ISE統合によるFlexVPNの設定

内容

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)を使用してFlexVPNを設定し、スポークに設定を動的に割り当てる方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine(ISE)の設定
- RADIUS プロトコル
- Flexバーチャルプライベートネットワーク(FlexVPN)

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco CSR1000V(VXE)：バージョン17.03.04a
- Cisco Identity Services Engine(ISE) - 3.1

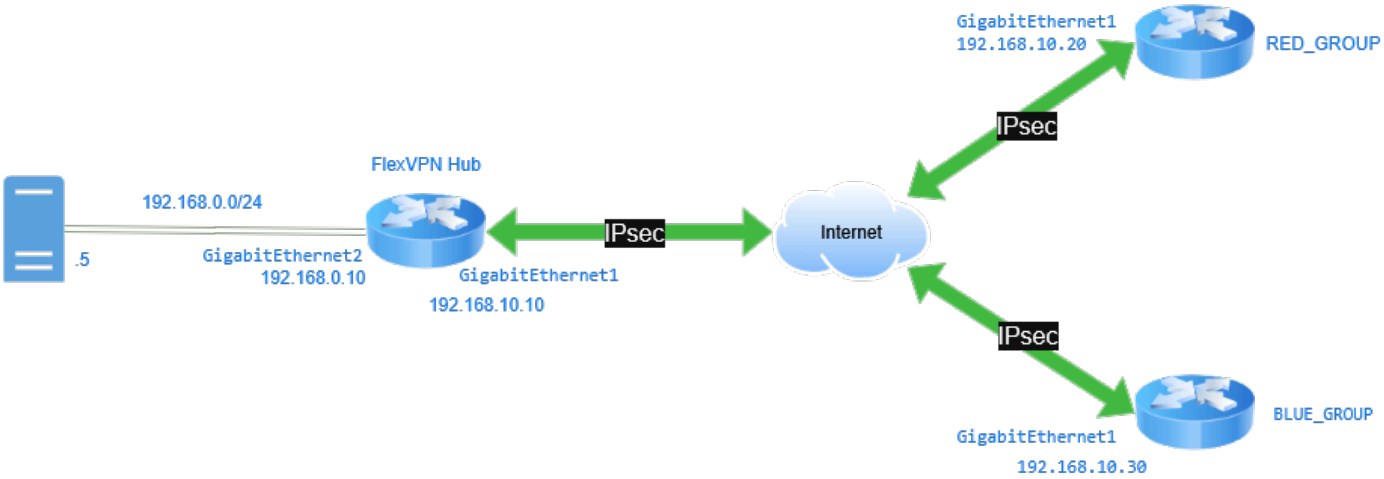
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

FlexVPNは、スポークとの接続を確立し、通信とトラフィック管理を可能にする特定の設定を割り当てることができます。この図では、スポークがハブに接続する際に、スポークが属するグループまたはブランチに応じてトンネルソースおよびDHCPプールのパラメータが割り当てられるように、FlexVPNがISEと統合する方法を示しています。スポークの認証に証明書を使用し、次にRADIUSを許可およびアカウンティングサーバとして使用するISEを使用します。



FlexVPNとISEの統合

ステップ1：ハブの設定

a.ルータ証明書を保存するようにtrustpointを設定します。スポークの認証には証明書が使用されます。

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

b. **certificate map**を設定します。certificate mapの目的は、ルータに複数の証明書がインストールされている場合に、指定された情報に基づいて証明書を識別および照合することです。

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

c.デバイスで許可とアカウンティング用にRADIUS serverを設定します。

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

d. RADIUSトラフィックのIPアドレス、通信ポート、共有キー、および送信元インターフェイスを使用して「**RADIUS server group**」を定義します。

```
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
```

e. **loopback interfaces**を設定します。loopback interfacesはトンネルのソース接続として使用され、接続されているグループに応じて動的に割り当てられます。

```
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
```

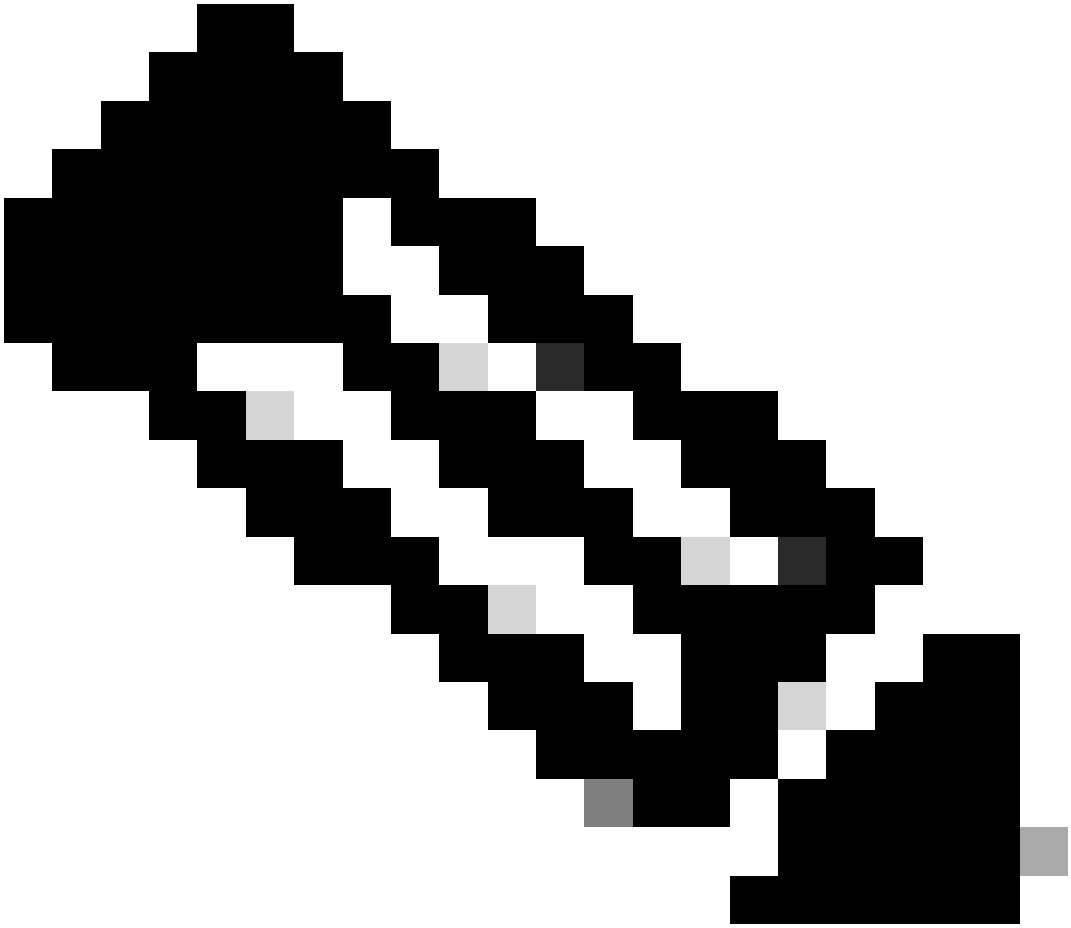
f.グループごとに「**IP local pool**」を定義します。

```
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
```

g. EIGRPを設定して、各グループのネットワークをアドバタイズします。

```
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
```



注:FlexVPNは、OSPF、EIGRP、BGP over VPNトンネルなどのダイナミックルーティングプロトコルをサポートしています。このガイドでは、EIGRPが使用されています。

---

h. **crypto ikev2 name mangler**を設定します。IKEv2 name manglerは、IKEv2認可のユーザ名を取得するために使用されます。この場合、スポーク上の証明書からの組織ユニット(OU)情報を認証用のユーザ名として使用するように設定されています。

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

i. **IKEv2 profile**を設定します。certificate map、 AAA server group、 および name mangler。IKEv2プロファイル内で参照されます。

この特定のシナリオでは、ローカルおよびリモート認証が**RSA-SIG**として設定されています。

（次の設定で指定されているように）organization-unitの値とパスワードに一致するユーザ名を持つCisco1234ローカルユーザアカウントを「RADIUS server」で作成する必要があります。

```
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
```

j. IPsec profileを設定し、 IKEv2 profileを参照します。

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

k. virtual-templateを作成します。このコマンドは、「virtual-access interface」を作成し、作成した「IPsec profile」をリンクするために使用します。

IPアドレスなしで「**virtual-template**」を設定します。これは、RADIUS serverによって割り当てられるためです。

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

2つのloopbacksを設定して内部ネットワークをシミュレートする。

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

```
ip address 10.10.2.10 255.255.255.255
```

ステップ2：スポークの設定

a.スポークルータの証明書を保存するようにtrustpointを設定します。

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

b. certificate mapを設定します。certificate mapの目的は、ルータに複数の証明書がインストールされている場合に、指定された情報に基づいて証明書を識別および照合することです。

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

c. AAAローカル認可ネットワークを設定します。

aaa authorization networkコマンドは、ネットワークサービスに関連するアクセス要求を認可するために使用されます。認証後に、ユーザが要求されたサービスにアクセスする権限を持っているかどうかを確認する作業も含まれます。

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

d. IKEv2 profileを設定します。certificate mapおよびAAA authorization localは、IKEv2 profileで参照されます。

ローカルおよびリモート認証は、次のように設定されます **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
```

e. IPsec profileを設定し、 IKEv2 profile.

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

f. tunnel interfaceを設定します。tunnel interfaceは、許可結果に基づいてハブからトンネルIPアドレスを受信するように設定されています。

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

g.スポークのローカルネットワークおよびtunnel interfaceをアドバタイズしながら、EIGRPを設定します。

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

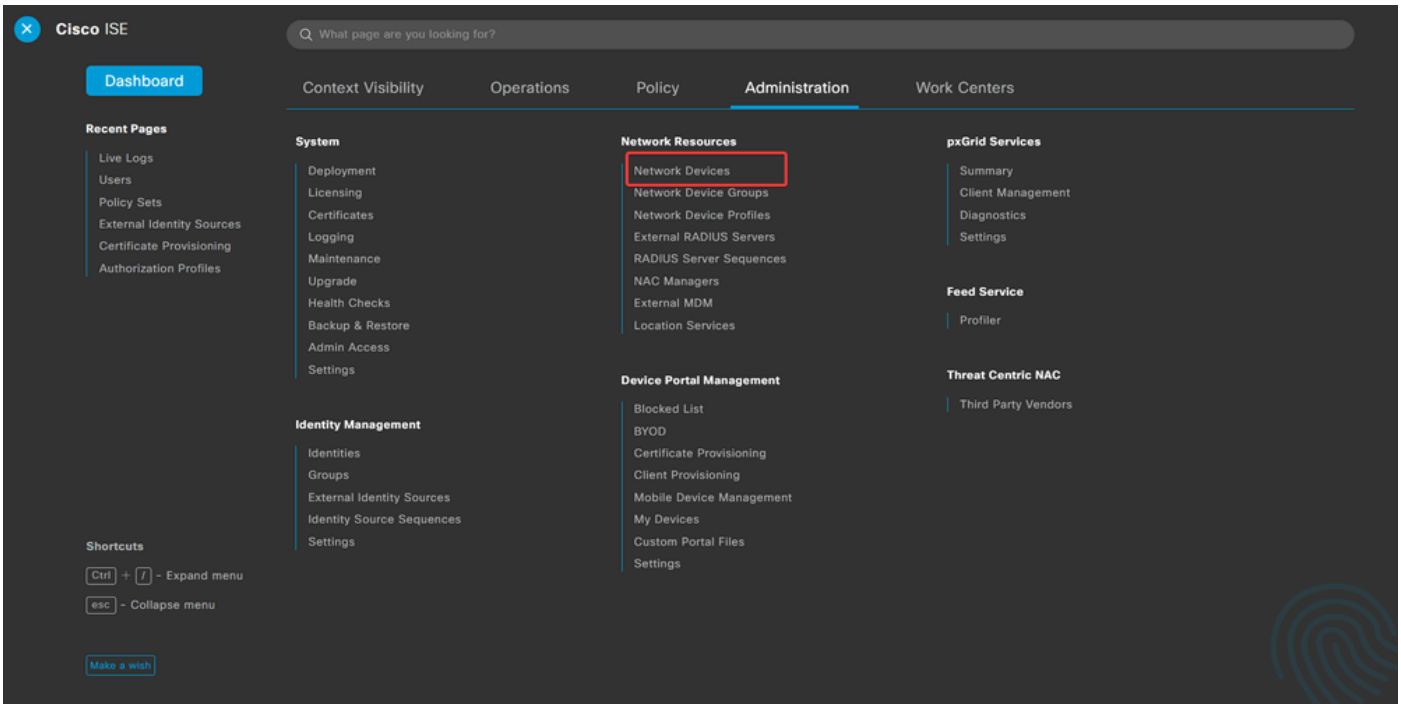
内部ネットワークをシミュレートするようにloopbackを設定します。

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

ステップ3:ISEの設定

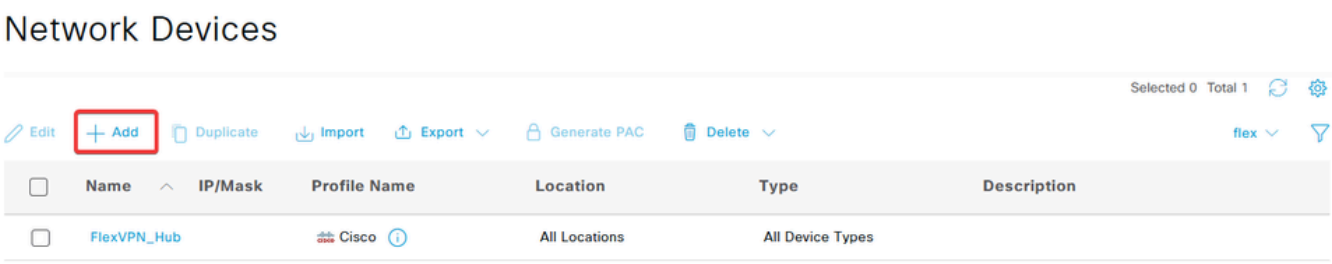
ステップ3.1：ユーザ、グループの作成、およびネットワークデバイスの追加

a. ISEサーバにログインし、**Administration** > **Network Resources** > **Network Devices**に移動します。



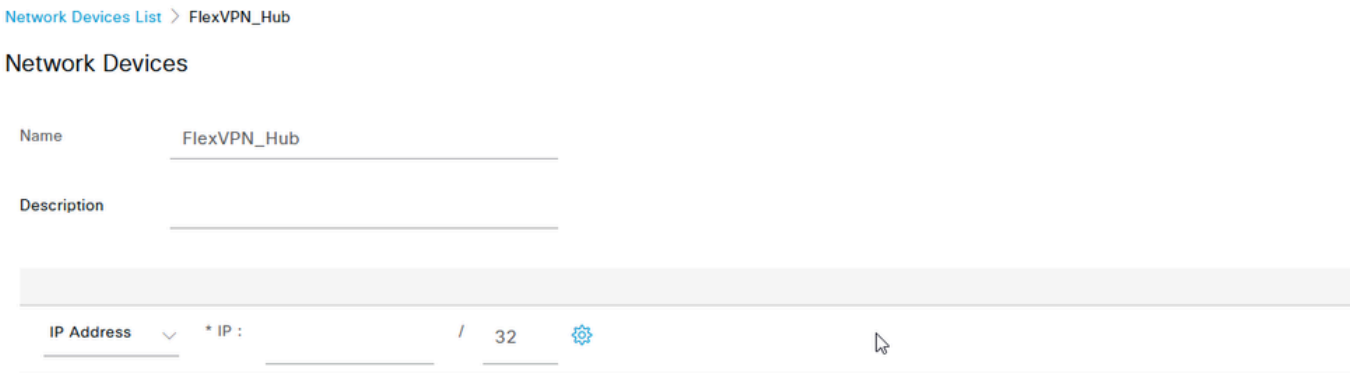
管理 – ネットワークリソース – ネットワークデバイス

b. **Add**をクリックして、FlexVPNハブをAAAクライアントとして設定します。

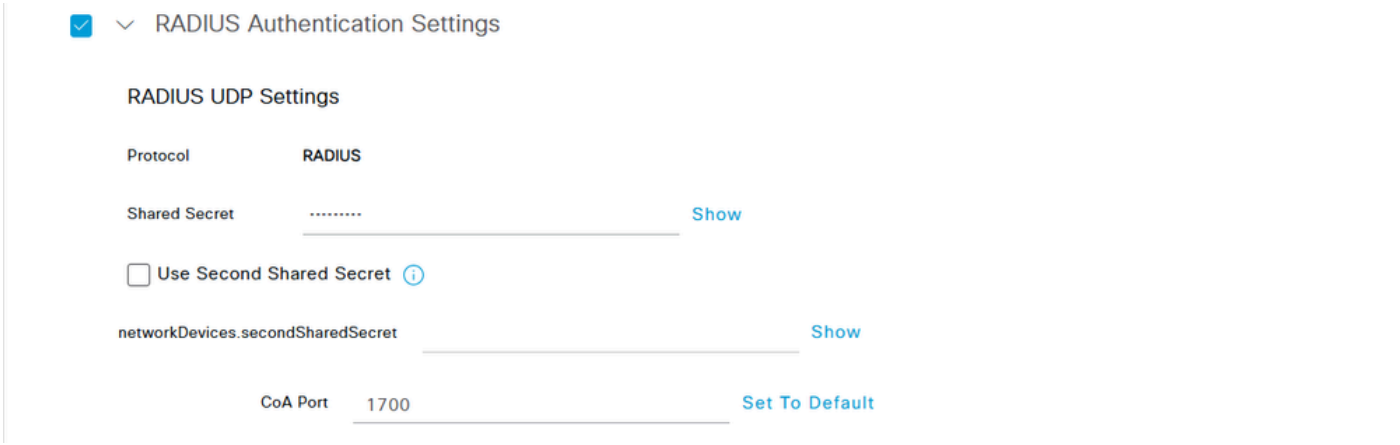


AAAクライアントとしてのFlexVPNルータの追加

c. ネットワークデバイスの名前とIPアドレスフィールドを入力してから、**RADIUS Authentication Settings**ボックスにチェックマークを入れて、**Shared Secret.**を追加します。共有秘密パスワードは、FlexVPNハブでRADIUSサーバグループを作成したときに使用したものと同じでなければなりません。をクリックします。Save

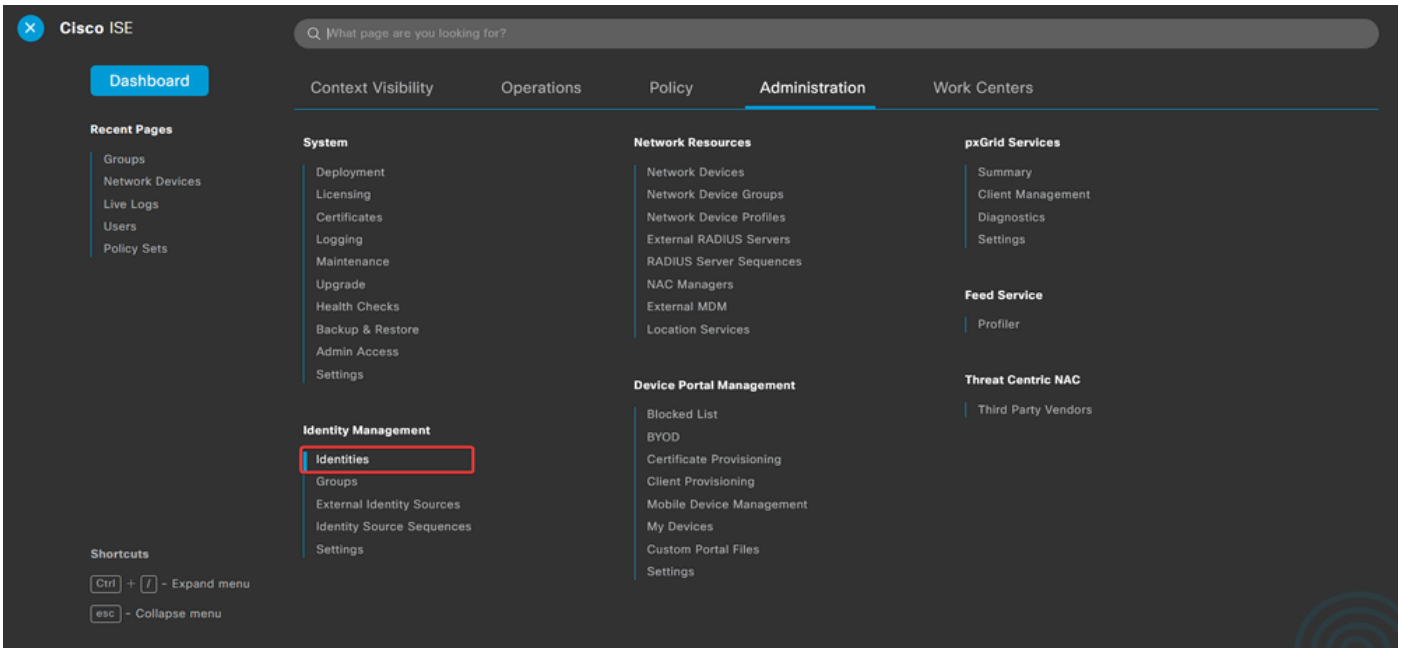


ネットワークデバイスのIPアドレス



ネットワークデバイスの共有キー

d. **Administration** > **Identity Management** > **Identities**に移動します。

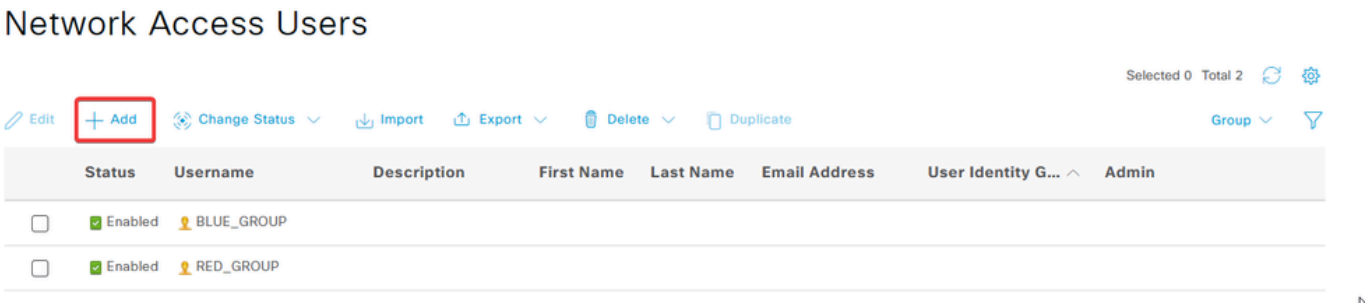


管理 – 管理の識別 – 識別

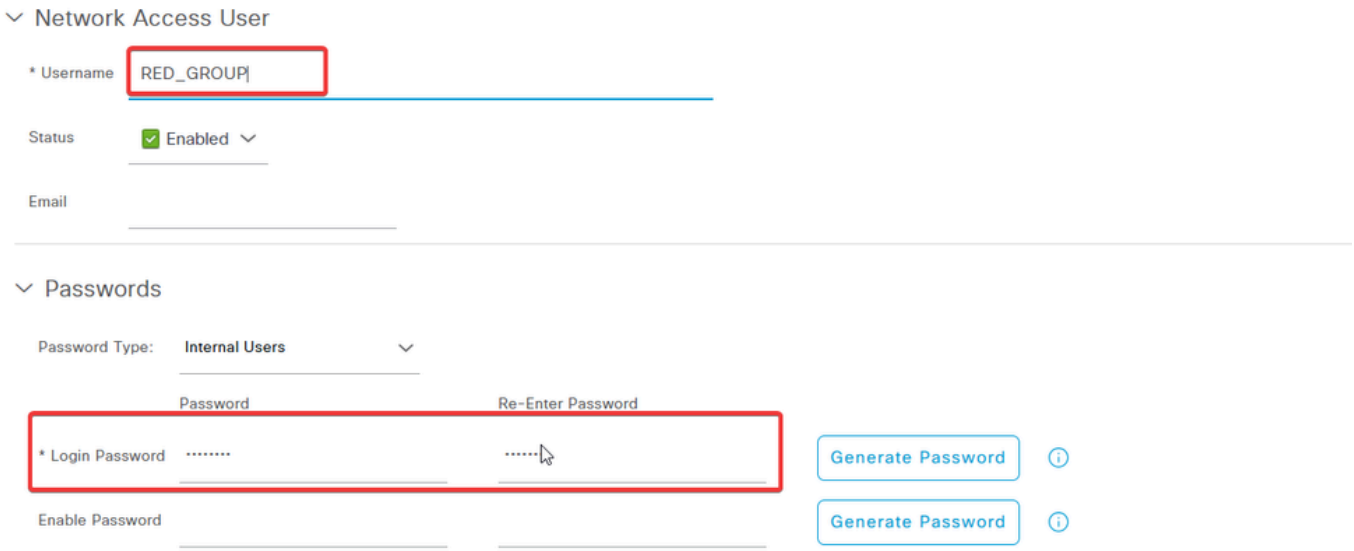
e.サーバのローカルデータベースに新しいユーザを作成するには、Addをクリックします。

Usernameおよび**Login Password**を入力します。ユーザ名は、証明書の証明書の組織単位(OU)の値と同じ名前です。ログインパスワードは、IKev2プロファイルで指定したパスワードと同じである必要があります。

をクリックします。**Save**



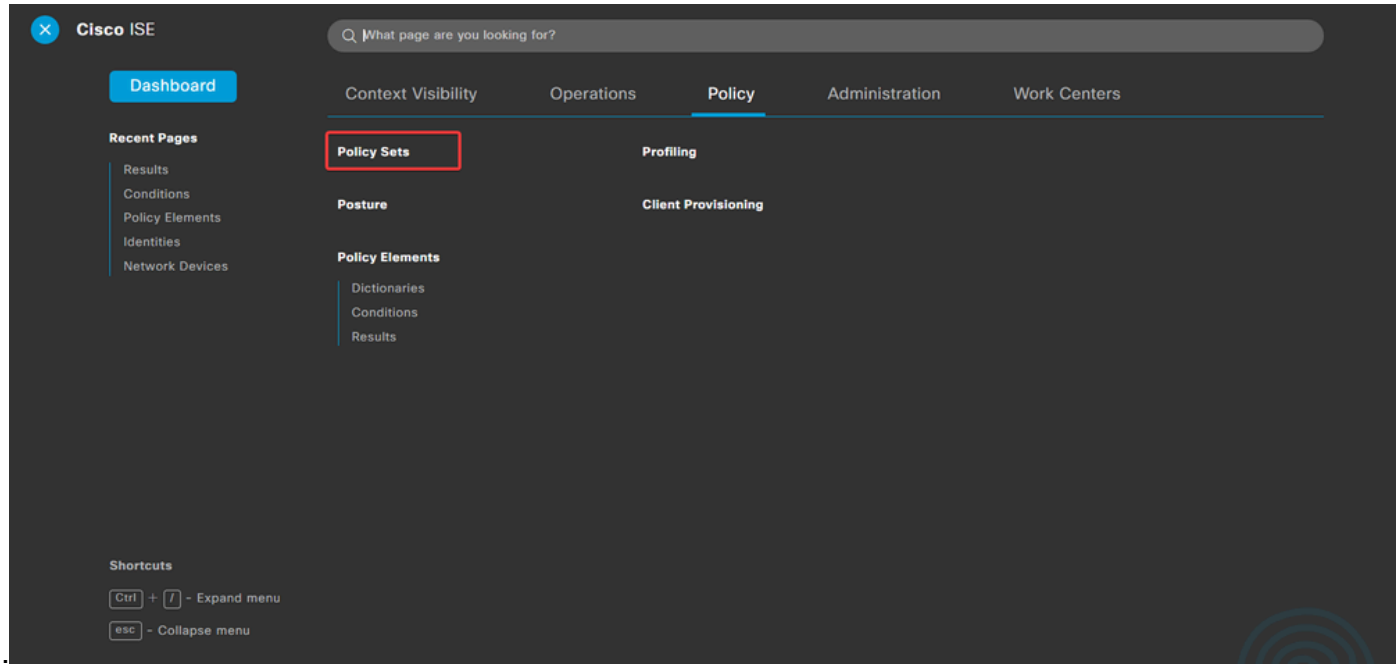
管理 – 管理の識別 – 識別



グループ作成組織単位値と同じ

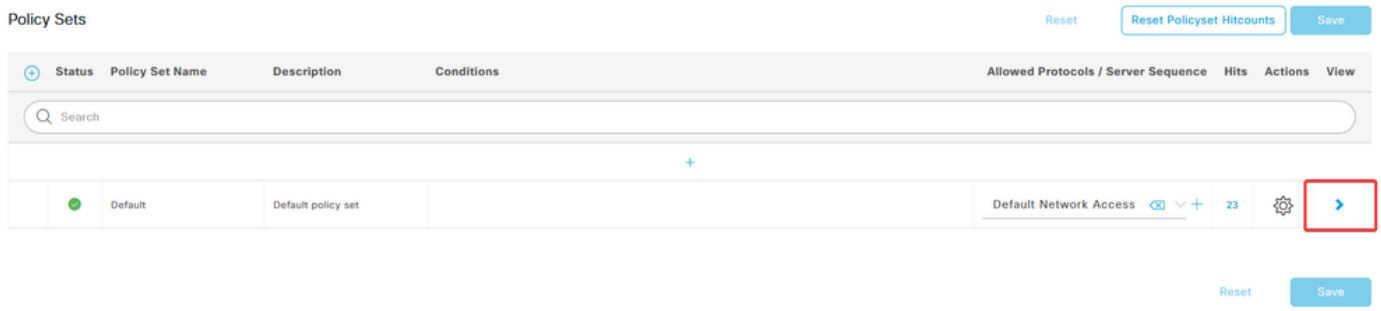
ステップ3.2：ポリシーセットの設定

a. **Policy > Policy Sets**に移動します。



ポリシーポリシーセット

b.画面右側の矢印をクリックして、デフォルトの認可ポリシーを選択します。

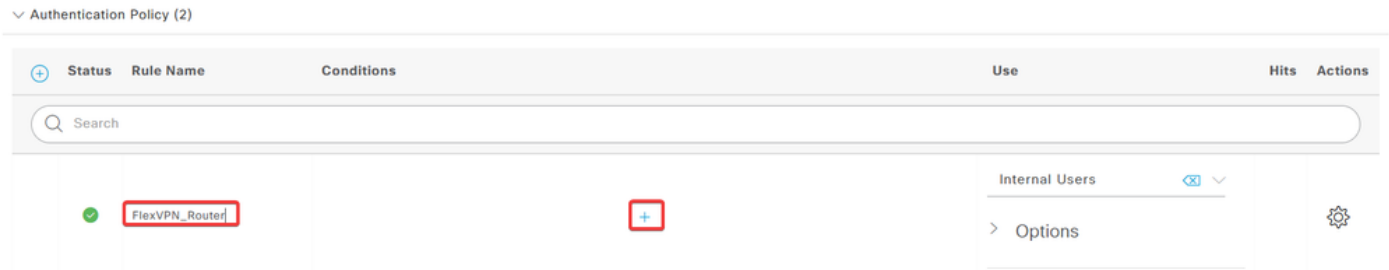


既定のポリシーの編集

c. Authentication Policyの横にあるドロップダウンメニューの矢印をクリックして展開します。次に、**add (+)**アイコンをクリックして新しいルールを追加します。

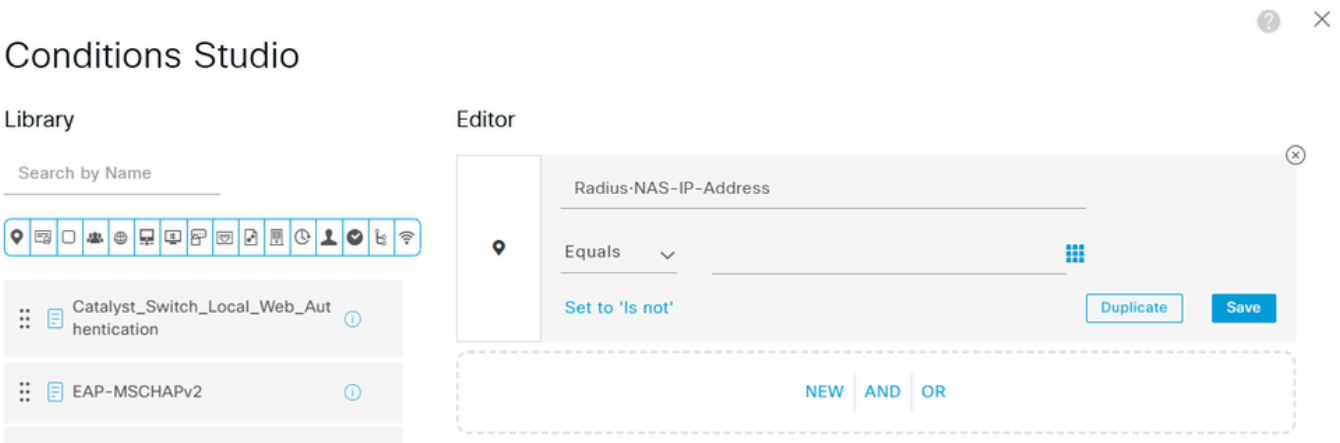
認証ポリシーの追加

d.ルールの名前を入力し、Conditions列でadd (+)アイコンを選択します。

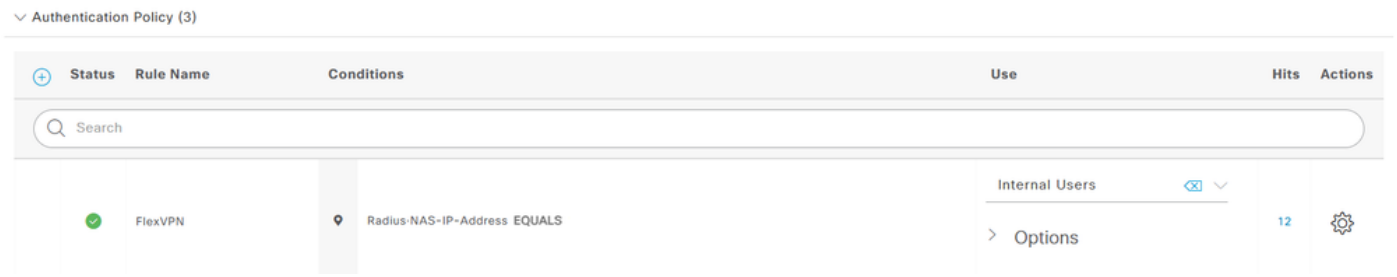


認証ポリシーの作成

e. Attribute Editorテキストボックスをクリックし、NAS-IP-Addressアイコンをクリックします。FlexVPNハブのIPアドレス(192.168.0.10)を入力します。



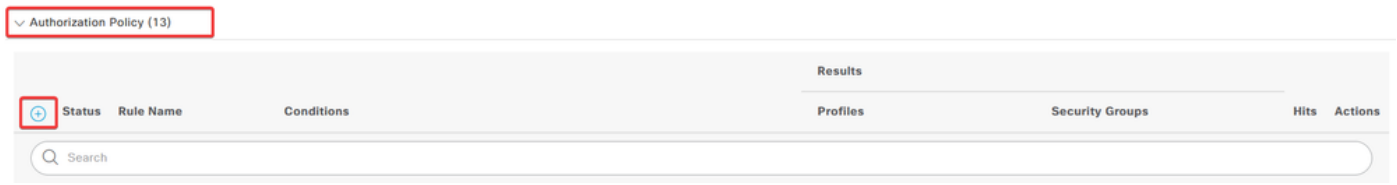
Authenticate FlexVPN Hub



認証ポリシー

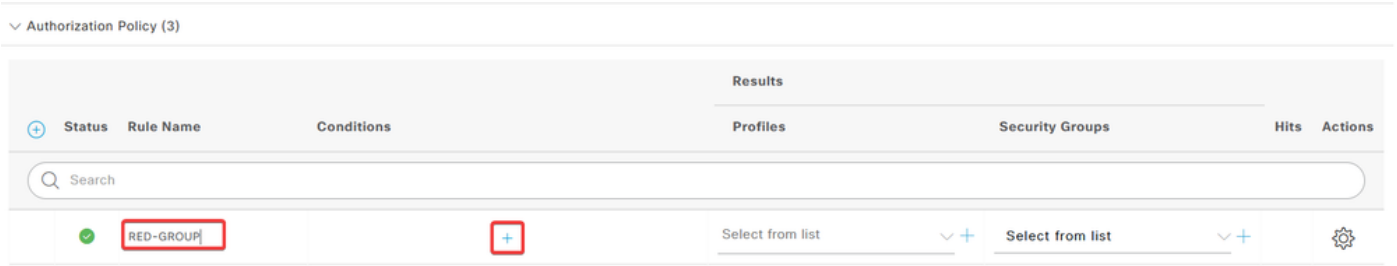
ステップ3.3：許可ポリシーの設定

a.の横にあるドロップダウンメニューの矢印をクリックAuthorization Policyして展開します。次に、**add (+)**アイコンをクリックして新しいルールを追加します。



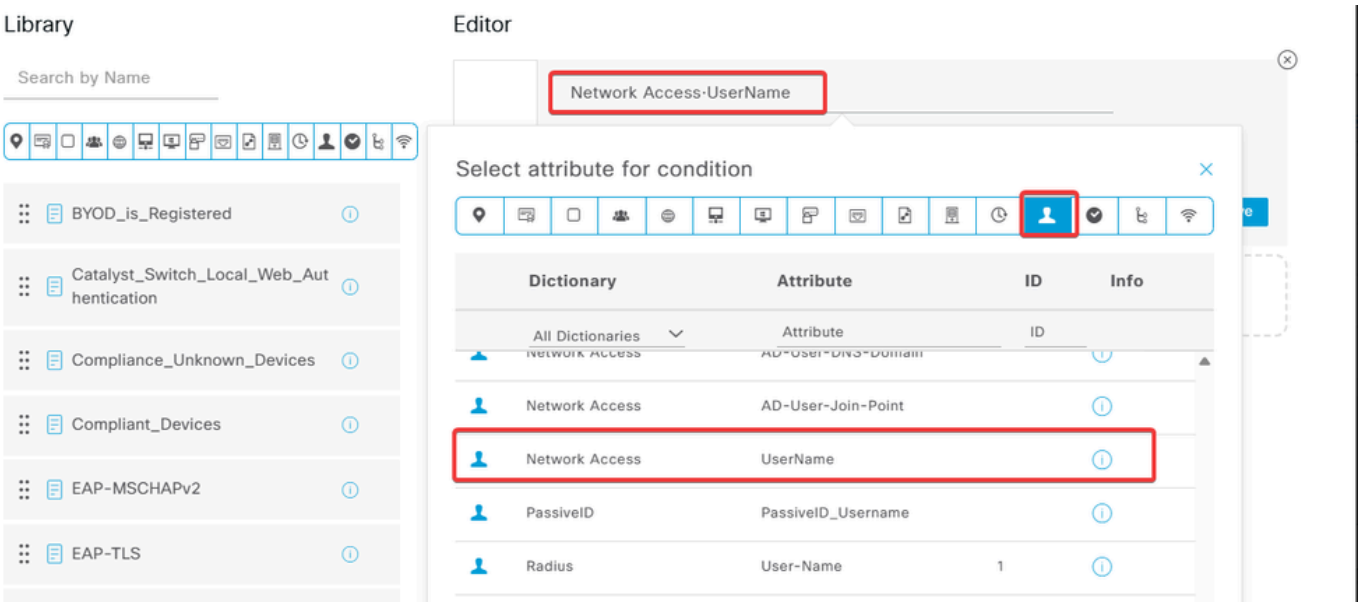
新しい許可ポリシーの作成

b.ルールの名前を入力し、Conditions列の下にある**add (+)**アイコンを選択します。



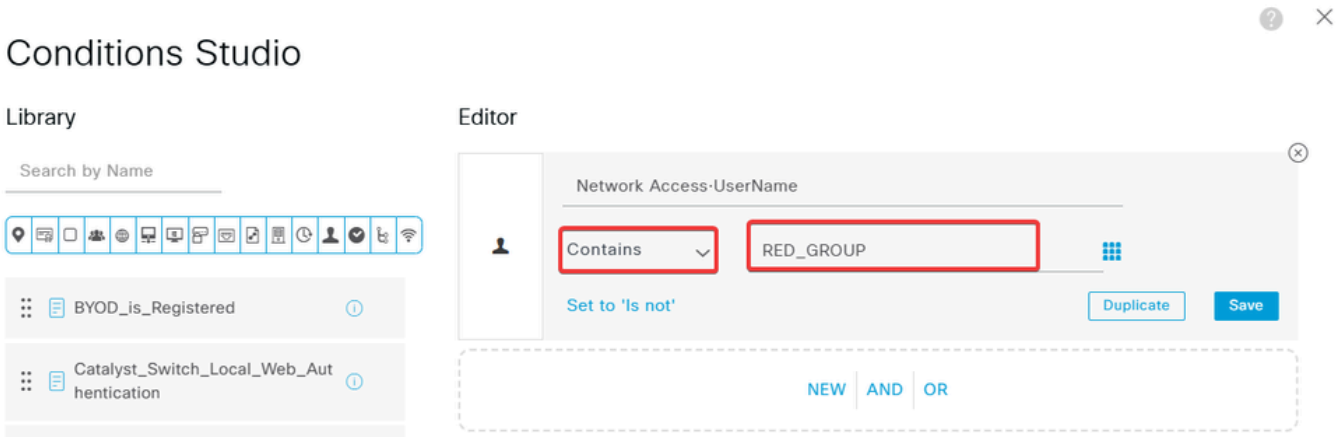
新しいルールの作成

c. Attribute Editorテキストボックスをクリックし、Subjectアイコンをクリックします。**Network Access - UserName**属性を選択します。



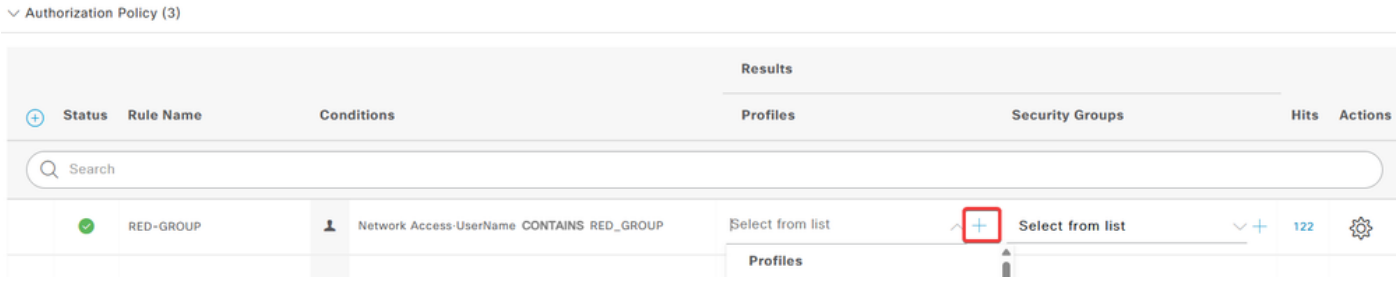
ネットワークアクセスの選択 – UserName

d.演算子としてContainsを選択し、証明書のOrganization-Unit値を追加します。



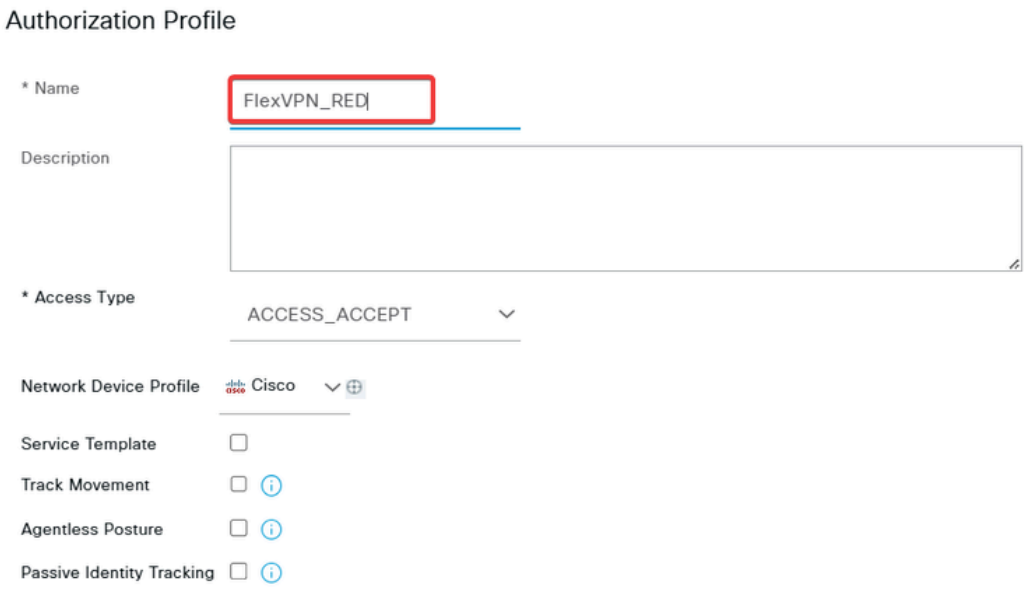
グループ名の追加

e. Profilesカラムでadd (+)アイコンをクリックし、**Create a New Authorization Profile**を選択します。



新しい認可プロファイルの追加

f.profileを入力します(profile **Name**)。



許可プロファイルに名前を付けます。

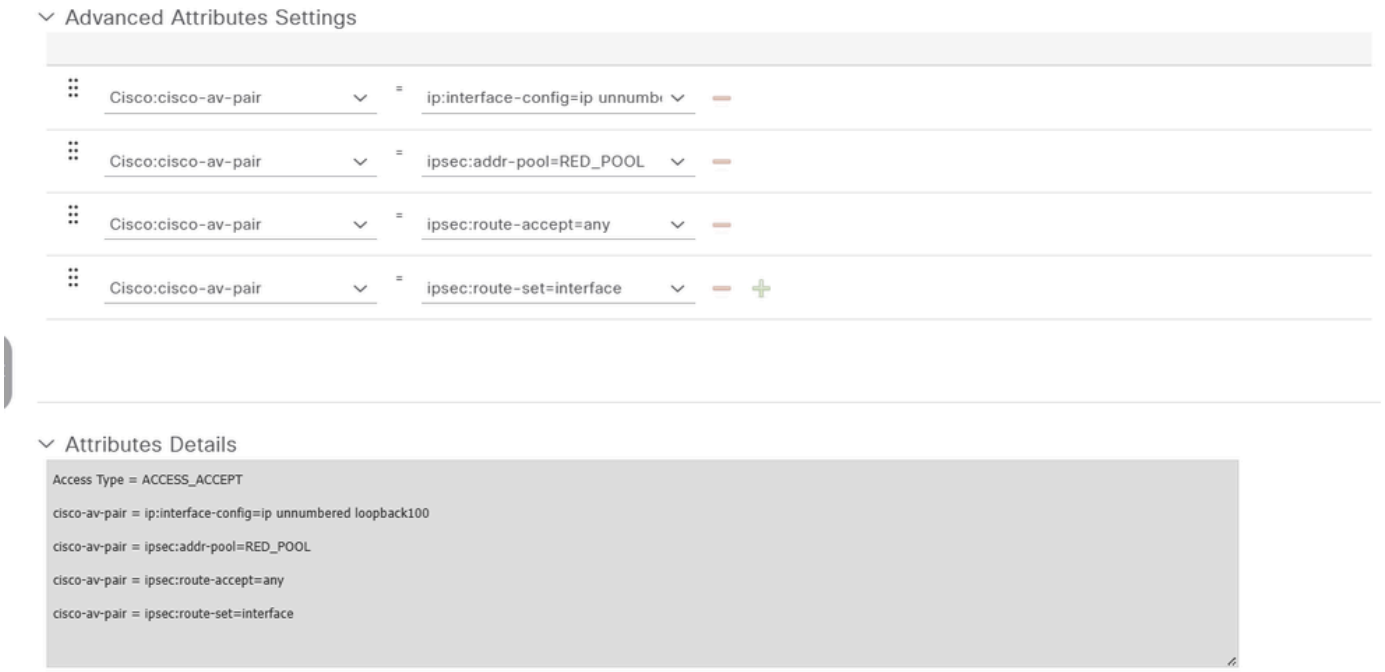
g. **Advanced Attributes Settings**に移動します。次に、左側のドロップダウンメニューからcisco-av-pair属性を選択し、グループに応じてFlexVPNスポークに割り当てられている属性を追加します。

この例で割り当てる属性は次のとおりです。

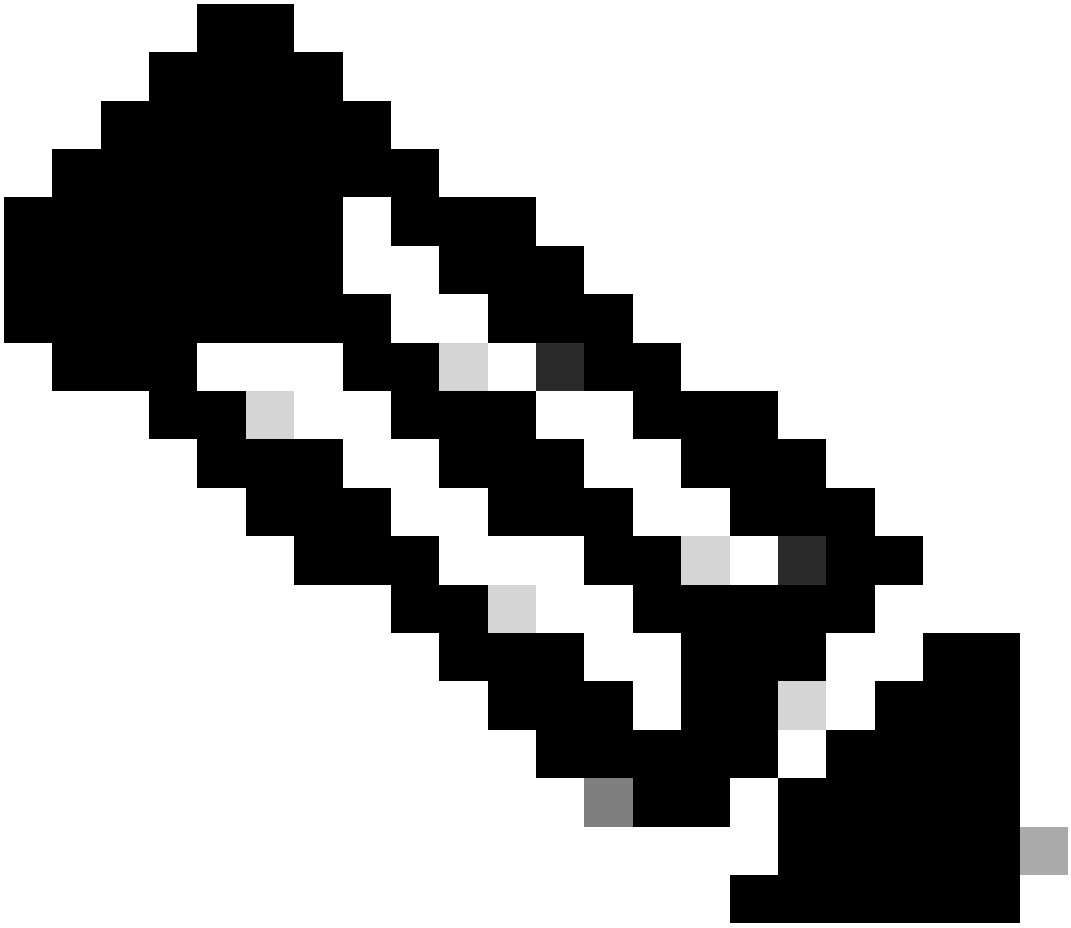
- 送信元としてループバックインターフェイスを割り当てます。
- スポークがIPアドレスを取得するプールを指定します。

route accept any属性とroute set interface属性がないとスポークにルートが正しくアドバタイズされないため、これらの属性は必要です。

```
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
```


Advanced Attributes Settings
Cisco:cisco-av-pair
ip:interface-config=ip unnumb
Cisco:cisco-av-pair
ipsec:addr-pool=RED_POOL
Cisco:cisco-av-pair
ipsec:route-accept=any
Cisco:cisco-av-pair
ipsec:route-set=interface
Attributes Details
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

高度な属性の設定

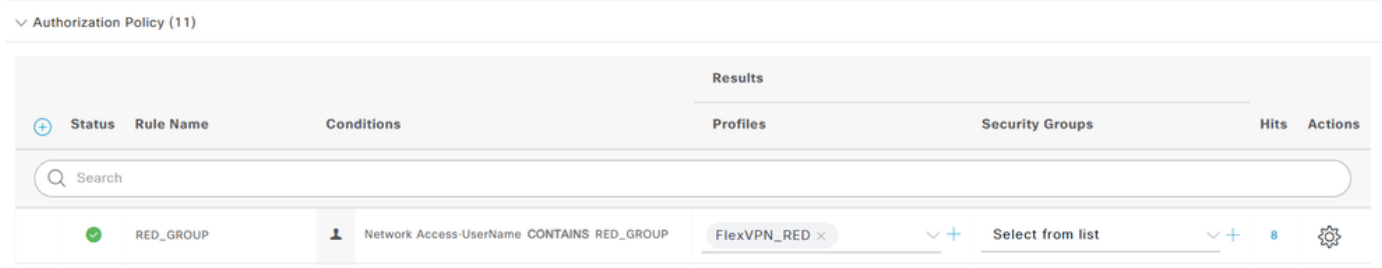


注：属性の指定（名前、構文、説明、例など）については、FlexVPN RADIUS属性設定ガイドを参照してください。

FlexVPNおよびインターネットキーエクスチェンジ(IKE)バージョン2コンフィギュレーションガイド、Cisco IOS XE Gibraltar 16.12.x

---

h. profilesカラムにauthorization profileを割り当てます。



許可ルール

i. Saveをクリックします。

確認

- **show ip interface brief**コマンドを使用して、トンネル、バーチャルテンプレート、およびバーチャルアクセスのステータスを確認します。

ハブでは、仮想テンプレートのup/downステータスは正常で、仮想アクセスは、ハブとの接続を確立し、up/upステータスを示すスポークごとに作成されます。

<#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
```

スポークでは、トンネルインターフェイスはグループに割り当てられたプールからIPアドレスを受信し、up/upステータスを示します。

<#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
```

- コマンドを使用します。**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
```

- **show crypto session** コマンドを使用して、ルータ間にセキュアな接続が確立されていることを確認します。

```
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
```

- show ip eigrp neighborsコマンドを使用して、EIGRPアジャセンシー関係が他のサイトと確立されていることを確認します。

```
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
```

- ルートがスポークにプッシュされたことを確認するには、コマンドshow ip routeを使用します。
  - スポーク上の10.20.1.10ループバックインターフェイスのルートは、EIGRPによってハブに学習されており、仮想アクセスを介してアクセスできます

<#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
```

- 10.10.1.10と10.10.2.10のルートはEIGRP経由で学習され、Tunnel0経由でアクセス可能なRED_GROUP(10.100.100.1)の送信元IP経由で到達可能です。

<#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
```

トラブルシュート

このセクションでは、このタイプの導入のトラブルシューティングに役立つ情報を提供します。トンネルネゴシエーションプロセスをデバッグするには、次のコマンドを使用します。

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

AAAおよびRADIUSのデバッグは、スポークの認可のトラブルシューティングに役立ちます。

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

Working Scenario

このログには、許可プロセスとパラメータの割り当てが表示されます。

```
     <#root>


RADIUS(OOOOO1A7): Received from id 1645/106
AAA/BIND(OOOOO1A8): Bind i/f
AAA/AUTHOR (Ox1A8): 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 5O F2 6E FO O9 - 3D BO 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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。