配置和验证FlexVPN解决方案

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- IKEv2与IKEv1
- 可扩展性
- 主要特点
- 路由
- 授权策略
- FlexVPN与其他技术的比较

网络图

配置

- 站点到站点FlexVPN配置
  - 步骤 1：路由器 A 配置
  - 步骤 2：路由器 B 配置
  - 验证
- 集中星型FlexVPN
  - 步骤 1：中心配置
  - 步骤 2：分支配置
  - 验证
- 分支到分支FlexVPN
  - 步骤 1：中心配置
  - 步骤 2：辐条A配置
  - 步骤 3：分支B配置
  - 验证

故障排除

简介

本文档介绍Flex虚拟专用网络环境，介绍其功能，并说明如何配置每个FlexVPN拓扑。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS和Cisco IOS XE

- 互联网密钥交换(IKE)版本2
- Internet协议安全(IPsec)
- FlexVPN

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科IOS XE Amsterdam-17.3.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FlexVPN是思科提供的功能全面的VPN解决方案，旨在为各种类型的VPN连接提供统一框架。FlexVPN基于IKEv2（Internet密钥交换版本2）协议构建，旨在简化VPN的配置、管理和部署，利用一组一致的工具，将相同的命令和配置步骤应用于不同的VPN类型（站点到站点、远程访问等）。 这种一致性有助于减少错误并使部署过程更加直观。

IKEv2与IKEv1

FlexVPN利用IKEv2，它支持现代加密算法，例如AES（高级加密标准）和SHA-256（安全散列算法）。 这些算法提供强大的加密和数据完整性，保护通过VPN传输的数据不被拦截或篡改。

与IKEv1相比，IKEv2提供了更多身份验证方法。除了预共享密钥(PSK)和基于证书的身份验证类型和混合身份验证类型外，IKEv2还允许响应方使用可扩展身份验证协议(EAP)进行客户端身份验证。

在FlexVPN中，EAP用于客户端身份验证，路由器充当中继，在客户端和后端EAP服务器（通常是RADIUS服务器）之间传递EAP消息。FlexVPN支持各种EAP方法，包括EAP-TLS、EAP-PEAP、EAP-PSK等，以保护身份验证过程。

下表显示了IKEv1和IKEv2功能之间的差异：

	IKEv2	IKEv1
协议建立消息	4条消息	6条消息
EAP支持	是（2条额外消息）	无
安全关联协商	2条额外消息	3条额外消息
通过UDP 500/4500运行	Yes	Yes
NAT穿越(NAT-T)	Yes	Yes
重新传输和确认功能	Yes	Yes
提供身份保护、DoS保护机制和完全向前保密(PFS)	Yes	Yes

下一代密码支持	Yes	无

可扩展性

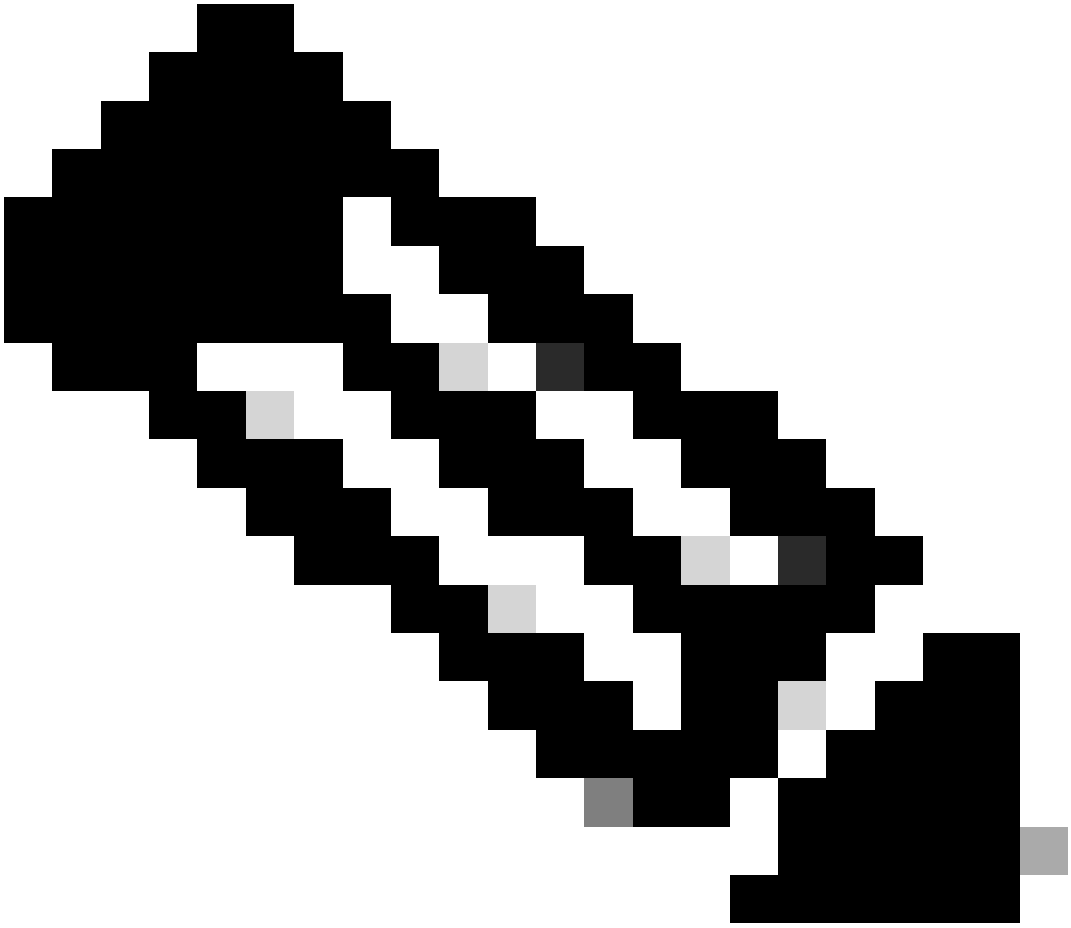
FlexVPN可以轻松地从小型办公室扩展到大型企业网络。这使它成为拥有大量远程用户、需要安全可靠的网络访问的组织的理想选择。

主要特点

- 动态配置和按需隧道：
  - 启动FlexVPN连接，系统根据预配置的模板生成虚拟访问接口。此接口在连接期间充当隧道终端。一旦不再需要隧道，虚拟访问接口就会被关闭，从而释放系统资源。

- 部署灵活性：
  - 中心辐射型模型：一个中心集线器连接到多个分支机构。FlexVPN通过单一框架简化了这些连接的设置，使其成为大型网络的理想选择。
  - 全网状拓扑和部分网状拓扑：所有站点可以直接通信，无需通过中央集线器，从而减少了延迟并提高了性能。

- 高可用性和冗余：
  - 冗余集线器：支持多个集线器进行备份。如果一台集线器发生故障，分支机构可以连接到另一台集线器，确保连续连接。
  - 负载均衡：这将VPN连接分布到多个设备上，以避免任何单个设备过载，这对于在大型部署中保持性能至关重要。



注意：下一指南提供有关集线器连接的负载平衡配置的详细信息。

配置IKEv2负载均衡器

- 可扩展的身份验证和授权：
  - AAA集成：与Cisco ISE或RADIUS等AAA服务器配合使用，集中管理用户凭证和策略，这对于大规模使用至关重要。
  - PKI和证书：支持用于安全身份验证的公钥基础设施(PKI)和数字证书，比使用预共享密钥更具可扩展性，尤其是在大型环境中。

路由

FlexVPN中的路由功能旨在增强可扩展性并高效管理多个VPN连接，并允许以动态方式将流量路由到每个连接。使FlexVPN路由变得高效的下一个关键组件和机制：

- 虚拟模板接口:这是一个配置模板，其中包含VPN连接的所有必要设置，例如IP地址分配、隧道源和IPsec设置。在此接口中，配置命令以借用IP地址ip unnumbered，通常是从环回接口借用

，而不是将特定IP地址配置为隧道源。这使每个分支可以使用相同的模板，从而允许每个分支使用其自己的源IP地址。

- 虚拟访问接口：这些是动态创建的接口，从虚拟模板接口继承其设置。每次建立新的VPN连接时，都会基于虚拟模板创建新的虚拟访问接口。这意味着每个VPN会话都有自己的唯一接口，从而简化了管理和扩展。

- 动态路由协议：它与OSPF、EIGRP和BGP over VPN隧道等路由协议配合使用。这可以保持路由信息的自动更新，这对于大型和动态网络非常重要。

- IKEv2通过允许FlexVPN服务器将网络属性推送到客户端（客户端在隧道接口上安装这些路由）来通告路由。在配置模式交换期间，客户端还会将其自己的网络与服务器通信，从而在两端启用路由更新。

- NHRP（下一跳解析协议）是一种动态地址解析协议，用于集中星型拓扑，将公有IP地址映射到私有VPN终端。它使分支能够发现用于直接通信的其他分支IP。

授权策略

可以配置FlexVPN的IKEv2授权策略以控制VPN连接的各个方面。IKEv2授权策略定义本地授权策略并包含本地和/或远程属性：

- 本地属性(例如VPN路由和转发(VRF)以及QOS策略)在本地应用。
- 远程属性（例如路由）通过配置模式推送到对等设备。
- 使用crypto ikev2 authorization policy命令定义本地策略。
- IKEv2授权策略通过AAA授权命令从IKEv2配置文件中引用。

下表概述了可在IKEv2授权策略下配置的密钥参数。

参数	描述
AAA	与AAA服务器集成，以验证用户凭证、授权访问并记录使用情况。策略可以指定是在路由器上本地执行验证，还是远程执行验证，例如通过RADIUS服务器。
客户端配置	将配置设置（如空闲超时值、保持连接、DNS和WINS服务器分配等）推送到客户端。
客户端特定配置	允许根据客户端的身份或组成员身份为不同的客户端进行不同的配置。
路由集	此配置允许特定流量通过VPN隧道。这将执行路由注入，在连接成功时推送到VPN客户端。

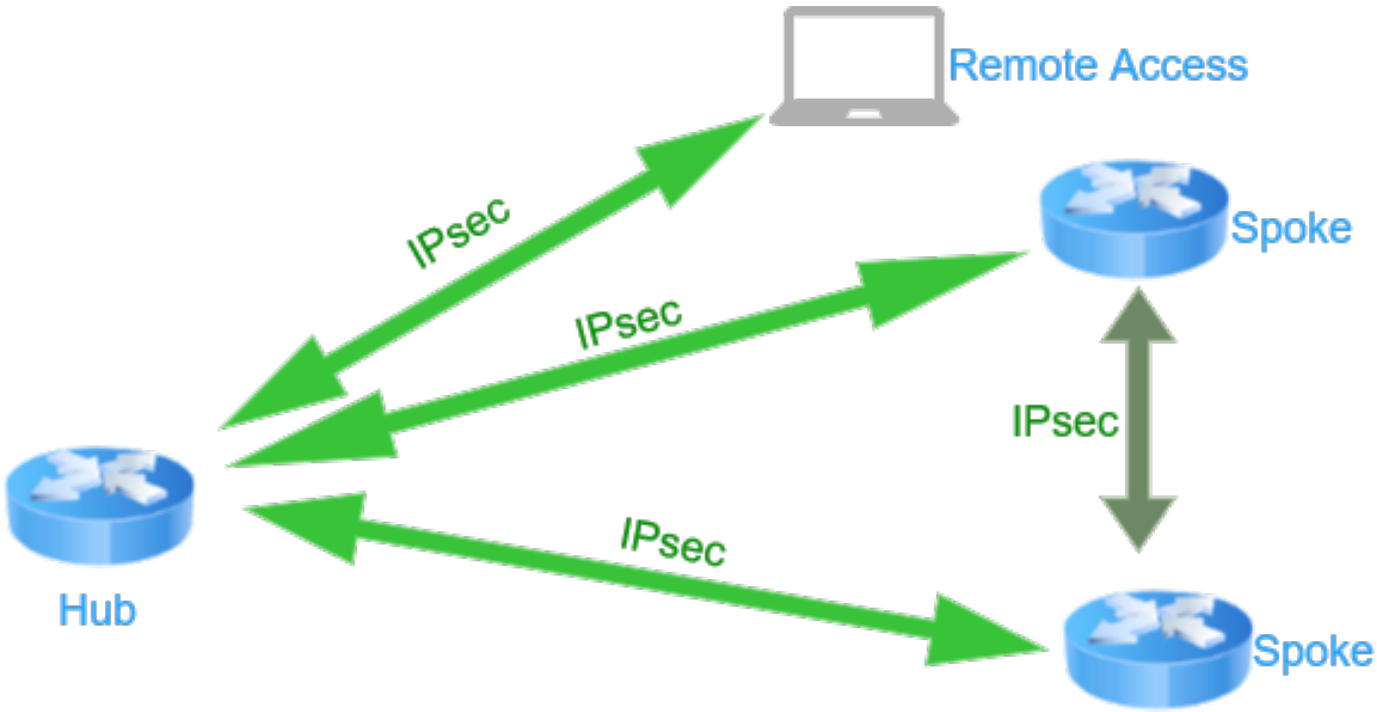
FlexVPN与其他技术的比较

FlexVPN提供一系列优势，使其成为现代网络环境的理想选择。通过提供统一框架，FlexVPN可简化配置和管理、增强安全性、支持可扩展性、确保互操作性并降低复杂性。

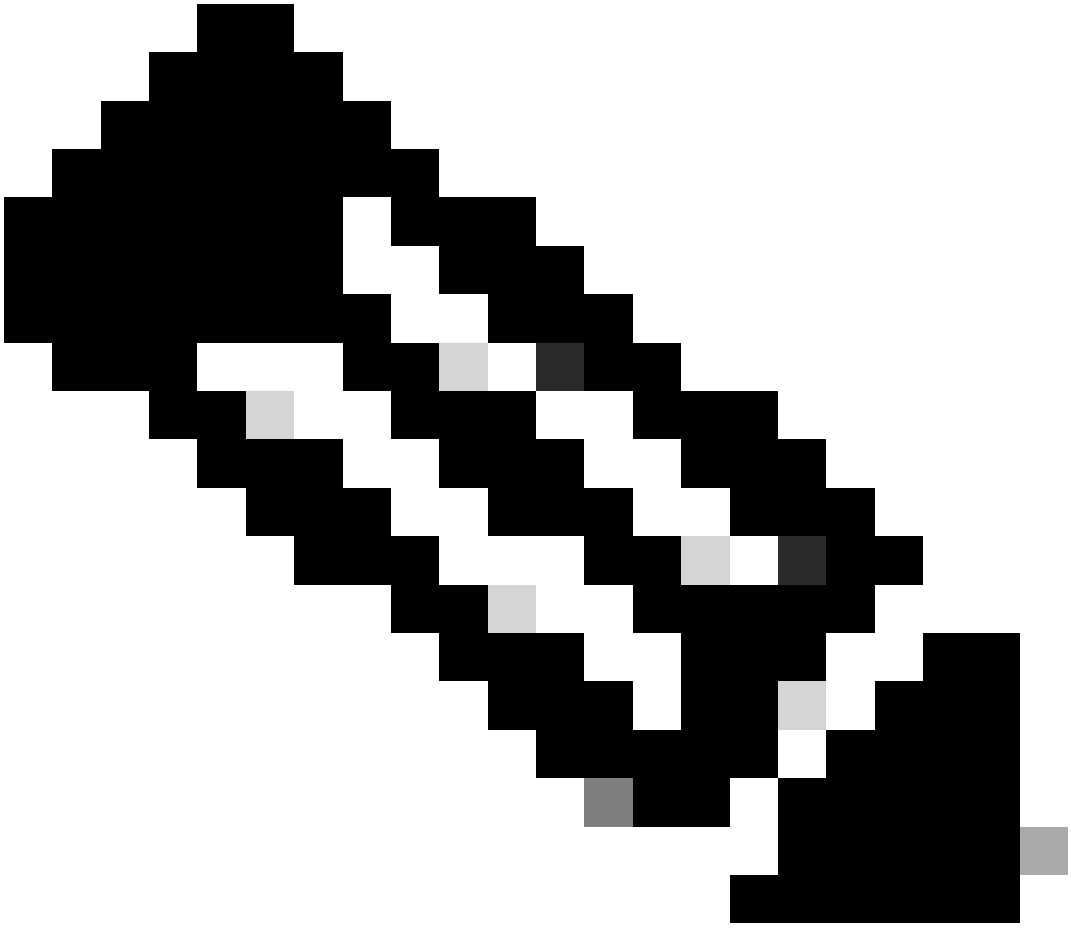
	加密映射	DMVPN	FlexVPN
动态路由	无	Yes	Yes
动态分支到分支直接连接	无	Yes	Yes
远程访问 VPN	Yes	无	Yes
配置传出	无	无	Yes
对等体配置	无	无	Yes
对等体Qos	无	Yes	Yes
AAA服务器集成	无	无	Yes

网络图

FlexVPN允许在设备之间创建隧道，从而建立集线器和辐射点之间的通信。它还支持为远程访问VPN用户的分支和连接之间的直接通信创建隧道，如图所示。



FlexVPN图



注意：本指南未介绍远程访问VPN的配置。有关其配置的详细信息，请参阅指南：

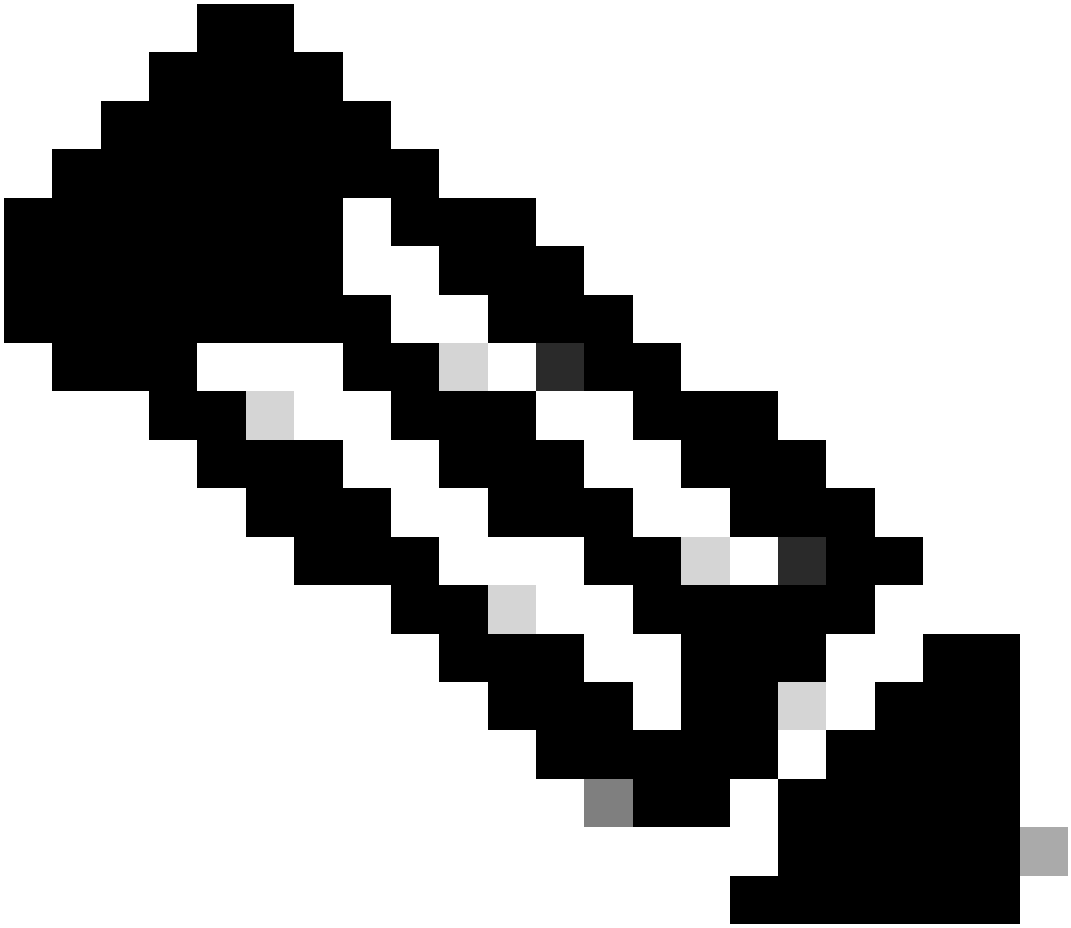
使用本地用户数据库为安全客户端(AnyConnect)IKEv2远程访问配置FlexVPN前端

配置

FlexVPN的特点是其配置简单。这种简单性在用于各种类型的VPN的一致配置块中非常明显。FlexVPN提供简单明了且一般适用的配置块，可根据拓扑的特定功能或要求提供可选配置或其他步骤：

- IKEv2提议：定义在IKEv2安全关联(SA)协商中使用的算法。 创建后，将此建议附加到IKEv2策略，以便在协商期间进行选择。
- IKEv2策略：将建议书链接到虚拟路由和转发(VRF)实例或本地IP地址。指向IKEv2提议的策略链接。
- IKEv2密钥环：指定预共享密钥(PSK)，如果用于对等身份验证，则可以是非对称的。

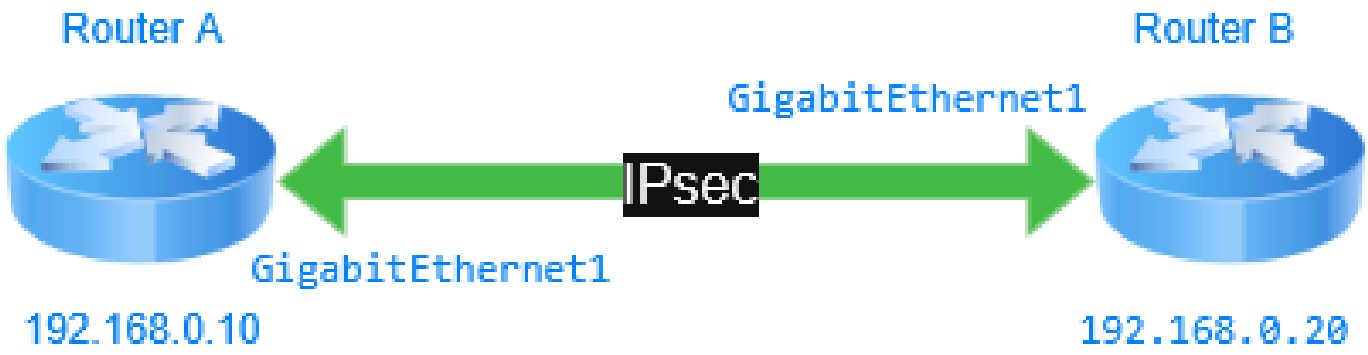
- 信任点（可选）：使用公钥基础设施(PKI)作为身份验证方法时，配置对等身份验证的身份和证书颁发机构(CA)属性。
- AAA集成（可选）：FlexVPN集成了AAA服务器，例如思科ISE（身份服务引擎）或RADIUS服务器作为身份验证方法。
- IKEv2配置文件：存储IKE SA的不可协商参数，例如VPN对等体地址和身份验证方法。没有默认IKEv2配置文件，因此您必须配置一个配置文件并将其附加到启动器上的IPsec配置文件。如果使用PSK身份验证，则IKEv2配置文件引用IKEv2密钥环。如果使用PKI身份验证或AAA身份验证方法，请参阅此处。
- IPsec转换集：指定IPsec SA可接受的算法组合。
- IPSec 简档:将FlexVPN设置整合到可应用于接口的单个配置文件中。此配置文件引用IPsec转换集和IKEv2配置文件。



注意：配置示例利用预共享密钥直观地展示了FlexVPN配置和简便性。虽然可以使用预共享密钥实现轻松部署和小型拓扑，但AAA或PKI方法更适用于大型拓扑。

站点到站点FlexVPN配置

FlexVPN站点到站点拓扑设计用于两个站点之间的直接VPN连接。每个站点都配备一个隧道接口，用于建立流量可以流经的安全通道。该配置说明了如何在两个站点之间建立直接VPN连接，如图所示。



Site_to_Site_Diagram

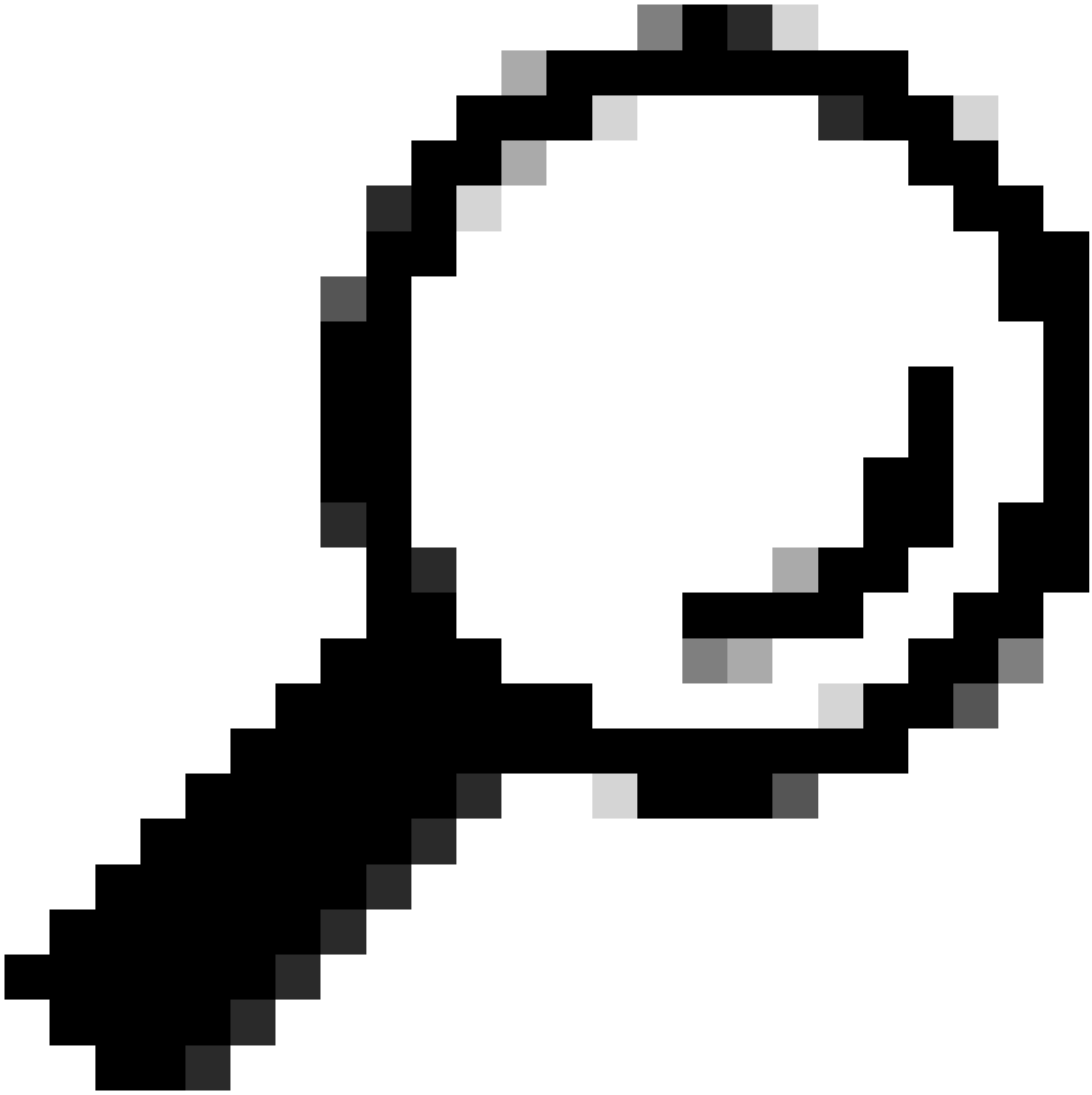
步骤 1：路由器 A 配置

a.定义IKEv2建议和策略。

b.配置密钥环并输入Pre-Shared Key用于对等体进行身份验证的。

c.创建IKEv2 profile并分配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：该功**IKEv2 Smart Defaults**能通过覆盖FlexVPN大多数使用案例来最大程度地减少配置。您可以为特**IKEv2 Smart Defaults**定使用案例进行自定义，但思科不建议使用此实践。

d.创建并Transport Set定义用于保护数据的加密和散列算法。

e.创建**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.配置隧道接口。

```
!
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.配置动态路由以通告隧道接口。之后，它可以通告必须通过隧道的其他网络。

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

步骤 2：路由器 B 配置

a.定义IKEv2建议和策略。

b.配置并keyring输入用于Pre-Shared Key验证对等体身份的。

c.创建IKEv2 profile并分配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.创建并Transport Set定义用于保护数据的加密和散列算法。

e.创建并分IPsec profile配先前创建的IKEv2配置文件和转换集。

```
!
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.配置动态路由以通告隧道接口。之后，它可以通告必须通过隧道的其他网络。

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

验证

- 使用show ip interface brief命令查看隧道接口状态并验证隧道是否处于up/up状态。

<#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命令确认路由器之间已建立安全连接。

<#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命令确认流量已加密并通过隧道，方法是验证封装和封装计数器是否正在递增。

<#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:

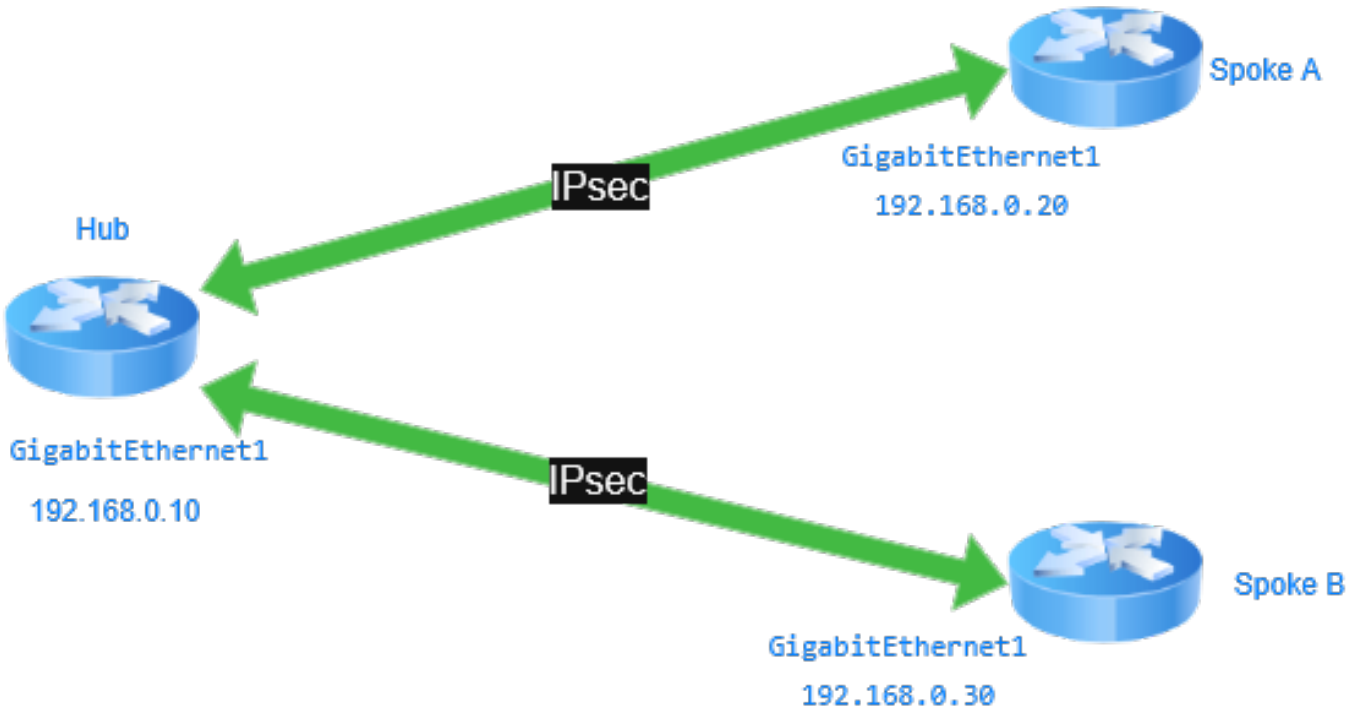
```
      outbound pcp sas:
```

- 使用show ip eigrp neighbors命令确认已与其他站点建立了EIGRP邻接关系。

```
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
```

集中星型FlexVPN

在集中星型拓扑中，多个分支路由器连接到中央中心路由器。此配置最适合辐射点主要与集线器通信的情况。在FlexVPN中，可以配置动态隧道以提高通信效率。中心使用IKEv2路由将路由分发到分支路由器，确保无缝连接。如图所示，配置说明了中心点和分支点之间的VPN连接，以及中心点如何配置为与多个分支建立动态连接并能够添加更多分支。



Hub_and_Spoke_Diagram

步骤 1：中心配置

a.定义IKEv2建议和策略。

b.配置并keyring输入用于Pre-Shared Key对辐射点进行身份验证的。

```
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.在中心路由器上启用AAA服务，然后定义一个名为的网络授权列表FlexAuth，该列表从本地设备配置指定策略。

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

d.定义一个IP address pool命名FlexPool，其中包含地址10.1.1.2到10.1.1.254。此池用于自动为分支的隧道接口分配IP地址。

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

e.定义一个名为FlexTraffic、允许网络10.10.1.0/24的标准IP访问列表。此ACL定义推送到FlexVPN分支以通过隧道到达它们的网络。

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

中引用了访问列表和IP地址池**IKEv2 Authorization Policy**。

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

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

f.创建，IKEv2 profile分配和keyringAAA授权组。

```
!
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.创建，Transport Set定义用于保护数据的加密和哈希算法。

h.创建，IPsec profile分配和IKEv2 profile先Transport Set前创建。

```
!
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**。将接口引用为IP unnumbered address，并应用 **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
!
```

步骤 2：分支配置

a.定义IKEv2建议和策略。

b.配置密钥环并输入用于向集线器进行身份验证的预共享密钥。

```
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.在中心路由器上启用AAA服务，然后定义一个名为的网络授权列表，**FlexAuth**该列表从本地设备配置指定策略。接下来，配置模式配置策略以将IP地址和路由推送到FlexVPN分支。

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

d.定义命名并允许网络**FlexTraffic**10.20.2.0/24. 的标准IP访问列表此ACL定义此分支共享的网络，以便通过隧道。

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

在中分配访问列**IKEv2 Authorization Policy**表。

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

e.创建，IKEv2 profile分配和keyringAAA授权组。

```
!
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.创建传输集并定义用于保护数据的加密和散列算法。

g.创建IPsec配置文件，分配之前创建的IKEv2配置文件和传输集。

```
!
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.使用协商的IP地址属性配置隧道接口，该属性是从隧道接口在集线器上配置的池中获得的。

```
!
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
!
```

验证

使用show ip interface brief命令查看隧道、虚拟模板和虚拟访问状态：

- 在集线器上，虚拟模板处于正常up/down状态。系统会为每个分支创建虚拟访问，这些分支与中心建立连接并显示打开/打开状态。
- 在分支上，隧道接口接收到IP地址并显示打开/打开状态。

```
<#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命令确认中心点和分支点之间已建立安全连接。

<#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命令确认流量已加密并通过隧道，方法是验证封装和封装计数器是否正在递增。

<#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命令验证路由是否已推送到分支：
  - 由于HUB配置中的route set interface语句，10.1.1.1/32的路由是通过IKEv2配置负载推送的。
  - 由于HUB配置中的route set access-list FlexTraffic语句，通过IKEv2配置负载推送了10.10.1.0/24的路由。

<#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命令验证与通告网络的连接。

<#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#
```

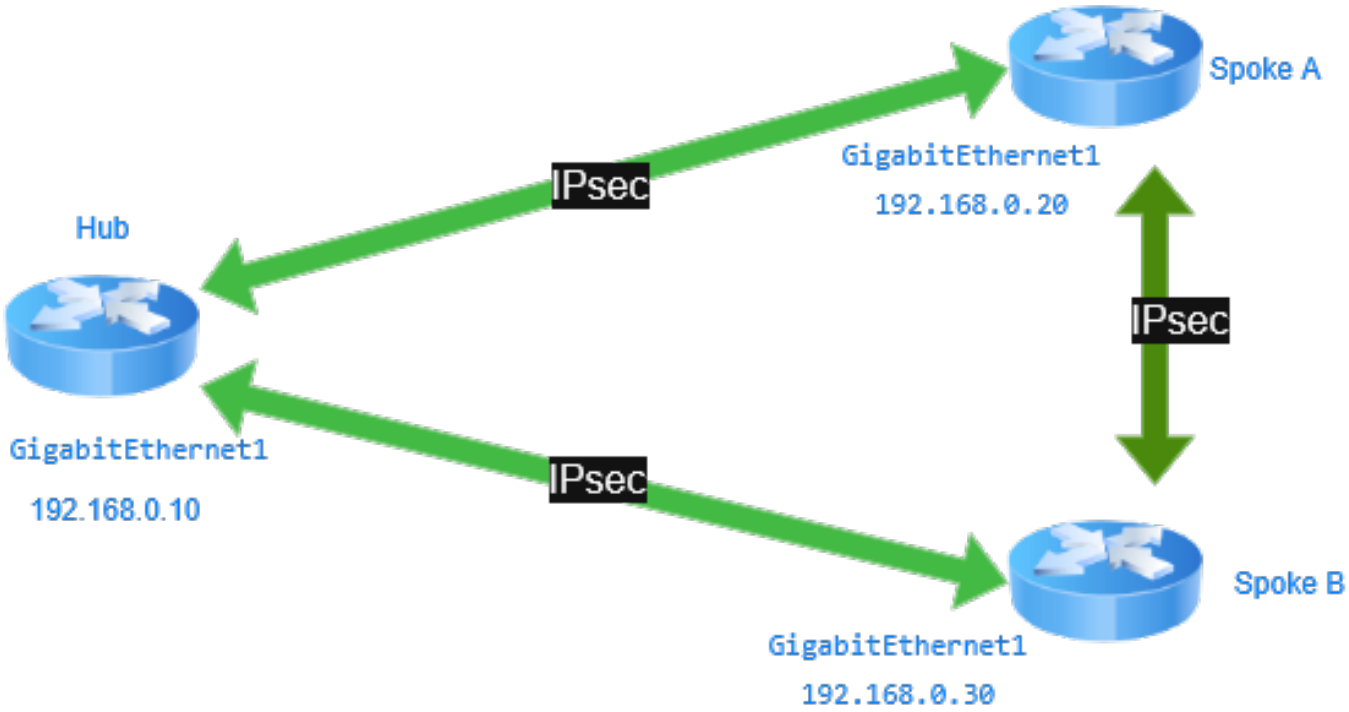
ping 10.10.1.10

```
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

中心辐射型拓扑中支持分支到分支连接的FlexVPN可实现动态、可扩展且安全的VPN通信。集线器用作集中控制点，其中NHRP允许辐条查询集线器的其他辐条IP地址，从而启用直接辐条到辐条IPsec隧道，以实现高效通信并降低延迟。

在集线器上，命令用于通知辐条可以直接进行辐条到辐条通信，从而通过绕过集线器进行数据平面流量来优化流量**ip nhrp redirect**。在辐射点上，该命**ip nhrp shortcut**令允许它们在收到来自集线器的重定向后，与其他辐射点动态建立直接隧道。该图引用中心辐射点与辐射点之间的流量，以及辐射点与辐射点之间的通信。



Spoke_to_Spoke_Diagram

步骤 1：中心配置

a.定义IKEv2策略和配置文件。

b.配置并keyring输入用于Pre-Shared Key对辐射点进行身份验证的。

```
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.在中心路由器上启用AAA服务，然后定义一个名为的网络授权列表，该列表从本地设备配置指定策略，然后配置模式配置策略，将IP地址和路由推送到FlexVPN分支**FlexAuth**。

```
!
aaa new-model
```

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

d.定义一个IP address pool命名**FlexPool**,，该名称包含地址10.1.1.2到10.1.1.254。此池用于将IP地址自动分配给辐条的隧道接口。

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

e.定义一个名为FlexTraffic、允许网络10.0.0.0/8的标准IP访问列表。此ACL定义推送到FlexVPN分支的网络，包括连接到集线器的其他分支的网络，因此这些分支知道首先通过集线器到达这些网络。

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

访问列表和IP address pool在中进行分**IKEv2 Authorization Policy**配。

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

f.创建，IKEv2 profile分配和keyringAAA授权组。

```
!
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.创建并Transport Set定义用于保护数据的加密和散列算法。

h.创建，IPsec profile分配和IKEv2 profile先Transport Set前创建。

```
!
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**。将接口引用**IP unnumbered address**为并应**IPsec profile**用。

该命**ip nhrp redirect**令在虚拟模板上配置，以通知辐条与其他辐条建立直接连接以到达其网络。

```
!
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
!
```

步骤 2：辐条A配置

a.定义IKEv2策略和配置文件。

b.配置并keyring输入用于Pre-Shared Key对辐射点进行身份验证的。

```
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.在中心路由器上启用AAA服务，然后定义一个名为的网络授权列表，**FlexAuth**该列表从本地设备配置指定策略。接下来，配置模式配置策略以将IP地址和路由推送到FlexVPN分支。

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

d.定义一个命名并允许网络10.20.2.0/24的标准IP访问列**FlexTraffic**。此ACL定义此分支共享的网络以通过隧道。

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

访问列表在 **IKEv2 Authorization Policy.**

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

e.创建，IKEv2 profile分配和keyringAAA授权组。

```
!
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.创建并Transport Set定义用于保护数据的加密和散列算法。

g.创建IPsec配置文件，分配之前创建的IKEv2配置文件和传输集。

```
!
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.配置隧道接口和虚拟**Virtual-Template1**模板。指定为支持而创建的**NHRP shortcuts**dVTI。另外，tunnel0上的未编号地址也设置为virtual-template。

命令**ip nhrp shortcut**在分支上配置，使它们能够根据来自集线器的NHRP重定向消息动态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
!
```

步骤 3：分支B配置

a.定义IKEv2策略和配置文件。

b.配置并keyring输入用于Pre-Shared Key对辐射点进行身份验证的。

```
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.在中心路由器上启用AAA服务，然后定义一个名为的网络授权列表，该列表从本地设备配置指定策略，然后配置模式配置策略以将IP地址和路由推送到FlexVPN分支**FlexAuth**。

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

d.定义命名并允许网络**FlexTraffic**10.30.3.0/24. 的标准IP访问列表此ACL定义此分支共享的网络，以便通过隧道。

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

访问列表在中引用 IKEv2 Authorization Policy.

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

e.创建，IKEv2 profile分配和keyringAAA授权组。

```
!
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.创建并Transport Set定义用于保护数据的加密和散列算法。

g.创建、IPsec profile分配和IKEv2 profile先Transport Set前创建。

```
!
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**定为支持而创建的NHRP shortcutsdVTI。另外，tunnel0上的未编号地址也设置为virtual-template。

命令**ip nhrp shortcut**在分支上配置，使它们能够根据来自集线器的NHRP重定向消息动态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
!
```

验证

使用show ip interface brief命令查看隧道、虚拟模板和虚拟访问状态。现在，它是分支到分支的直接连接：

- 在辐射点上，虚拟模板处于正常up/down状态。为处于up/up状态的连接创建虚拟访问。

```
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命令确认每台设备之间均已建立安全连接。
- 使用show crypto ipsec sa命令确认流量已加密并通过隧道，方法是验证封装和封装计数器是否正在递增。
- 使用show ip nhrp命令验证分支之间流量的重定向。

<#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命令验证路由是否已推送到分支：

- 这两个路由与Virtual-Access1接口相关联，是新的，并与NHRP快捷方式相关联。
- %字符表示下一跳覆盖。

<#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命令验证与通告网络的连接。

```
<#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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。使用以下命令调试隧道协商过程：

```
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调试有助于排除分支到分支连接的故障。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。