配置和驗證FlexVPN解決方案

目錄

簡介

本檔案介紹Flex虛擬私人網路環境，介紹其功能，並說明如何設定每個FlexVPN拓撲。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS和Cisco IOS XE

- 網際網路金鑰交換(IKE)版本2
- 網際網路通訊協定安全(IPsec)
- FlexVPN

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS XE阿姆斯特丹版–17.3.6

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。

背景資訊

FlexVPN是思科提供的一種多功能、全面的VPN解決方案，旨在為各種型別的VPN連線提供統一框架。FlexVPN基於IKEv2（Internet金鑰交換版本2）協定構建，旨在簡化VPN的配置、管理和部署，利用一組一致的工具，可在不同的VPN型別（站點到站點、遠端訪問等）上應用相同的命令和配置步驟。 這種一致性有助於減少錯誤並使部署過程更加直觀。

IKEv2與IKEv1

FlexVPN利用IKEv2，後者支援現代加密演算法，例如AES（高級加密標準）和SHA-256（安全雜湊演算法）。 這些演算法提供強大的加密和資料完整性，保護通過VPN傳輸的資料不被攔截或篡改。

與IKEv1相比，IKEv2提供了更多身份驗證方法。除了預共用金鑰(PSK)和基於證書的以及混合身份驗證型別以外，IKEv2還允許響應方使用可擴展身份驗證協定(EAP)進行客戶端身份驗證。

在FlexVPN中，EAP用於客戶端身份驗證，路由器充當中繼，在客戶端和後端EAP伺服器（通常是RADIUS伺服器）之間傳遞EAP消息。FlexVPN支援各種EAP方法，包括EAP-TLS、EAP-PEAP、EAP-PSK等，以保護身份驗證流程。

下表顯示了IKEv1和IKEv2功能之間的差異：

	IKEv2	IKEv1
協定建立消息	4條消息	6條消息
EAP支援	是（2條額外消息）	否
安全關聯的協商	2條額外消息	3條額外消息
在UDP 500/4500上運行	是	是
NAT穿越(NAT-T)	是	是
重新傳輸和確認功能	是	是
提供身份保護、DoS保護機制和	是	是

完善的前向保密(PFS)		
下一代密碼支援	是	否

可擴充性

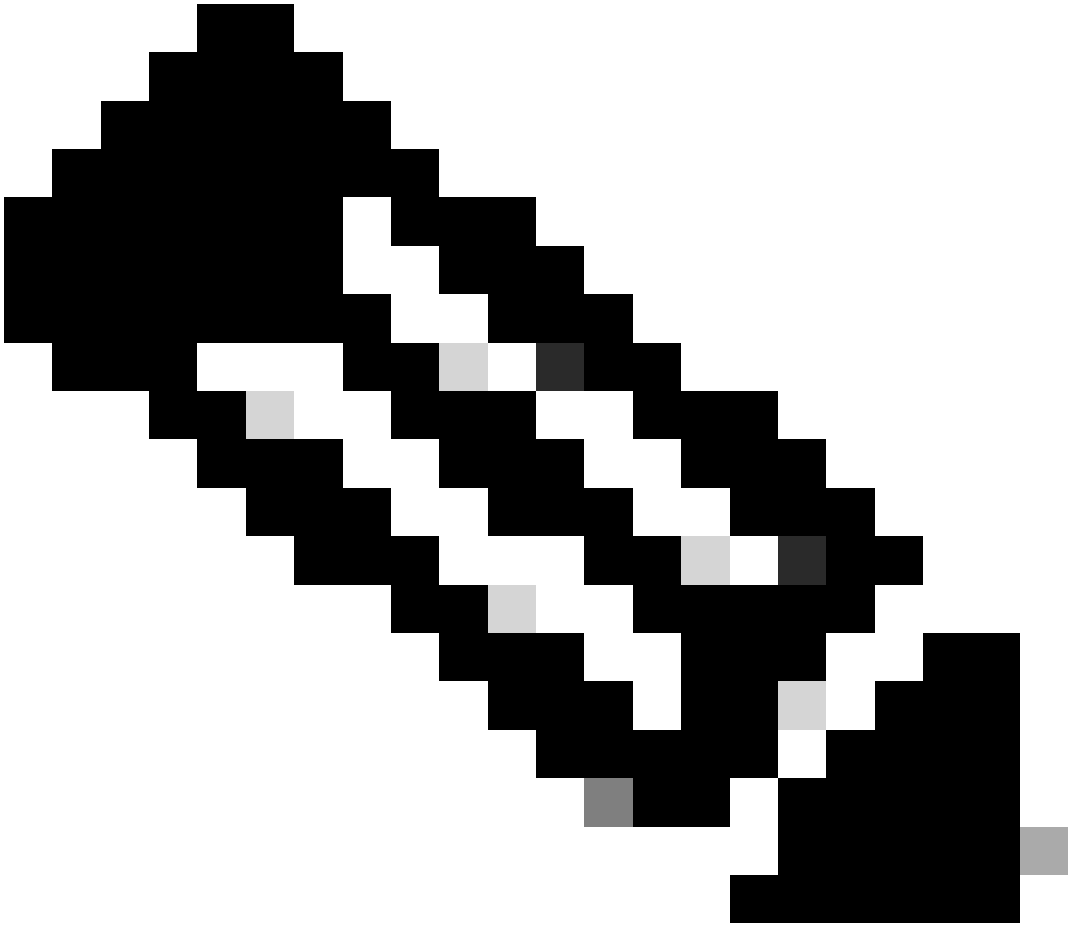
FlexVPN可輕鬆從小型辦公室擴展到大型企業網路。這使它成為擁有大量需要安全可靠網路訪問的遠端使用者的組織的理想選擇。

主要功能

- 動態配置和按需隧道：
  - 啟動FlexVPN連線，系統基於預配置的模板生成虛擬訪問介面。此介面在連線期間充當隧道端點。一旦不再需要隧道，虛擬訪問介面就會關閉，從而釋放系統資源。

- 部署靈活性：
  - 中心輻射型模型：一個中心集線器連線到多個分支機構。FlexVPN通過單個框架簡化了這些連線的設定，使其成為大型網路的理想選擇。
  - 全網狀和部分網狀拓撲：所有站點無需通過中心集線器即可直接通訊，從而減少延遲並提高效能。

- 高可用性和冗餘：
  - 冗餘集線器：支援多個集線器進行備份。如果一個集線器發生故障，分支機構可以連線到另一個集線器，確保連續連線。
  - 負載平衡：這樣可將VPN連線分佈到多個裝置上，以避免任何單個裝置過載，這對於在大型部署中保持效能至關重要。



附註：下一本指南提供有關集線器連線的負載平衡配置的詳細資訊。

[配置IKEv2負載平衡器]

- 可擴展的身份驗證和授權：
  - AAA整合：與Cisco ISE或RADIUS等AAA伺服器配合使用，集中管理使用者憑證和策略，這對於大規模使用至關重要。
  - PKI和證書：支援用於安全身份驗證的公鑰基礎架構(PKI)和數位證書，其可擴充性比使用預共用金鑰更高，尤其是在大型環境中。

路由

FlexVPN中的路由功能旨在增強可擴充性並高效管理多個VPN連線，並允許以動態方式將流量路由到每個連線。提高FlexVPN路由效率的下一個關鍵元件和機制：

- 虛擬模板介面：這是一個配置模板，其中包括VPN連線的所有必要設定，例如IP地址分配、隧道源和IPsec設定。在此介面中，ip unnumbered命令設定為借用IP位址（通常是從迴環取得），而

不是將特定IP位址設定為通道來源。這樣，每個分支就可以使用相同的模板，從而允許每個分支使用其自己的源IP地址。

- 虛擬訪問介面：這些是動態建立的介面，它們從虛擬模板介面繼承其設定。每次建立新的VPN連線時，都會基於虛擬模板建立新的虛擬訪問介面。這意味著每個VPN會話都有其自己的唯一介面，從而簡化了管理和擴展。

- 動態路由協定：它與OSPF、EIGRP和BGP over VPN隧道等路由協定配合使用。這樣可以自動更新路由資訊，這對於大型網路和動態網路非常重要。

- IKEv2通過允許FlexVPN伺服器向客戶端推送網路屬性來通告路由，客戶端會在隧道介面上安裝這些路由。客戶端還在配置模式交換期間將自己的網路與伺服器進行通訊，從而在兩端啟用路由更新。

- NHRP（下一跳解析協定）是一種動態地址解析協定，用於集中星型拓撲，用於將公共IP地址對映到專用VPN終端。它使分支可以發現其他分支IP以進行直接通訊。

授權策略

可以配置FlexVPN的IKEv2授權策略以控制VPN連線的各個方面。IKEv2授權策略定義本地授權策略並包含本地和/或遠端屬性：

- 本地屬性(例如VPN路由和轉發(VRF)以及QOS策略)在本地應用。
- 遠端屬性（例如路由）通過配置模式推送到對等裝置。
- 使用crypto ikev2 authorization policy命令定義本地策略。
- IKEv2授權策略通過AAA授權命令從IKEv2配置檔案引用。

此表概述了可在IKEv2授權策略下配置的金鑰引數。

參數	說明
AAA	與AAA伺服器整合，以驗證使用者憑證、授權訪問並記錄使用情況。策略可以指定是在路由器本地執行驗證，還是遠端執行驗證，例如通過RADIUS伺服器。
客戶端配置	將配置設定（如空閒超時值、keepalive、DNS和WINS伺服器分配等）推送到客戶端。
客戶端特定的配置	允許根據客戶端身份或組成員身份為不同客戶端配置不同的客戶端。
路由集	此組態允許特定流量通過VPN通道。這將執行在成功連線後推送到VPN客戶端的路由注入。

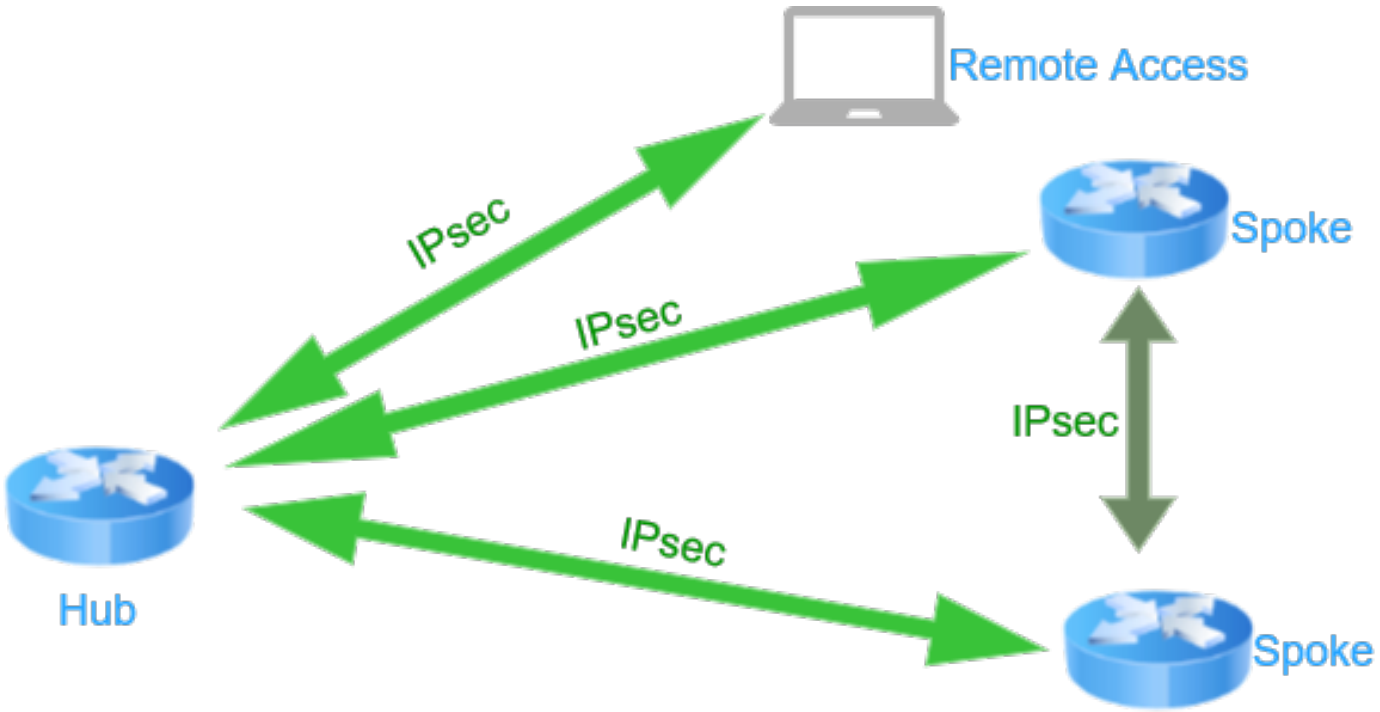
FlexVPN與其他技術的比較

FlexVPN提供一系列優勢，使其成為現代網路環境的理想選擇。通過提供統一框架，FlexVPN簡化了配置和管理，增強了安全性，支援可擴充性，確保了互操作性，並降低了複雜性。

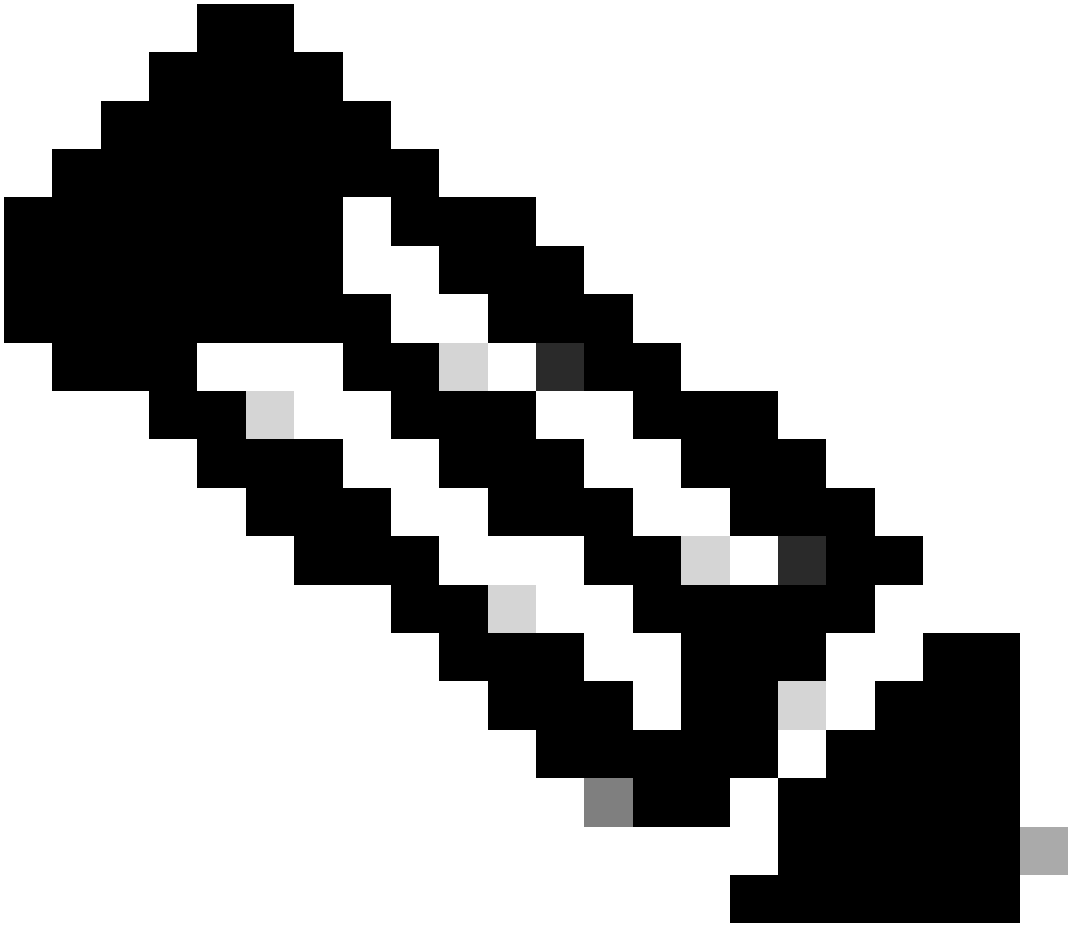
	密碼編譯對應	DMVPN	FlexVPN
動態路由	否	是	是
動態輻條到輻條直接連線	否	是	是
遠端存取VPN	是	否	是
配置推送	否	否	是
對等配置	否	否	是
對等Qos	否	是	是
AAA伺服器整合	否	否	是

網路圖表

FlexVPN允許在裝置之間建立隧道，在集線器和輻條之間建立通訊。它還支援為遠端訪問VPN使用者建立分支和連線之間的直接通訊隧道，如圖所示。



FlexVPN圖



附註：本指南未介紹遠端訪問VPN的配置。有關其配置的詳細資訊，請參閱指南：

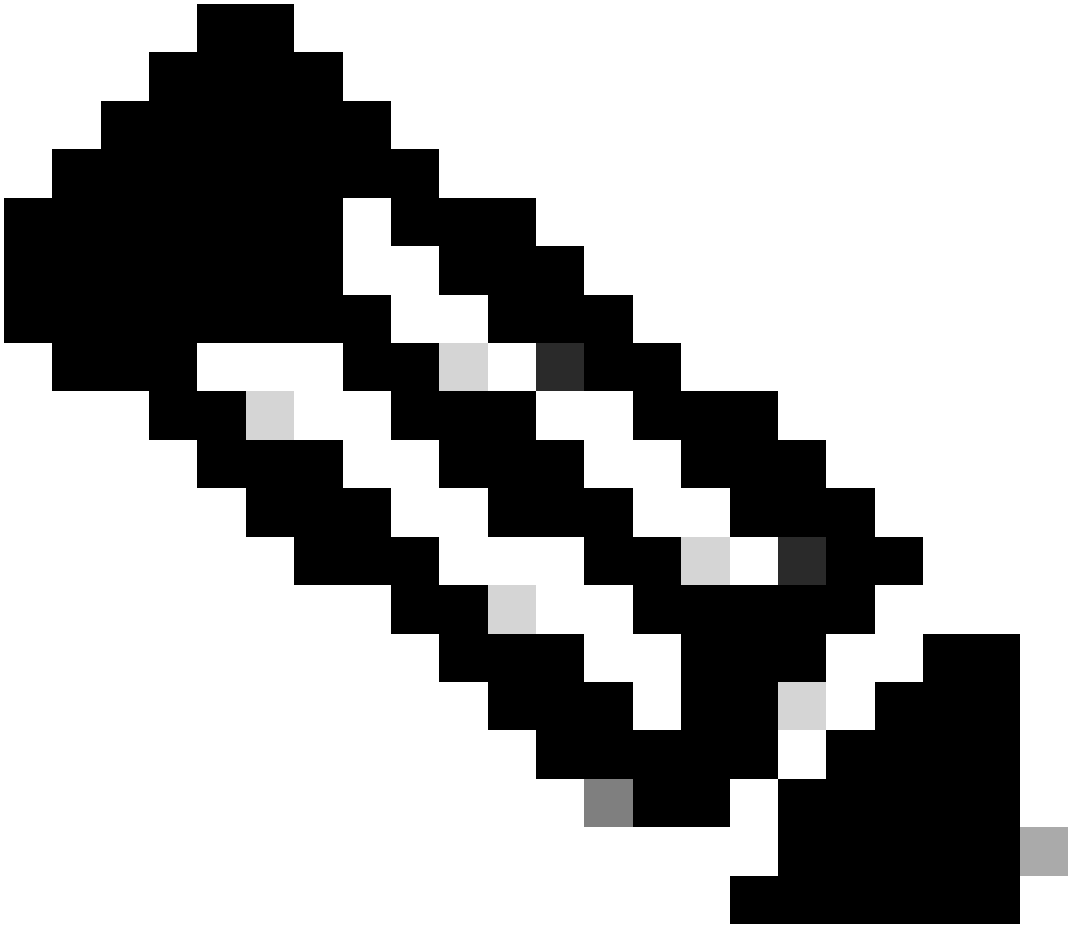
使用本地使用者資料庫為安全客戶端(AnyConnect)IKEv2遠端訪問配置FlexVPN頭端

設定

FlexVPN的特點是其配置的簡單。這種簡單性在用於各種型別VPN的一致配置塊中非常明顯。FlexVPN提供簡單的配置塊（通常適用），並根據拓撲的特定功能或要求提供可選配置或其他步驟：

- IKEv2建議：定義IKEv2安全關聯(SA)協商中使用的演算法。 建立後，將此建議附加到IKEv2策略中，以便在協商期間選擇它。
- IKEv2策略：將建議書連結到虛擬路由和轉發(VRF)例項或本地IP地址。指向IKEv2提議的策略連結。
- IKEv2金鑰環：指定預共用金鑰(PSK)，如果用於對等身份驗證，該金鑰可以是非對稱的。

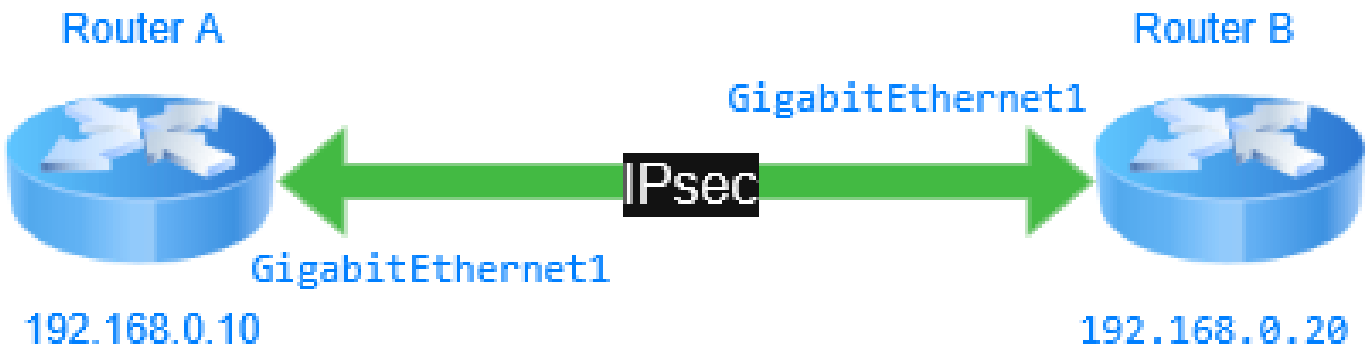
- 信任點（可選）：使用公鑰基礎設施(PKI)作為身份驗證方法時，配置對等身份驗證的身份和證書頒發機構(CA)屬性。
- AAA整合（可選）：FlexVPN將AAA伺服器(如思科ISE（身份服務引擎）或RADIUS伺服器)整合為身份驗證方法。
- IKEv2配置檔案：儲存IKE SA的不可協商引數，例如VPN對等體地址和身份驗證方法。沒有預設IKEv2配置檔案，因此您必須配置一個配置檔案並將其連線到啟動器上的IPsec配置檔案。如果使用PSK身份驗證，則IKEv2配置檔案引用IKEv2金鑰環。如果使用PKI身份驗證或AAA身份驗證方法，此處引用。
- IPsec轉換集：指定IPsec SA可接受的演算法組合。
- IPsec配置檔案：將FlexVPN設定整合到可應用於介面的單個配置檔案中。此配置檔案引用IPsec轉換集和IKEv2配置檔案。



附註：配置示例利用預共用金鑰對FlexVPN配置和簡單性進行簡單演示。雖然預共用金鑰可用於輕鬆部署和小型拓撲，但AAA或PKI方法更適用於大型拓撲。

站點到站點FlexVPN配置

FlexVPN站點到站點拓撲設計用於兩個站點之間的直接VPN連線。每個站點都配備一個隧道介面，用於建立流量可以流經的安全通道。如圖所示，該配置說明了如何在兩個站點之間建立直接VPN連線。



Site_to_Site_Diagram

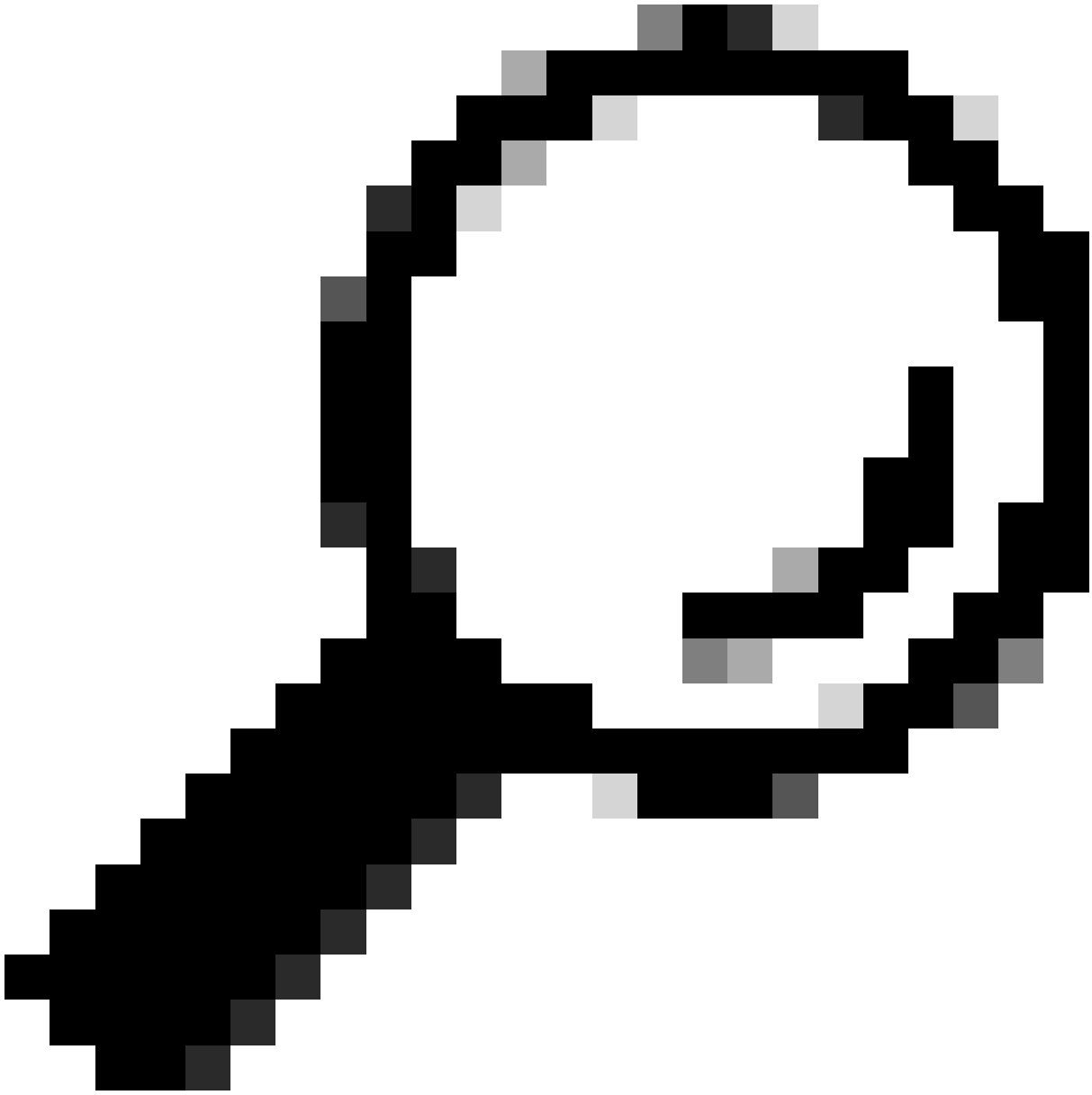
步驟 1:路由器A的配置

a.定義IKEv2建議和策略。

b.配置金鑰環並輸Pre-Shared Key入用於驗證對等體的。

c.建立IKEv2 profile並分配keyring。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



提示：該功**IKEv2 Smart Defaults**能通過覆蓋大多數使用案例而最大程度地減少了配置FlexVPN。您可以為特**IKEv2 Smart Defaults**定使用案例進行自定義，但思科不建議使用此實踐。

d.建立並Transport Set定義用於保護資料的加密和雜湊演算法。

e.建立**IPsec profile**。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f.配置隧道介面。

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g.配置動態路由以通告隧道介面。之後，它可以通告必須通過通道的其他網路。

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

步驟 2:路由器B配置

a.定義IKEv2建議和策略。

b.配置keyring並輸入用Pre-Shared Key於驗證對等體的。

c.建立IKEv2 profile並分配keyring。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
```

```
dpd 10 2 on-demand
!
```

d.建立並Transport Set定義用於保護資料的加密和雜湊演算法。

e.建立並分IPsec profile配先前建立的IKEv2配置檔案和轉換集。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f.配置Tunnel interface。

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g.配置動態路由以通告隧道介面。之後，它可以通告必須通過通道的其他網路。

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

驗證

- 使用show ip interface brief 命令檢查通道介面狀態並驗證通道是否處於up/up狀態。

<#root>

RouterB#

show ip interface brief

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

up

up

1. 使用show crypto ikev2 sa 命令確認路由器之間已建立安全連線。

<#root>

RouterB#

show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvrf/ivrf	Status
2	192.168.0.20/500	192.168.0.10/500	none/none	

READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/3139 sec

IPv6 Crypto IKEv2 SA

- 使用show crypto ipsec sa命令以確認流量已加密並通過隧道，方法是驗證封裝和解除封裝計數器是否正在遞增。

<#root>

RouterB#

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}
```

#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669

#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x93DCB8AE(2480715950)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x89C141EB(2311143915)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4607913/520)

IV size: 16 bytes
replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x93DCB8AE(2480715950)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4607991/3137)

IV size: 16 bytes
replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

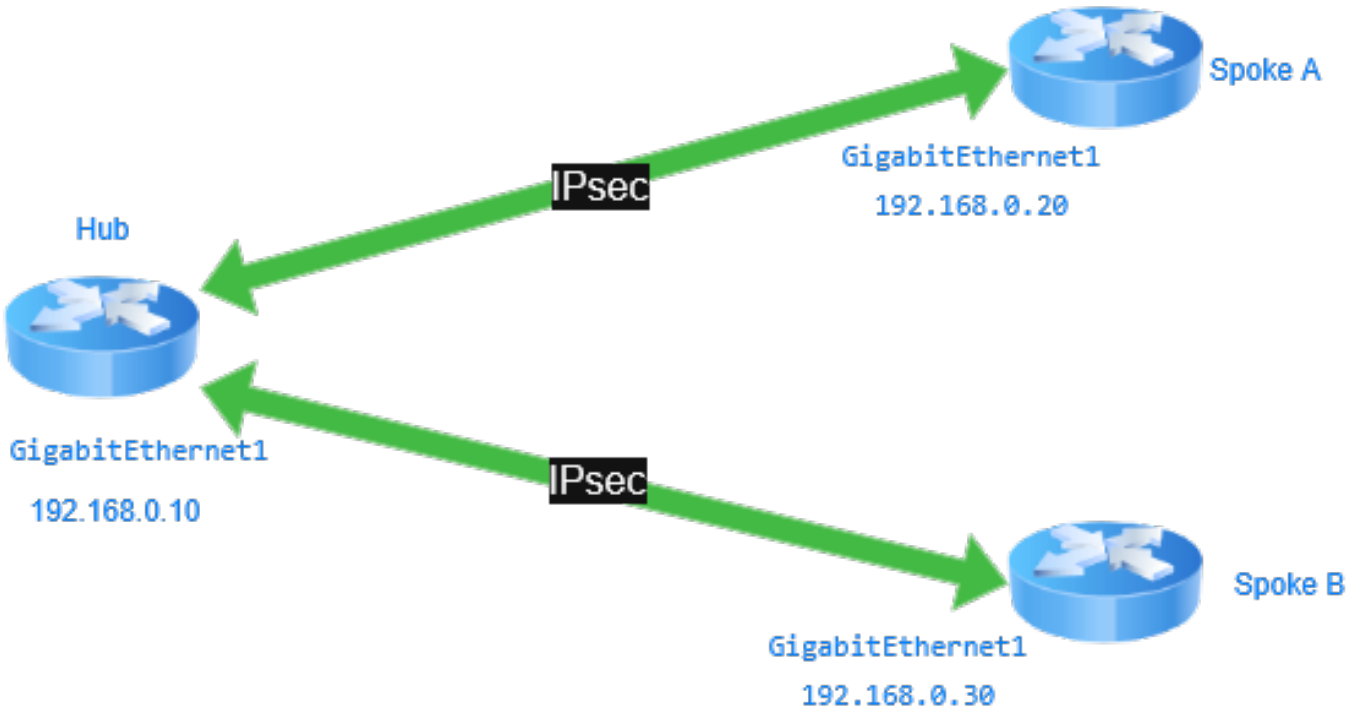
```
      outbound pcp sas:
```

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

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

中心輻射型FlexVPN

在中心輻射型拓撲中，多個分支路由器連線到中心中心路由器。此配置最適合輻條主要與集線器通訊的情況。在FlexVPN中，可以配置動態隧道以提高通訊效率。中心使用IKEv2路由將路由分發到分支路由器，從而確保無縫連接。如圖所示，配置說明了中心與分支之間的VPN連線，以及如何配置中心與多個分支建立動態連線，並能夠新增更多分支。



Hub_and_Spoke_Diagram

步驟 1:集線器配置

a.定義IKEv2建議和策略。

b.配置keyring並輸入用Pre-Shared Key於對輻條進行身份驗證的。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.在中心路由器上啟用AAA服務，然後定義一個名為FlexAuth、指定本地裝置配置策略的網路授權清單。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d.定義一個IP address poolnamedFlexPool，其中包含地址10.1.1.2到10.1.1.254。此池用於將IP地址自動分配給輻條的隧道介面。

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e.定義一個名為FlexTraffic、允許網路10.10.1.0/24的標準IP訪問清單。此ACL定義推送到FlexVPN分支以通過隧道到達它們的網路。

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

中引用了訪問清單和IP地址池**IKEv2 Authorization Policy**。

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
```

```
 route set interface
 route set access-list FlexTraffic
!
```

f.建立，IKEv2 profile分配和keyringAAA授權組。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g.建立，Transport Set定義用於保護資料的加密和雜湊演算法。

h.建立，IPsec profile分配和先IKEv2 profile前Transport Set建立的。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i.配置**virtual-template 1** as **type tunnel**。將介面引用為IP unnumbered address，並應用 **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

步驟 2:分支配置

a.定義IKEv2建議和策略。

b.配置金鑰環並輸入用於向集線器進行身份驗證的預共用金鑰。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.在中心路由器上啟用AAA服務，然後定義一個名為的網路授權清單，**FlexAuth**該清單指定本地裝置配置中的策略。接下來，配置模式配置策略以將IP地址和路由推送到FlexVPN分支。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d.定義一個命名為並允許網路10.20.2.0/24. 的標準IP訪問清單**FlexTraffic**此ACL定義此分支共用的網路，以便通過隧道。

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

在中分配訪問列**IKEv2 Authorization Policy**表。

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e.建立IKEv2 profile，分配keyring和AAA授權組。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f.建立傳輸集並定義用於保護資料的加密和雜湊演算法。

g.建立IPsec配置檔案，分配之前建立的IKEv2配置檔案和傳輸集。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h.使用協商的IP地址屬性配置隧道介面，該屬性是從隧道介面在集線器上配置的池中獲取的。

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

驗證

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

- 在集線器上，虛擬模板處於正常啟動/關閉狀態。為與中心建立連線並顯示up/up狀態的每個分支建立了虛擬訪問。
- 在分支上，隧道介面收到IP地址並顯示開啟/開啟狀態。

```
<#root>

FlexVPN_HUB#
```

```
show ip interface brief


Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up

Virtual-Access1        10.1.1.1        YES unset  up               up

 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up


FlexVPN_Spoke#

show ip interface brief

Interface               IP-Address      OK? Method  Status            Protocol
GigabitEthernet1        192.168.0.20    YES NVRAM   up                up
GigabitEthernet2        10.20.2.20      YES manual  up                up

Tunnel0                 10.1.1.8        YES manual  up                up <<<<<<

The tunnel interface received an IP address from pool defined
```

- 使用show crypto ikev2 sa 命令確認中心輻射與分支之間建立安全連線。

<#root>

```
FlexVPN_HUB#

show crypto ikev2 sa

 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none

READY

 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec


 IPv6 Crypto IKEv2 SA
```

- 使用show crypto ipsec sa命令以確認流量已加密並通過隧道，方法是驗證封裝和解除封裝計數器是否正在遞增。

<#root>

```
FlexVPN_HUB#
show crypto ipsec sa

interface: Virtual-Access1

    Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   current_peer 192.168.0.20 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xAFC2F841(2948790337)
     PFS (Y/N): N, DH group: none

     inbound esp sas:

spi: 0x7E780336(2121794358)

        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h

sa timing: remaining key lifetime (k/sec): (4607998/3010)

        IV size: 16 bytes
        replay detection support: Y

Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
```

```
spi: 0xAFC2F841(2948790337)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-

sa timing: remaining key lifetime (k/sec): (4607998/3010)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      outbound ah sas:

      outbound pcp sas:
```

- 使用show ip route 命令驗證路由是否已推送到分支：
  - 由於HUB配置中的route set interface語句，10.1.1.1/32的路由是通過IKEv2配置負載推送的。
  - 由於HUB配置中的route set access-list FlexTraffic語句，10.10.1.0/24的路由是通過IKEv2配置負載推送的。

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- 使用ping命令驗證與通告的網路的連線。

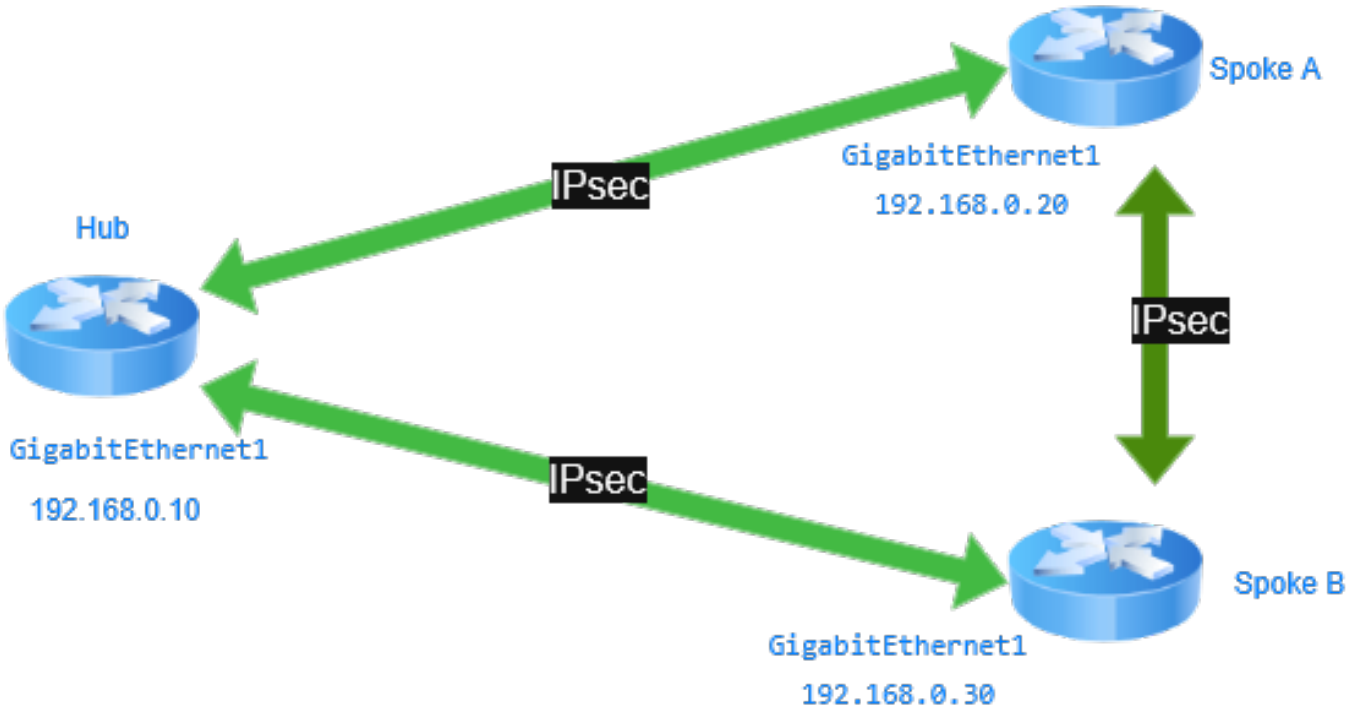
<#root>

```
FlexVPN_HUB#

ping 10.20.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms



FlexVPN_Spoke#

ping 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

分支到分支FlexVPN

在中心輻射型拓撲中，採用分支到分支連線方式的FlexVPN可實現動態、可擴展且安全的VPN通訊。集線器充當集中控制點，其中NHRP允許輻條查詢集線器的其他輻條IP地址，從而啟用直接輻條到輻條IPsec隧道，以實現高效通訊並降低延遲。

在集線器上，該命令用於通知輻條可以直接進行輻條到輻條通訊，從而通過繞過集線器進行資料平面流量來最佳化流量**ip nhrp redirect**。在分支上，該命令**ip nhrp shortcut**允許它們在收到來自集線器的重定向後，與其他分支動態建立直接隧道。該圖引用中心輻射點與輻射點之間的通訊量，以及輻射點與輻射點之間的通訊量。



Spoke_to_Spoke_Diagram

步驟 1:集線器配置

a.定義IKEv2策略和配置檔案。

b.配置keyring並輸入用Pre-Shared Key於對輻條進行身份驗證的。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.在中心路由器上啟用AAA服務，然後定義一個名為的網路授權清單，該清單從本地裝置配置中指定策略，然後配置模式配置策略以將IP地址和路由推送到FlexVPN分支FlexAuth。

```
!
aaa new-model
```

```
 aaa authorization network FlexAuth local
!
```

d.定義一個IP address pool命名**FlexPool**，，其中包含地址10.1.1.2到10.1.1.254。此池用於自動將IP地址分配給輻條的隧道介面。

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e.定義一個名為FlexTraffic、允許網路10.0.0.0/8的標準IP存取清單。此ACL定義推送到FlexVPN輻條的網路，包括連線到集線器的其他輻條的網路，因此這些輻條知道首先透過集線器到達這些網路。

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

訪問清單和在IP address pool中進行了分**IKEv2 Authorization Policy**配。

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f.建立IKEv2 profile ，分配keyring和AAA授權組。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g.建立並Transport Set定義用於保護資料的加密和雜湊演算法。

h.建立、IPsec profile分配和IKEv2 profile先Transport Set前建立。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i.配置**virtual-template 1** as **type tunnel**。將介面引用為**IP unnumbered address**並應用**IPsec profile**。

該命**ip nhrp redirect**令在虛擬模板上配置，以通知輻條與其他輻條建立直接連線以到達其網路。

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

步驟 2:分支A配置

a.定義IKEv2策略和配置檔案。

b.配置keyring並輸入用Pre-Shared Key於對輻條進行身份驗證的。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.在中心路由器上啟用AAA服務，然後定義一個名為的網路授權清單，**FlexAuth**該清單指定本地裝置配置中的策略。接下來，配置模式配置策略以將IP地址和路由推送到FlexVPN分支。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d.定義一個命名為並允許網路10.20.2.0/24的標準IP訪問列**FlexTraffic**表。此ACL定義此分支共用的網路，以便通過隧道。

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

訪問清單在 **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e.建立IKEv2 profile，分配keyring和AAA授權組。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f.建立並Transport Set定義用於保護資料的加密和雜湊演算法。

g.建立IPsec配置檔案，分配之前建立的IKEv2配置檔案和傳輸集。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h.配置隧道介面和虛擬模**Virtual-Template1**板。指定建立為支援的**NHRP shortcuts**dVTI。此外，還將tunnel0設定為上的未編號地virtual-template址。

在分支**ip nhrp shortcut**上配置該命令，以使它們能夠根據來自集線器的NHRP重定向消息動態建立到其他分支的直接隧道。

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

步驟 3:分支B配置

a.定義IKEv2策略和配置檔案。

b.配置keyring並輸入用Pre-Shared Key於對輻條進行身份驗證的。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
```

```
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.在中心路由器上啟用AAA服務，然後定義名為的網路授權清單，該清單從本地裝置配置中指定策略，然後配置模式配置策略以將IP地址和路由推送到FlexVPN分支**FlexAuth**。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d.定義一個命名為並允許網路10.30.3.0/24. 的標準IP訪問清單**FlexTraffic**此ACL定義此分支共用的網路，以便通過隧道。

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

訪問清單在中引用 IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e.建立IKEv2 profile ，分配keyring和AAA授權組。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f.建立並Transport Set定義用於保護資料的加密和雜湊演算法。

g.建立、IPsec profile分配和先IKEv2 profile前創Transport Set建的。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h.配置tunnel interface和virtual template。指**Virtual-Template1**定建立為支援的dVTINHRP shortcuts。此外，還將tunnel0設定為上的未編號地virtual-template址。

在分支**ip nhrp shortcut**上配置該命令，以使它們能夠根據來自集線器的NHRP重定向消息動態建立到其他分支的直接隧道。

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

驗證

使用show ip interface brief命令檢視隧道、虛擬模板和虛擬訪問狀態。現在，它是輻射到輻射的直接連線：

- 在輻條上，虛擬模板處於正常的up/down狀態。為處於up/up狀態的連線建立虛擬訪問。

```
FlexVPN_Spoke#
show ip interface brief

Interface                  IP-Address      OK?  Method  Status                Protocol
GigabitEthernet1           192.168.0.30    YES  NVRAM   up                    up
GigabitEthernet2           10.20.2.20      YES  manual  up                    up
Tunnel0                    10.1.1.12       YES  manual  up                    up


Virtual-Access1            10.1.1.12       YES  unset   up                    up
Virtual-Template1          10.1.1.12       YES  unset   up                    down
```

- 使用show crypto ikev2 sa 命令確認每台裝置之間建立安全連線。
- 使用show crypto ipsec sa命令以確認流量已加密並通過隧道，方法是驗證封裝和解除封裝計數器是否正在遞增。
- 使用show ip nhrp命令驗證輻條之間的流量重新導向。
  <#root>

```
FlexVPN_Spoke#
show ip nhrp

10.1.1.10/32 via 10.1.1.10
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:
dynamic
, Flags: router nhop rib nho
   NBMA address: 192.168.0.30
10.30.3.0/24 via 10.1.1.10

   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:
dynamic
, Flags: router rib nho
   NBMA address: 192.168.0.30
```

使用show ip route 命令檢驗路由是否已推送到分支：

- 這兩個路由與Virtual-Access1介面關聯，是新的，並與NHRP快捷方式關聯。
- %字元表示下一跳覆蓋。

<#root>

```
FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>
```

```
Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0

S  %     10.1.1.10/32 is directly connected, Virtual-Access1


C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2

S  %     10.30.3.0/24 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, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- 使用ping命令驗證與通告的網路的連線。

<#root>

```
FlexVPN_Spoke#

ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!


Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。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

NHRP調試有助於診斷分支到分支的連線。

debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing

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）。