

配置FlexVPN與ISE整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[步驟 1:集線器配置](#)

[步驟 2:分支配置](#)

[步驟 3:ISE 組態](#)

[步驟 3.1:建立使用者、組並新增網路裝置](#)

[步驟 3.2:配置策略集](#)

[步驟 3.3:配置授權策略](#)

[驗證](#)

[疑難排解](#)

[工作場景](#)

簡介

本文檔介紹如何使用思科身份服務引擎(ISE)配置FlexVPN以動態地將配置分配給分支。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身份服務引擎(ISE)配置
- RADIUS通訊協定
- Flex虛擬私人網路(FlexVPN)

採用元件

本檔案是根據以下軟體和硬體版本所編制：

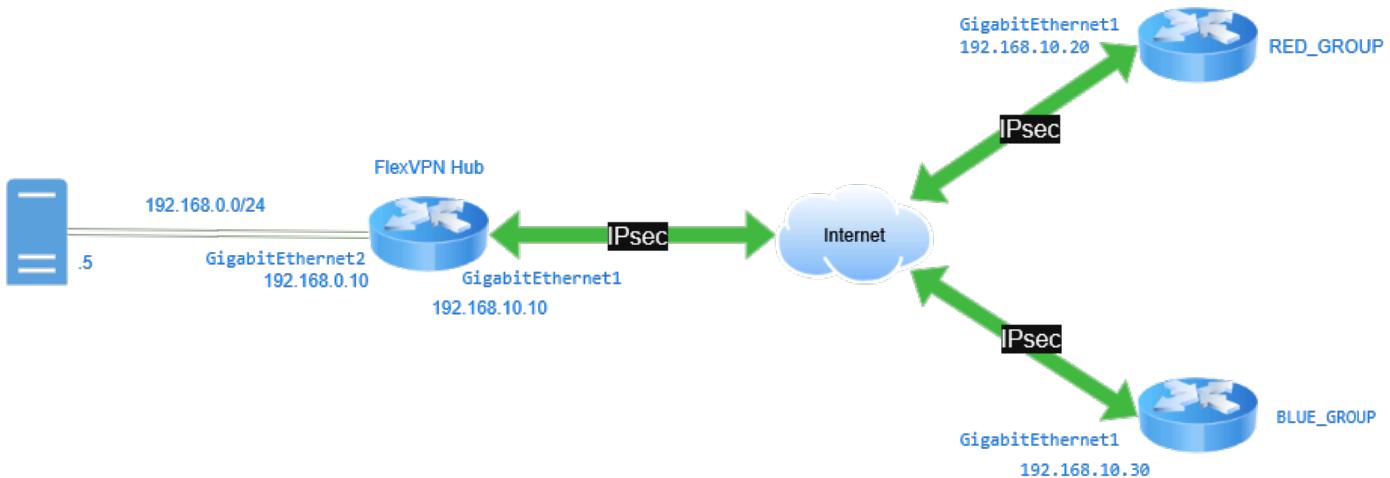
- Cisco CSR1000V(VXE) — 版本17.03.04a
- 思科身分識別服務引擎(ISE)- 3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

FlexVPN可與輻條建立連線，並分配啟用通訊和流量管理的特定配置。如圖所示，這展示了FlexVPN如何與ISE整合，以便當分支連線到HUB時，根據分支所屬的組或分支分配隧道源和DHCP池的引數。它使用證書對輻條進行身份驗證，然後使用Radius作為授權和記帳伺服器的ISE。



整合ISE的FlexVPN

步驟 1:集線器配置

a. 配置trustpoint，以儲存路由器證書。證書用於對分支進行身份驗證。

```
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. 配置certificate map。其目的是根據certificate map指定的資訊來識別和匹配證書，以便路由器安裝多個證書時使用。

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

c. 在裝置上配置用於授權和記帳的RADIUS server:

```
aaa new-model
!
```

```
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
```

d.為RADIUS server group流量定義其IP地址、通訊埠、共用金鑰和源介面。

```
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.配置loopback interfaces。將loopback interfaces用作隧道的源連線，並根據所連線的組進行動態分配。

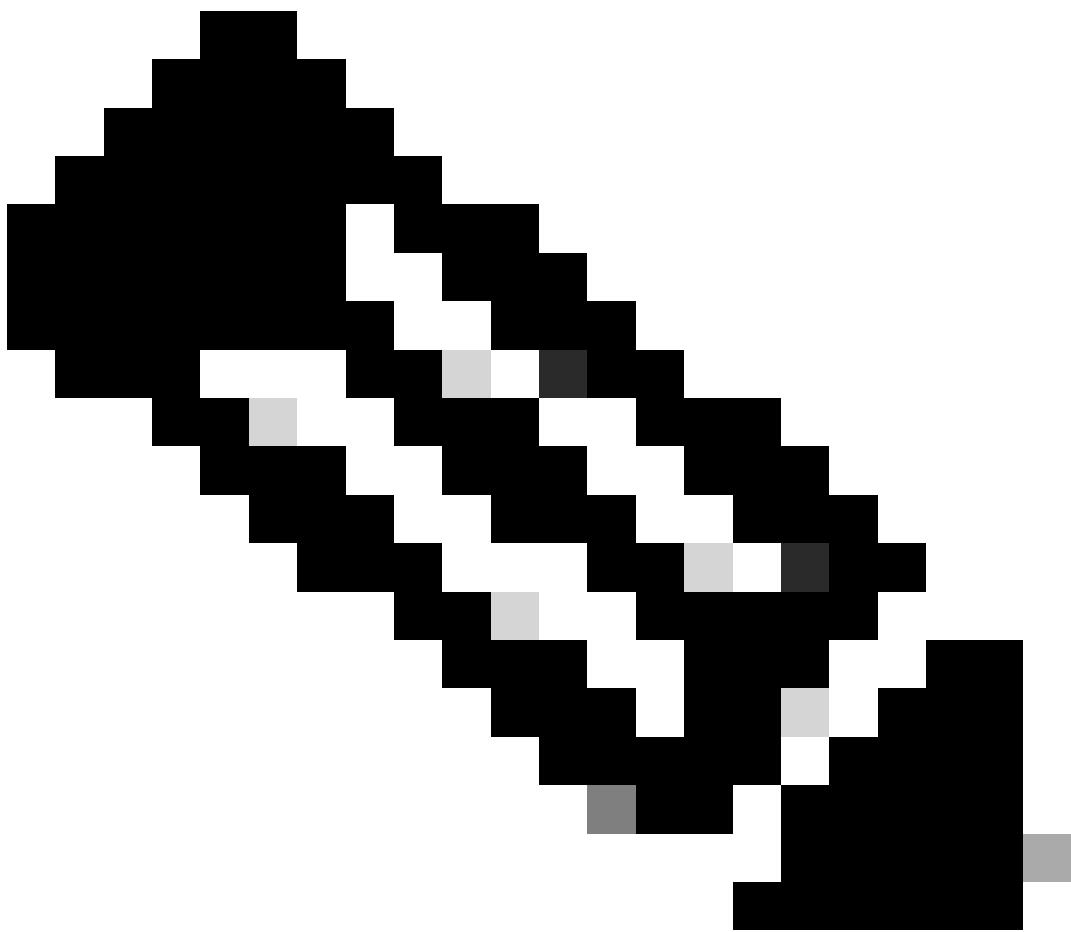
```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

f.為每個IP local pool組定義一個。

```
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.配置EIGRP並通告每個組的網路。

```
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
```



附註：FlexVPN支援動態路由協定，例如通過VPN隧道的OSPF、EIGRP和BGP。在本指南中，使用了EIGRP。

h.配置crypto ikev2 name mangler。用IKEv2 name mangler於獲取IKEv2授權的使用者名稱。在這種情況下，配置為使用輻條上的證書中的組織單元資訊作為授權使用者名稱。

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

i.配置IKEv2 profile。在certificate map IKEvAAA server group 2配置檔案中引用 name mangler、和。

在此特定場景中，本地和遠程身份驗證配置為。

必須使用與organization-unit RADIUS server值和密碼（如下面的配置中所指定）匹配的使用者名稱，在上建立本地使用者帳戶Cisco1234。

```
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. 配置IPsec profile，並引IKEv2 profile用。

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

k. 建立virtual-template。它用於建立並鏈virtual-access interface接所建立IPsec profile的。

設定無IPvirtual-template地址的，因為此地址由分RADIUS server配。

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

配置兩個loopbacks，以模擬內部網路。

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

步驟 2: 分支配置

a. 配置trustpoint，以儲存分支路由器的證書。

```
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. 配置certificate map。其目的是根據certificate map指定的資訊來識別和匹配證書，以便路由器安裝多個證書時使用。

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

c. 配置AAA本地授權網路。

aaa authorization network命令用於授權與網路服務相關的訪問請求。它包括驗證使用者在經過驗證之後是否具有訪問所請求的服務的許可權。

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

d. 配置IKEv2 profile。中certificate map引用和AAA本地授IKEv2 profile權。

本地和遠端身份驗證配置為 RSA-SIG.

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

e. 配置IPsec profile，並參考 IKEv2 profile.

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

f. 配置tunnel interface。配置tunnel interface為根據授權結果從集線器接收隧道IP地址。

```
interface Tunnel0
```

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

g. 配置EIGRP，通告分支和的本地網tunnel interface絡。

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

配置loopback，以模擬內部網路。

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

步驟 3:ISE 組態

步驟 3.1:建立使用者、組並新增網路裝置

a. 登入到ISE伺服器並導航到Administration > Network Resources > Network Devices。

The screenshot shows the Cisco ISE Administration interface. The top navigation bar has tabs: Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), and Work Centers. On the left, there's a sidebar with 'Recent Pages' (Live Logs, Users, Policy Sets, etc.) and 'Shortcuts' (Ctrl + F - Expand menu, Esc - Collapse menu). The main content area is divided into several sections: 'System' (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), 'Identity Management' (Identities, Groups, External Identity Sources, Identity Source Sequences, Settings), 'Network Resources' (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), 'Device Portal Management' (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Management, My Devices, Custom Portal Files, Settings), 'pxGrid Services' (Summary, Client Management, Diagnostics, Settings), 'Feed Service' (Profiler), and 'Threat Centric NAC' (Third Party Vendors). A red box highlights the 'Network Devices' link under the Network Resources section. A watermark of a fingerprint is visible in the bottom right corner.

管理 — 網路資源 — 網路裝置

b. 按一下Add將FlexVPN中心配置為AAA客戶端。

Network Devices

The screenshot shows a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. A red box highlights the '+ Add' button in the top left corner. The table has one row with the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
FlexVPN_Hub	Cisco	All Locations	All Device Types		

將FlexVPN路由器新增為AAA客戶端

c. 輸入網路裝置名稱和IP地址欄位，然後選中**RADIUS Authentication Settings****Shared Secret**。「共用金鑰密碼必須與FlexVPN中心上建立RADIUS伺服器組時使用的密碼相同」覈取方塊。按一下Save。

Network Devices List > FlexVPN_Hub

Network Devices

Name

Description

IP Address * IP : / 32

網路裝置IP地址

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Use Second Shared Secret

networkDevices.secondSharedSecret

CoA Port 1700

網路裝置共用金鑰

d. 導航到Administration > Identity Management > Identities。

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes tabs for Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), and Work Centers. A search bar at the top right says "What page are you looking for?". On the left, there's a sidebar with "Recent Pages" (Groups, Network Devices, Live Logs, Users, Policy Sets) and "Identity Management" (Groups, External Identity Sources, Identity Source Sequences, Settings). The main content area under Administration is divided into several sections: System (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), Network Resources (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), pxGrid Services (Summary, Client Management, Diagnostics, Settings), Feed Service (Profiler), Device Portal Management (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Management, My Devices, Custom Portal Files, Settings), and Threat Centric NAC (Third Party Vendors).

Administration-Identify Management-Identify

e.按一下Add，在伺服器本地資料庫中建立新使用者。

輸入和UsernameLogin Password。使用者名稱與證書在證書上的organization-unit值上的名稱相同，並且登入密碼必須與IKEv2配置檔案上指定的密碼相同。

按一Save下。

Network Access Users

Selected 0 Total 2													
Edit		Add		Change Status		Import		Export		Delete	Duplicate	Group	▼
Status	Username	Description		First Name	Last Name	Email Address	User Identity G...	Admin					
<input type="checkbox"/>	Enabled	BLUE_GROUP											
<input type="checkbox"/>	Enabled	RED_GROUP											

Administration-Identify Management-Identify

✓ Network Access User

* Username	RED_GROUP
Status	<input checked="" type="checkbox"/> Enabled ▾
Email	_____

✓ Passwords

>Password Type:	Internal Users ▾
Password	Re-Enter Password
* Login Password

Enable Password	_____

[Generate Password](#) (i)

[Generate Password](#) (i)

建立的組與組織單位值相同

步驟 3.2:配置策略集

a.導航到Policy > Policy Sets。

The screenshot shows the Cisco ISE dashboard with the 'Policy' tab selected. On the left sidebar under 'Recent Pages', 'Policy Sets' is highlighted with a red box. The main content area displays sections for 'Policy Sets', 'Posture', 'Profiling', and 'Client Provisioning'. A sidebar on the left contains 'Recent Pages' (Results, Conditions, Policy Elements, Identities, Network Devices) and 'Policy Elements' (Dictionaries, Conditions, Results). At the bottom, there are 'Shortcuts' for expanding and collapsing menus.

策略 — 策略集

b.通過單擊螢幕右側的箭頭選擇預設授權策略：

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	Default	Default policy set		Default Network Access 23	23		

Search: +

Reset Save

編輯預設策略

c.按一下旁邊的下拉菜單箭頭Authentication Policy，展開它。然後，單add (+)擊該圖示以新增新規則。

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
	FlexVPN_Router				

Search: +

新增身份驗證策略

d.輸入規則的名稱，然後在add (+)Conditions列下選擇圖示。

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
	FlexVPN_Router				

Search: +

Internal Users
Options

建立身份驗證策略

e.按一下「Attribute Editor」(屬性編輯器)文本框，然後按一下該NAS-IP-Address圖示。輸入FlexVPN集線器的IP地址(192.168.0.10)。

Conditions Studio

Library

Search by Name

- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2

Editor

Radius-NAS-IP-Address

Equals

Set to 'Is not'

Duplicate Save

NEW AND OR

Authenticate FlexVPN Hub

✓ Authentication Policy (3)

The screenshot shows a table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is at the top. The table has one row: FlexVPN, Radius-NAS-IP-Address EQUALS, Internal Users, 12, and a gear icon.

身份驗證策略

步驟 3.3:配置授權策略

a.按一下旁邊的下拉菜單箭頭Authorization Policy將其展開。然後，單add (+)擊該圖示以新增新規則。

The screenshot shows a table with columns: Status, Rule Name, Conditions, Results, Profiles, Security Groups, Hits, and Actions. A search bar is at the top. The 'Status' column for the first row is highlighted with a red box.

建立新的授權策略

b.輸入規則的名稱，然後在條件add (+)列下選擇圖示。

The screenshot shows a table with columns: Status, Rule Name, Conditions, Results, Profiles, Security Groups, Hits, and Actions. A search bar is at the top. The 'Rule Name' field contains 'RED-GROUP' and the 'Conditions' column has a '+' button highlighted with a red box.

建立新規則

c.按一下「屬性編輯器」文本框，然後按一下該Subject圖示。選擇屬Network Access - UserName性。

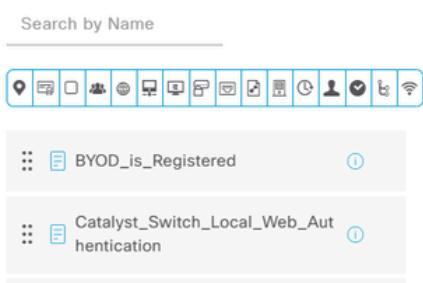
The screenshot shows two panels: 'Library' and 'Editor'. The 'Editor' panel has a search bar and a 'Select attribute for condition' section. In the 'Dictionary' dropdown, 'All Dictionaries' is selected. In the 'Attribute' dropdown, 'AD-User-Name-Domain' is selected. In the 'Info' column, 'ID' is shown. Below this, a table lists attributes: 'Network Access' with 'Attribute' 'AD-User-Join-Point' and 'Info' 'ID', and 'Network Access' with 'Attribute' 'UserName' and 'Info' 'ID'. The 'UserName' row is highlighted with a red box.

選擇Network Access - UserName

d. 選擇Contains作為運算子，然後新增證書的Organization-Unit值。

Conditions Studio

Library



Editor

Network Access-UserName
Contains RED_GROUP
Set to 'Is not'
NEW AND OR
Duplicate Save

新增組名稱

e. 在Profiles列中，按一下圖示add (+)，然後選擇Create a New Authorization Profile。

Authorization Policy (3)
Status Rule Name Conditions Profiles Security Groups Hits Actions
RED-GROUP Network Access-UserName CONTAINS RED-GROUP Select from list + Select from list 122
Profiles

新增新授權配置檔案

f. 輸入profileName。

Authorization Profile

* Name FlexVPN_RED
Description
* Access Type ACCESS_ACCEPT
Network Device Profile Cisco
Service Template
Track Movement
Agentless Posture
Passive Identity Tracking

命名授權配置檔案

g. 導航到Advanced Attributes Settings。然後，從左側的下拉選單中選擇cisco-av-pair屬性，並根據組新增分配給FlexVPN輻條的屬性。

要為此示例分配的屬性包括：

- 將環回介面指定為源。
- 指定輻條從中獲取IP地址的池。

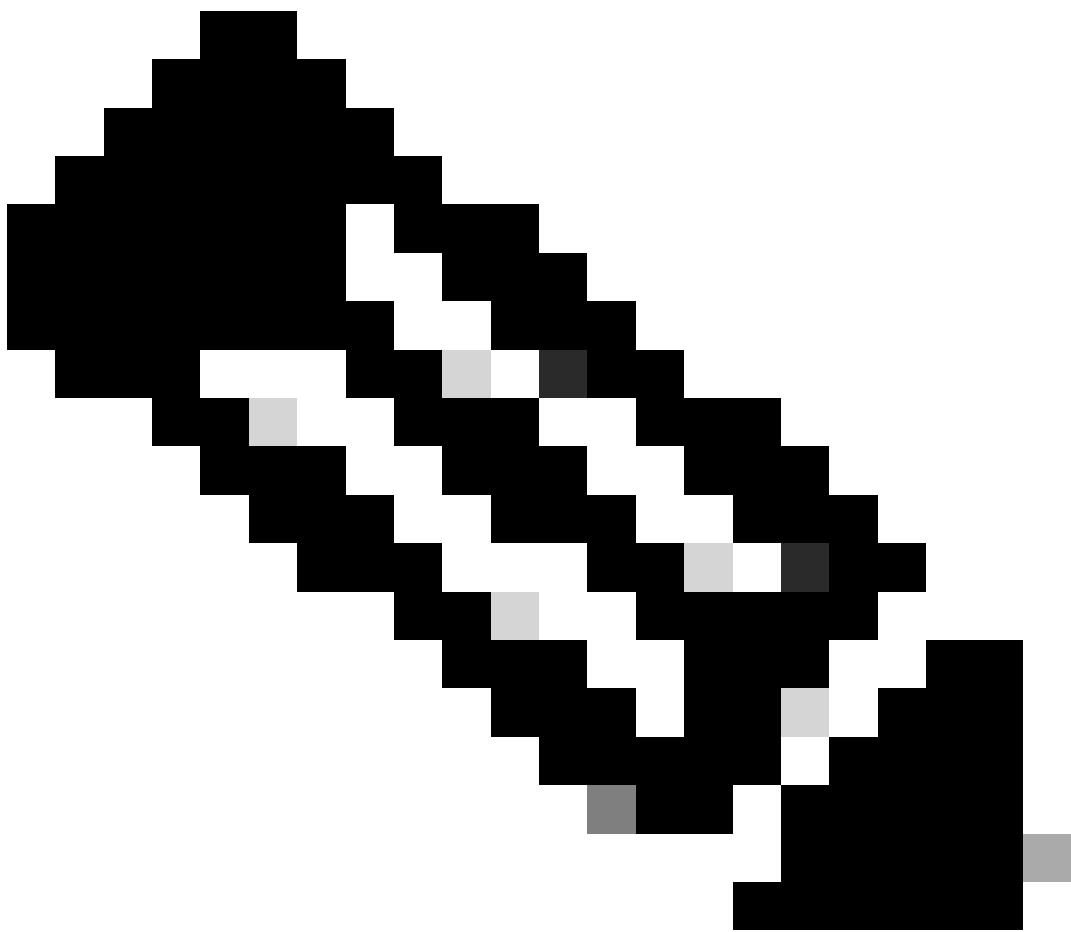
和route accept any屬route set interface性是必需的，因為沒有它們，路由將無法正確通告到分支。

```
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
```

The screenshot shows the Cisco ASA configuration interface. The top section, "Advanced Attributes Settings", displays four entries under the "Cisco:cisco-av-pair" category. The first three entries have their "Value" dropdowns expanded, showing their corresponding configurations: "ip:interface-config=ip unnumbered loopback100", "ipsec:addr-pool=RED_POOL", and "ipsec:route-accept=any". The fourth entry's "Value" dropdown is collapsed. The bottom section, "Attributes Details", shows the same four configuration lines in a text box.

```
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
```

高級屬性設定



附註：有關屬性規範（名稱、語法、說明、示例等），請參閱FlexVPN RADIUS屬性配置指南：

[FlexVPN和網際網路金鑰交換版本2配置指南，Cisco IOS XE直布羅陀版16.12.x](#)

h.在概要文authorization profile件列中分配引數。

✓ Authorization Policy (11)

		Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits Actions
<input type="checkbox"/>	RED_GROUP	<input type="checkbox"/> Network Access-UserName CONTAINS RED_GROUP	FlexVPN_RED <input type="button" value="X"/>	<input type="button" value="▼"/> <input type="button" value="+"/> Select from list	<input type="button" value="▼"/> <input type="button" value="+"/> 8

授權規則

i.按一下Save。

驗證

- 使用命令 `show ip interface brief` 令檢視隧道、虛擬模板和虛擬訪問狀態。

在集線器上，虛擬模板具有正常的up/down狀態，並且為與集線器建立連線並顯示開啟/up狀態的每個分支建立了虛擬訪問。

<#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           down
```

在分支上，隧道介面從分配給組的池接收了IP地址並顯示開啟/up狀態。

<#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
```

- 使用命令 `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
```

- 使用命令show crypto session 確認路由器之間已建立安全連線。

```
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
```

- 使用命令show ip eigrp neighbors , 確認已與其他站點建立了EIGRP鄰接關係。

```
FlexVPN_HUB#show ip eigrp neighbors  
EIGRP-IPv4 VR(Flexvpn) Address-Family Neighbors for AS(10)  
H   Address           Interface      Hold Uptime      SRTT    RT0     Q     Seq  
    (sec)             (ms)          Cnt  Num  
0   172.16.10.107    Vi1           10  00:14:00      8  1494   0   31
```

- 使用命令show ip route , 檢驗路由是否已推送到分支。

- 分支上10.20.1.10環回介面的路由已由集線器通過EIGRP獲取，並且可以通過虛擬訪問訪問

<#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和10.10.2.10的路由是通過EIGRP獲取的，可通過RED_GROUP(10.100.100.1)的源IP到達，後者可通過Tunnel0訪問。

```
<#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
```

疑難排解

本節提供的資訊可用於對此型別的部署進行故障排除。使用以下命令對通道交涉流程進行偵錯：

```
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和RADIUS調試有助於診斷輻條的授權。

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

Working Scenario

此日誌顯示授權過程和引數的分配。

```
<#root>

RADIUS(000001A7): Received from id 1645/106
AAA/BIND(000001A8): Bind i/f
AAA/AUTHOR (0x1A8): Pick method list 'FLEX'
RADIUS/ENCODE(000001A8):Orig. component type = VPN IPSEC

RADIUS(000001A8): Config NAS IP: 192.168.0.10

vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(000001A8): Config NAS IPv6: ::

RADIUS/ENCODE(000001A8): acct_session_id: 4414
RADIUS(000001A8): sending
RADIUS(000001A8): 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]
fdb 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, Ten 20

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。