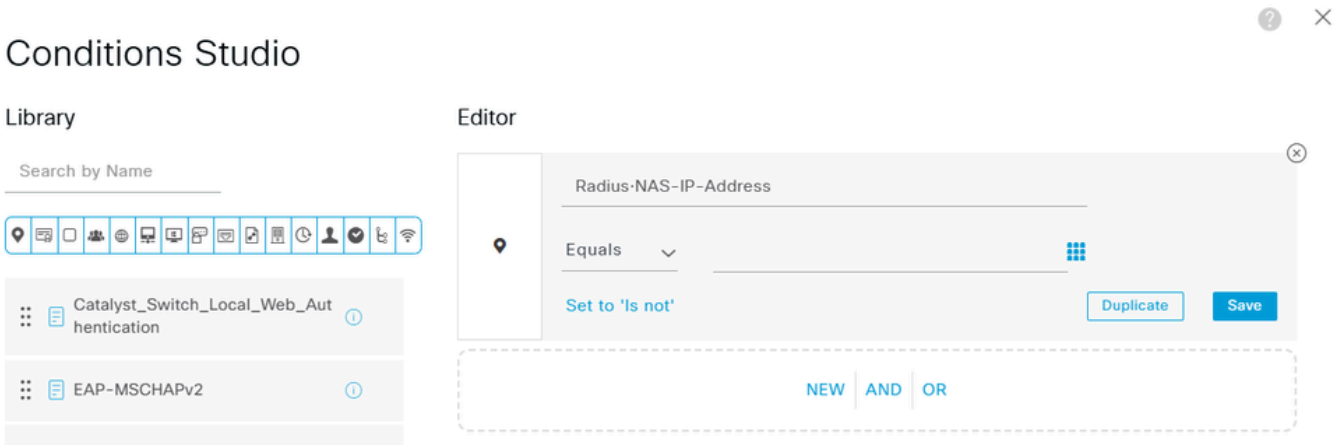
ج. انقر فوق سهم القائمة المنسدلة المجاورAuthentication Policyلتمديده. ثم انقر فوق الأيقونة **add (+)** لإضافة قاعدة جديدة.

إضافة نهج المصادقة

د. أدخل اسم القاعدة وحدد رمزadd (+)تحت عمود الشروط.

إنشاء سياسة مصادقة

هـ. انقر مربع نص محرر السمات وانقر فوقNAS-IP-Addressالأيقونة. دخلت العنوان (192.168.0.10) من FlexVPN صرة.

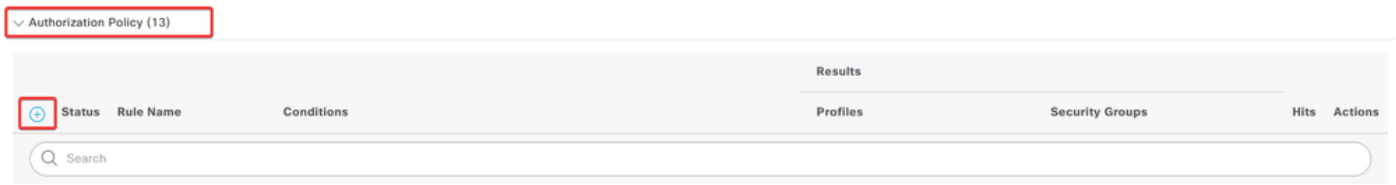


Authenticate FlexVPN Hub

نهج المصادقة

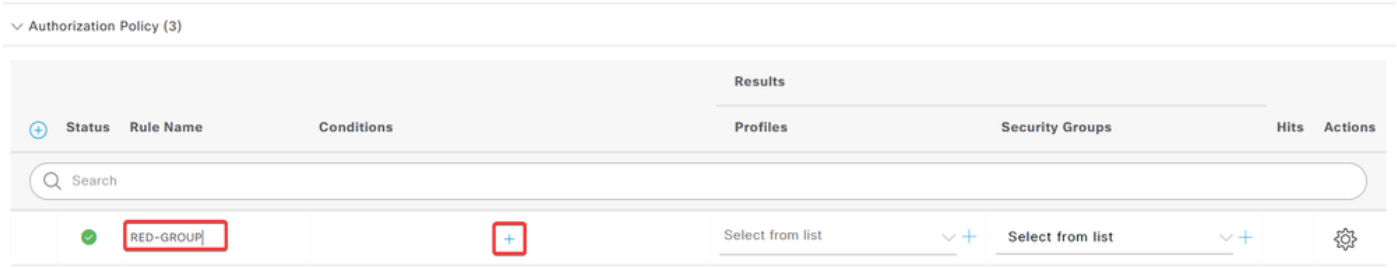
الخطوة 3.3: تكوين نهج التخويل

أ. انقر فوق سهم القائمة المنسدلة المجاورAuthorization Policyلتمديده. ثم انقر فوق الأيقونة **add (+)** لإضافة قاعدة جديدة.



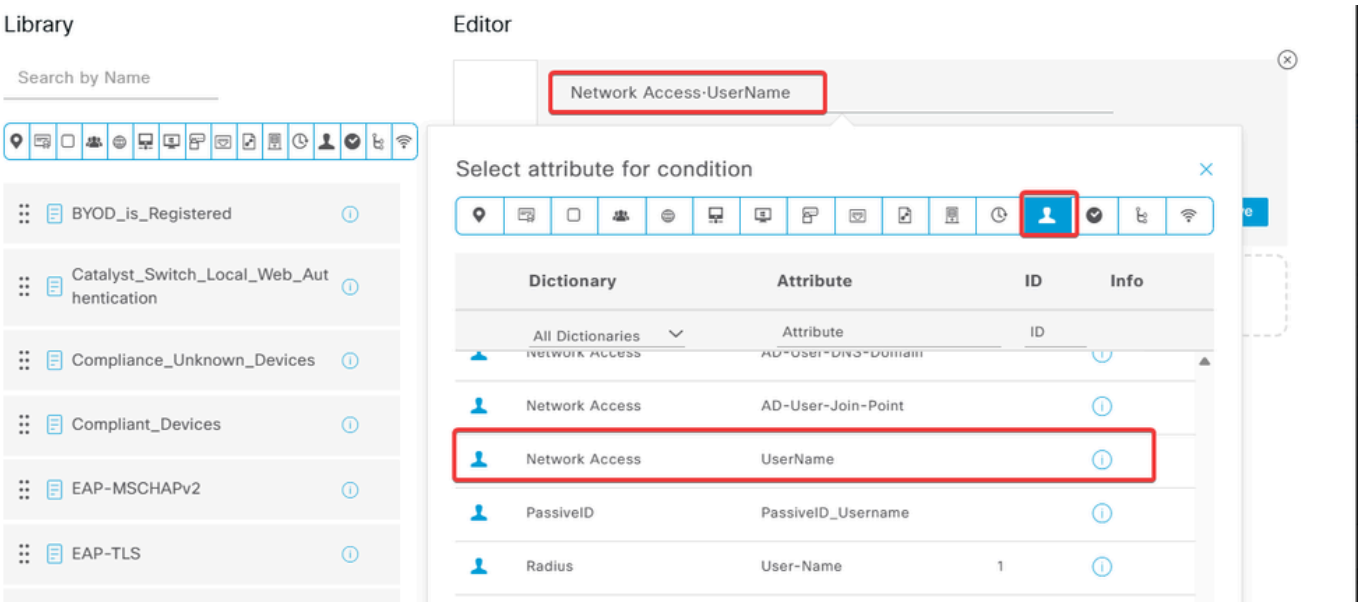
إنشاء نهج تخويل جديد

ب. **add (+)** أدخل اسم القاعدة وحدد الأيقونة تحت عمود الشروط.



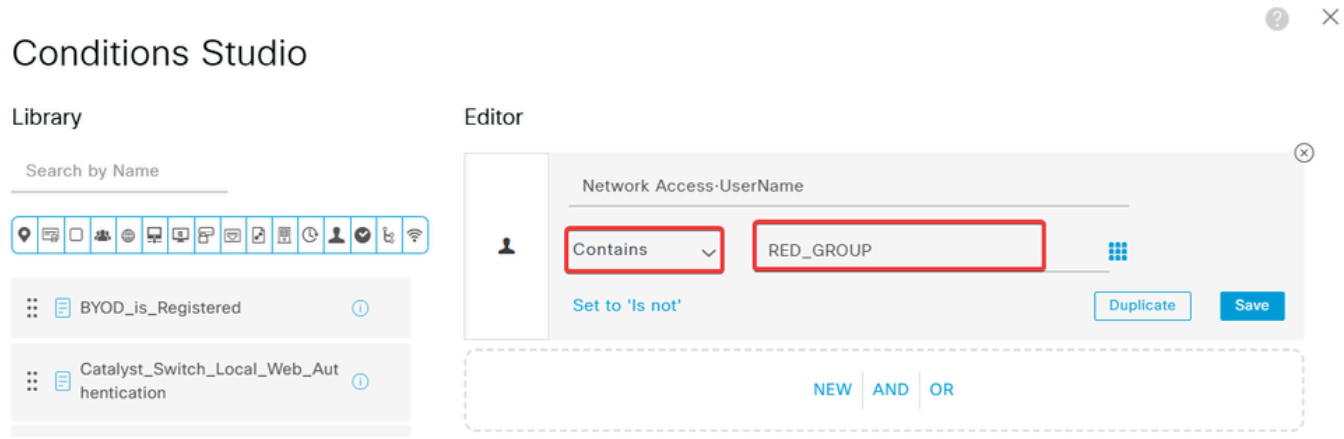
إنشاء قاعدة جديدة

ج. انقر مربع نص محرر السمات وانقر فوقSubjectالأيقونة. حدد **Network Access - UserName** السمة.



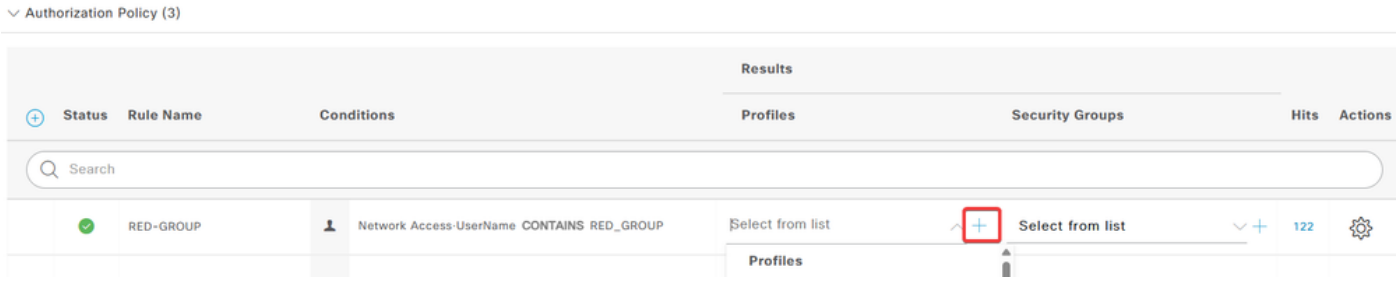
تحديد الوصول إلى الشبكة - اسم المستخدم

د. حددContainsكمشغل، ثم أضف قيمة المؤسسة-الوحدة للشهادات.



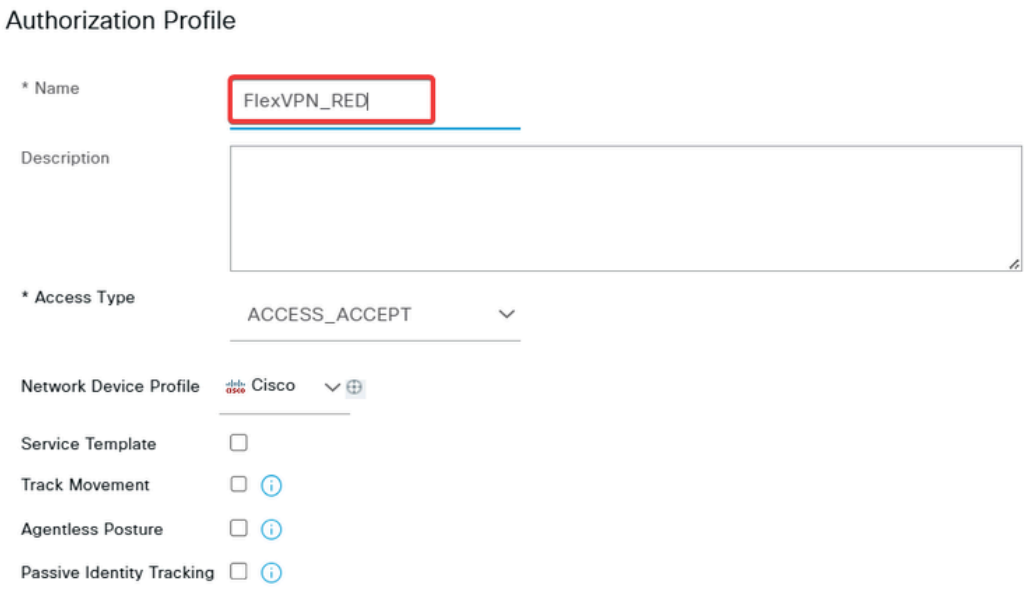
إضافة اسم مجموعة

هـ. في عامود التوصيفات، انقر علىadd (+)أيقونة واختر **Create a New Authorization Profile.**



إضافة ملف تعريف تخويل جديد

و. أدخل التوصيفName.



تسمية ملف تعريف التخويل

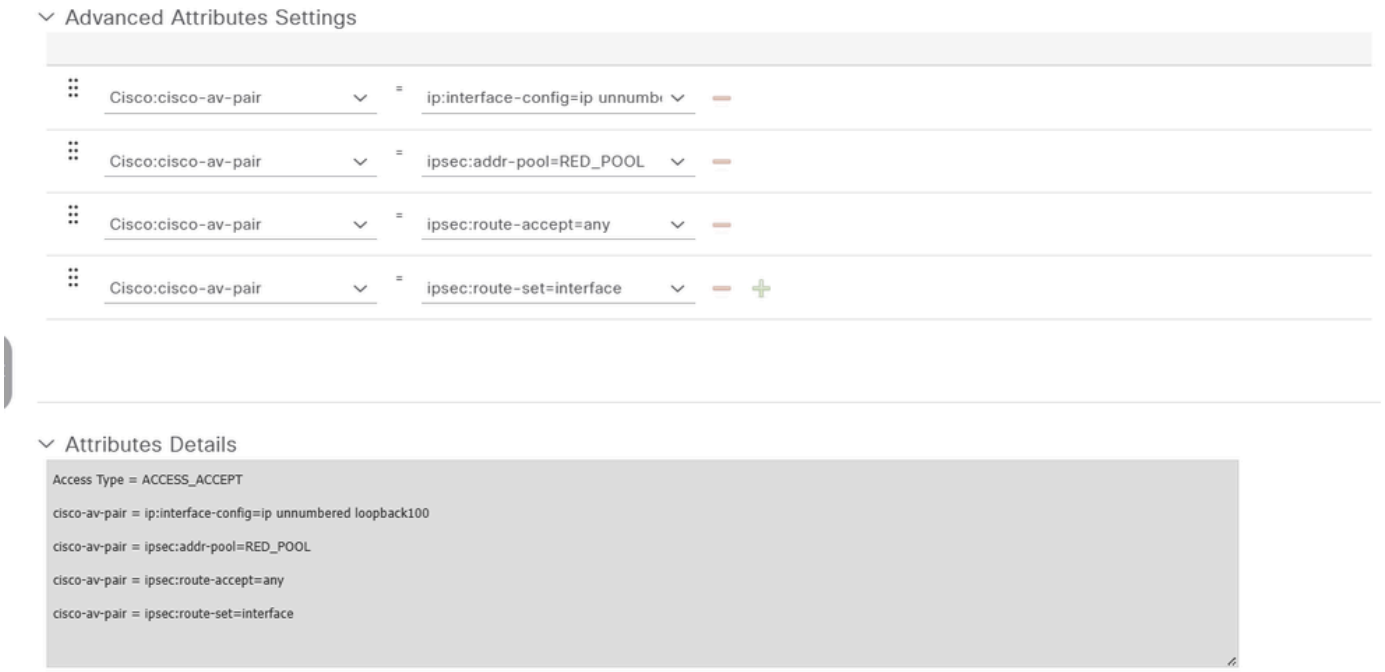
ز. انتقل إلى **Advanced Attributes Settings**. بعد ذلك، حدد cisco-av-pairالسمة من القائمة المنسدلة على الجانب الأيسر، وأضف السمة التي تم تعيينها إلى FlexVPN Talkحسب المجموعة.

تتضمن السمات التي سيتم تعيينها لهذا المثال:

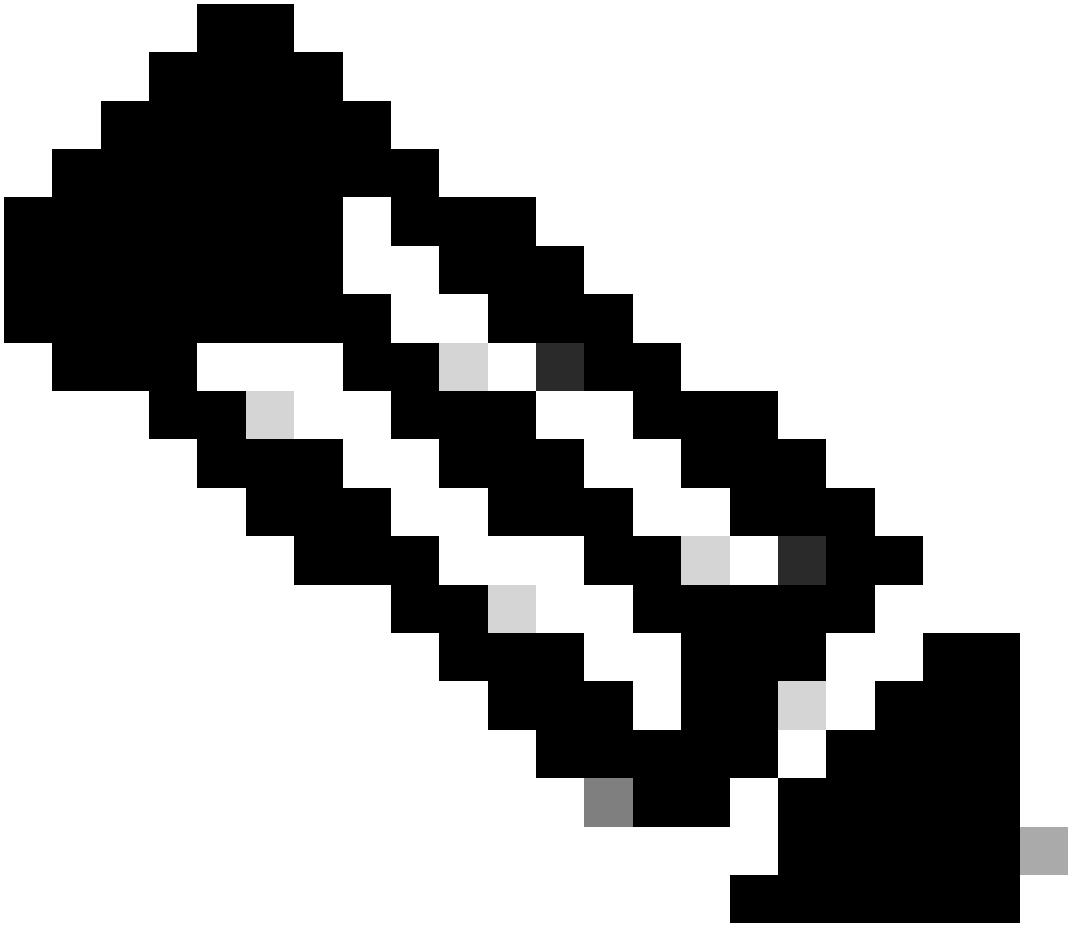
- تعيين واجهة الاسترجاع كمصدر.
- تحديد المجموعة التي تحصل منها الفروع على عنوان IP.

كما يلزم توفر route accept any السمات route set interface لأنه بدون هذه السمات لا يتم الإعلان عن الموجهات بشكل صحيح إلى الخوادم الفرعية.

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip unnumbered loopback100
cisco-av-pair = ipsec:addr-pool=RED_POOL
cisco-av-pair = ipsec:route-accept=any
cisco-av-pair = ipsec:route-set=interface
```



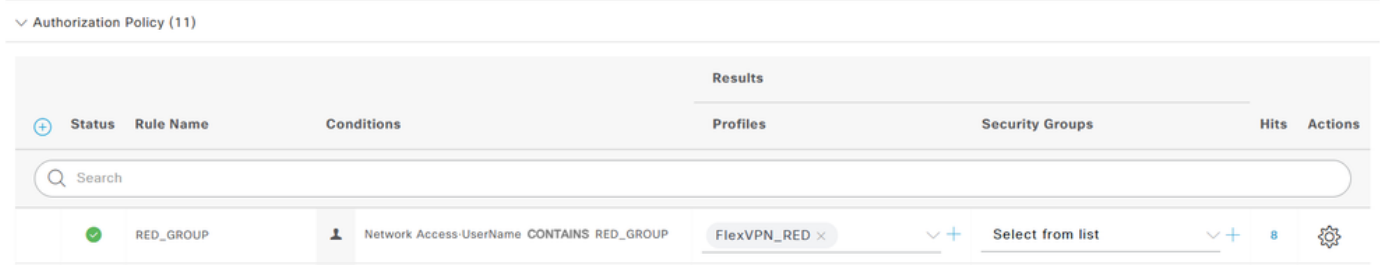
إعدادات الخصائص المتقدمة



ملاحظة: بالنسبة لمواصفات السمات (الاسم وبناء الجملة والوصف والمثال وما إلى ذلك)، يرجى مراجعة دليل تكوين سمات FlexVPN RADIUS:

دليل تكوين FlexVPN و Internet Key Exchange الإصدار 2، Cisco IOS XE Gibraltar، الإصدار 16.12.x

ج. قم بتعيين **authorization profile** في عمود التوصيفات.



قاعدة التخويل

أولا - انقر **Save**.

التحقق من الصحة

- أستخدم الأمر **show ip interface brief** لمراجعة النفق والقالب الظاهري وحالة الوصول الظاهري.

على الصرة، يتلقى القالب الظاهري حالة up/down وهي عادية، وينشئ الوصول الظاهري لكل Talk الذي أنشأ اتصالا بالموجه ويبدي حالة up/up.

<#root>

```
FlexVPN_HUB#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.10   YES  NVRAM    up              up
GigabitEthernet2           192.168.0.10    YES  manual   up              up
Loopback100                10.100.100.1    YES  manual   up              up
Loopback200                10.200.200.1    YES  manual   up              up
Loopback1010               10.10.1.10      YES  manual   up              up
Loopback1020               10.10.2.1       YES  manual   up              up

Virtual-Access1            10.100.100.1    YES  unset    up              up


Virtual-Template2          unassigned      YES  unset    up              dow
```

على ال Talk، إستلمت قارن النفق عنوان من التجمع يعين إلى المجموعة ويبدي up/up وضع.

<#root>

```
FlexVPN_RED_SPOKE#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.20    YES  NVRAM    up              up
Loopback2                  10.20.1.10      YES  manual   up              up

Tunnel0                    172.16.10.107   YES  manual   up              up
```

- استخدم الأمر **show interfaces virtual-access**.

configuration

```
FlexVPN_HUB#show interfaces virtual-access 1 configuration
Virtual-Access1 is in use, but purpose is unknown
Derived configuration : 232 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback100
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPSEC_FlexPROFILE
```

```
 no tunnel protection ipsec initiate
end
```

- أستخدم الأمر **show crypto session** لتأكيد إنشاء الاتصال الآمن بين الموجهات.

```
FlexVPN_HUB#show crypto session
Crypto session current status
Interface: Virtual-Access1
Profile: Flex_PROFILE
Session status: UP-ACTIVE
Peer: 192.168.10.20 port 500
  Session ID: 306
  IKEv2 SA: local 192.168.10.10/500 remote 192.168.10.20/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

- أستخدم الأمرshow ip eigrp neighborsلتأكيد إنشاء تجاور EIGRP مع الموقع الآخر.

```
FlexVPN_HUB#show ip eigrp neighbors
EIGRP-IPv4 VR(Flexvpn) Address-Family Neighbors for AS(10)
H   Address                 Interface              Hold Uptime     SRTT   RTO   Q   Seq
                                                   (sec)           (ms)       Cnt  Num
0   172.16.10.107           Vi1                      10 00:14:00      8  1494   0   31
```

- أستخدم الأمرshow ip routeللتحقق من أن المسارات قد دفعت إلى الخوادم.
  - تم التعرف على المسار ل 10.20.1.10، ووواجهة الاسترجاع على المكبر عبر EIGRP من قبل الموزع ويمكن الوصول إليه من خلال الوصول الظاهري

<#root>

```
FlexVPN_HUB#show ip route
<<<<< Output Ommitted >>>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
C        10.10.1.10 is directly connected, Loopback1010
C        10.10.2.10 is directly connected, Loopback1020
D        10.20.1.10 [90/79360000] via 172.16.10.107, 00:24:42, Virtual-Access1
C        10.100.100.1 is directly connected, Loopback100
C        10.200.200.1 is directly connected, Loopback200
      172.16.0.0/32 is subnetted, 1 subnets
S        172.16.10.107 is directly connected, Virtual-Access1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet2
```

```
L        192.168.0.10/32 is directly connected, GigabitEthernet2
C        192.168.10.0/24 is directly connected, GigabitEthernet1
L        192.168.10.10/32 is directly connected, GigabitEthernet1
```

- تم التعرف على المسارات 10.10.1.10 و 10.10.2.10 من خلال EIGRP ويمكن الوصول إليها عبر RED_GROUP (10.100.100.1)، ويمكن الوصول إليها من خلال مصدر IP الخاص بـ Tunnel0.

<#root>

```
FlexVPN_RED_SPOKE#sh ip route
<<<<< Output Ommitted >>>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
D        10.10.1.10 [90/26880032] via 10.100.100.1, 00:00:00


D        10.10.2.10 [90/26880032] via 10.100.100.1, 00:00:00


C        10.20.1.10 is directly connected, Loopback2
S        10.100.100.1 is directly connected, Tunnel0


D        10.200.200.1 [90/26880032] via 10.100.100.1, 00:00:00


      172.16.0.0/32 is subnetted, 1 subnets
C        172.16.10.107 is directly connected, Tunnel0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1
L        192.168.10.20/32 is directly connected, GigabitEthernet1
```

استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء هذه النوع من النشر وإصلاحها. أستخدم هذه الأوامر لتصحيح أخطاء عملية تفاوض النفق:

debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states

يمكن أن يساعد تصحيح أخطاء AAA و RADIUS في أستكشاف أخطاء اعتماد الفورع وإصلاحها.

debug aaa authentication
debug aaa authorization
debug aaa protocol radius
debug radius authentication

Working Scenario

تعرض هذه السجلات عملية التخويل وإحالة المعلمات..

```
     <#root>


RADIUS(OOOOO1A7): Received from id 1645/106
AAA/BIND(OOOOO1A8): Bind i/f
AAA/AUTHOR (0x1A8): Pick method list 'FLEX'
RADIUS/ENCODE(OOOOO1A8):Orig. component type = VPN IPSEC



RADIUS(000001A8): Config NAS IP: 192.168.0.10




vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(OOOOO1A8): Config NAS IPv6: ::
RADIUS/ENCODE(OOOOO1A8): acct_session_id: 4414
RADIUS(OOOOO1A8): sending
RADIUS(OOOOO1A8): Send Access-Request to 192.168.0.5:1645 id 1645/107, len 138
RADIUS:  authenticator 7A B5 97 50 F2 6E F0 09 - 3D B0 54 B4 1A DB BA BA



RADIUS:  User-Name           [1]   11  "RED_GROUP"
```

```
RADIUS:  User-Password       [2]   18  *

RADIUS:  Calling-Station-Id  [31]  14  "192.168.10.20"

RADIUS:  Vendor, Cisco       [26]  63

RADIUS:   Cisco AVpair       [1]   57  "audit-session-id=L2L496130A2ZP2L496130A21ZI1F401F4ZM134"

RADIUS:  Service-Type        [6]   6   Outbound                 [5]

RADIUS:  NAS-IP-Address      [4]   6   192.168.0.10

RADIUS(000001A8): Sending a IPv4 Radius Packet
```

```
RADIUS(000001A8): Started 5 sec timeout



RADIUS: Received from id 1645/107 192.168.0.5:1645, Access-Accept, len 248



RADIUS:  authenticator BE F4 FC FF 7C 41 97 A7 - 3F 02 A7 A3 A1 96 91 38
RADIUS:  User-Name           [1]   11  "RED_GROUP"
RADIUS:  Class               [25]  69
RADIUS:   43 41 43 53 3A 4C 32 4C 34 39 36 31 33 30 41 32  [CACS:L2L496130A2]
RADIUS:   5A 50 32 4C 34 39 36 31 33 30 41 32 31 5A 49 31  [ZP2L496130A21ZI1]
RADIUS:   46 34 30 31 46 34 5A 4D 31 33 34 3A 49 53 45 42  [F401F4ZM134:ISEB]
RADIUS:   75 72 67 6F 73 2F 35 33 34 36 34 30 33 32 39 2F  [urgos/534640329/]
RADIUS:   32 39 31               [ 291]



RADIUS:  Vendor, Cisco       [26]  53









RADIUS:   Cisco AVpair       [1]   47  "ip:interface-config=ip unnumbered loopback100"









RADIUS:  Vendor, Cisco       [26]  32









RADIUS:   Cisco AVpair       [1]   26  "ipsec:addr-pool=RED_POOL"
```

```
RADIUS:  Vendor, Cisco       [26]  33

RADIUS:   Cisco AVpair       [1]   27  "ipsec:route-set=interface"

RADIUS:  Vendor, Cisco       [26]  30

RADIUS:   Cisco AVpair       [1]   24  "ipsec:route-accept=any"

RADIUS(000001A8): Received from id 1645/107
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001A9): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001AA): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

AAA/BIND(000001AB): Bind i/f
RADIUS/ENCODE(000001AB):Orig. component type = VPN IPSEC
RADIUS(000001AB): Config NAS IP: 192.168.0.10
vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(000001AB): Config NAS IPv6: ::
RADIUS(000001AB): Sending a IPv4 Radius Packet
RADIUS(000001AB): Started 5 sec timeout
```

```
RADIUS: Received from id 1646/23 192.168.0.5:1646, Accounting-response, len 20



%DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 172.16.10.109 (Virtual-Access1) is up: new adjacency
```

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).