Configuration et vérification de la solution FlexVPN

Table des matières

Introduction

Ce document décrit l'environnement de réseau privé virtuel Flex, présente ses fonctionnalités et explique comment configurer chaque topologie FlexVPN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS et Cisco IOS XE
- IKE (Internet Key Exchange) version 2
- Sécurité du protocole Internet (IPSec)
- FlexVPN

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS XE Amsterdam-17.3.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

FlexVPN est une solution VPN polyvalente et complète fournie par Cisco, conçue pour offrir une structure unifiée pour différents types de connexions VPN. Basé sur le protocole IKEv2 (Internet Key Exchange version 2), FlexVPN est conçu pour simplifier la configuration, la gestion et le déploiement du VPN, en exploitant un ensemble cohérent d'outils. Les mêmes commandes et étapes de configuration s'appliquent à différents types de VPN (site à site, accès à distance, etc.). Cette cohérence permet de réduire les erreurs et rend le processus de déploiement plus intuitif.

IKEV2 CONTRE IKEV1

FlexVPN exploite IKEv2, qui prend en charge des algorithmes cryptographiques modernes tels que AES (Advanced Encryption Standard) et SHA-256 (Secure Hash Algorithm). Ces algorithmes assurent un chiffrement et une intégrité des données renforcés, protégeant les données transmises sur le VPN contre toute interception ou altération.

IKEv2 offre davantage de méthodes d'authentification qu'IKEv1. Outre la clé prépartagée (PSK) et les types d'authentification basée sur certificat et hybride, IKEv2 permet au répondeur d'utiliser le protocole EAP (Extensible Authentication Protocol) pour l'authentification client.

Dans FlexVPN, EAP est utilisé pour l'authentification du client, le routeur agit comme un relais, transmettant des messages EAP entre le client et le serveur EAP principal, généralement un serveur RADIUS. FlexVPN prend en charge diverses méthodes EAP, notamment EAP-TLS, EAP-PEAP, EAP-PSK, etc., pour sécuriser le processus d'authentification.

Le tableau présente les différences entre les fonctions IKEv1 et IKEv2 :

	IKEv2	IKEv1
Messages d'établissement de protocole	4 message	6 message

Prise en charge EAP	Oui (2 messages supplémentaires)	Non
Négociation des associations de sécurité	2 messages supplémentaires	3 messages supplémentaires
Exécuter sur UDP 500/4500	Oui	Oui
NAT Traversal (NAT-T)	Oui	Oui
Retransmissions et fonctions d’accusé de réception	Oui	Oui
Protection des identités, mécanisme de protection contre les attaques DoS et PFS (Perfect Forward Secrecy)	Oui	Oui
Prise en charge du chiffrement nouvelle génération	Oui	Non

Évolutivité

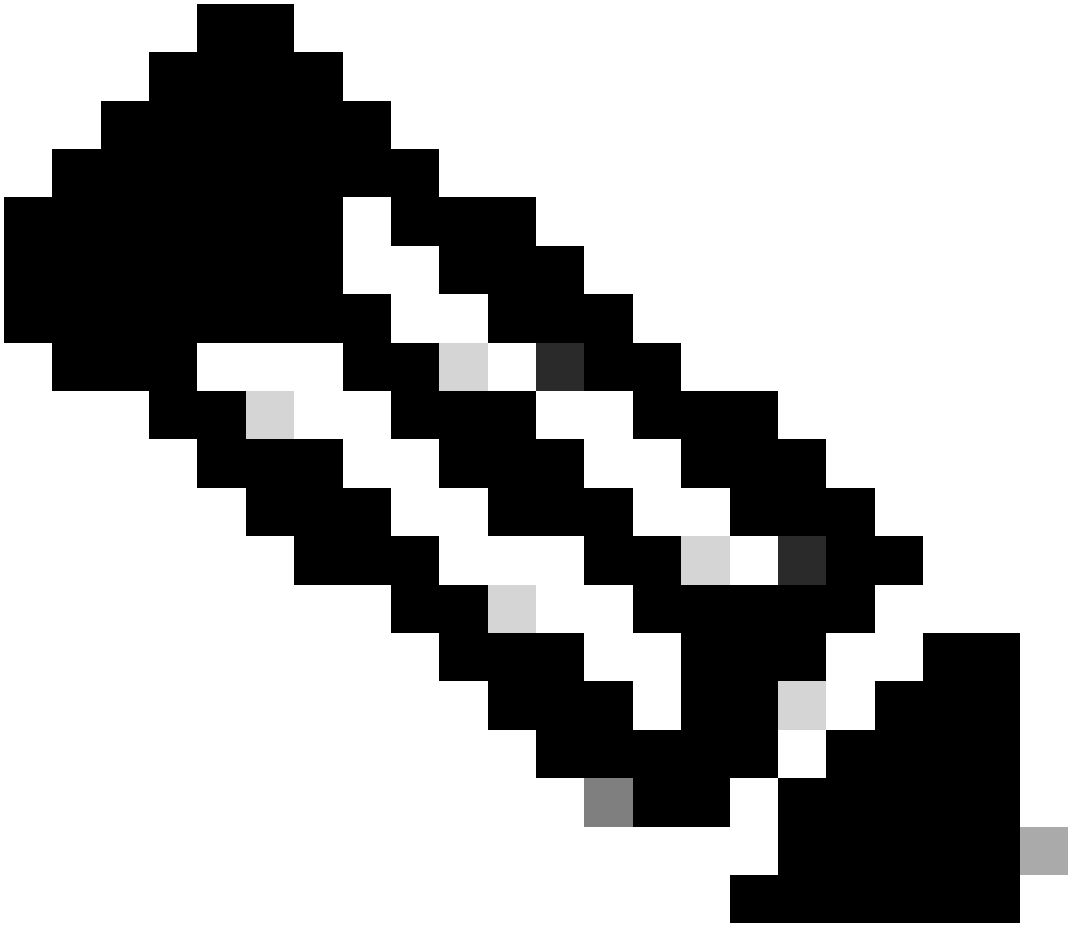
FlexVPN peut facilement s'étendre des petits bureaux aux grands réseaux d'entreprise. C'est donc un choix idéal pour les entreprises comptant un nombre important d'utilisateurs distants qui ont besoin d'un accès réseau sécurisé et fiable.

Fonctionnalités principales

- Configuration dynamique et tunnels à la demande :
  - Une connexion FlexVPN est initiée, le système génère une interface d'accès virtuelle basée sur un modèle préconfiguré. Cette interface agit comme point d'extrémité du tunnel pendant toute la durée de la connexion. Lorsque le tunnel n'est plus nécessaire, l'interface d'accès virtuelle est désactivée, libérant ainsi des ressources système.

- Flexibilité de déploiement :
  - Modèle Hub-and-Spoke : Un concentrateur central se connecte à plusieurs filiales. FlexVPN simplifie la configuration de ces connexions avec une structure unique, ce qui en fait la solution idéale pour les grands réseaux.
  - Topologies à maillage global et à maillage partiel : Tous les sites peuvent communiquer directement sans passer par un concentrateur central, ce qui réduit les délais et améliore les performances.

- Haute disponibilité et redondance :
  - Concentrateurs redondants : Prend en charge plusieurs concentrateurs pour la sauvegarde. Si un concentrateur tombe en panne, les filiales peuvent se connecter à un autre concentrateur, assurant ainsi une connectivité continue.
  - Équilibrage de charge : Cela répartit les connexions VPN sur plusieurs périphériques afin d'éviter qu'un seul périphérique ne soit surchargé, ce qui est essentiel pour maintenir les performances dans les grands déploiements.



Remarque : Le guide suivant fournit plus d'informations sur la configuration de l'équilibrage de charge pour la connexion des concentrateurs.

Configuration de l'équilibreur de charge IKEv2

- Authentification et autorisation évolutives :
  - Intégration AAA : Fonctionne avec des serveurs AAA tels que Cisco ISE ou RADIUS pour une gestion centralisée des informations d'identification et des politiques des utilisateurs, essentielle pour une utilisation à grande échelle.
  - PKI et certificats : Prend en charge l'infrastructure à clé publique (PKI) et les certificats numériques pour une authentification sécurisée, plus évolutive que l'utilisation d'une clé prépartagée, en particulier dans les environnements de grande taille.

Routage

La fonctionnalité de routage de FlexVPN est conçue pour améliorer l'évolutivité et gérer efficacement plusieurs connexions VPN et permettre un moyen dynamique d'acheminer le trafic

vers chacune d'elles. Les composants et mécanismes clés suivants qui rendent le routage FlexVPN efficace :

- Interface de modèle virtuel : Il s'agit d'un modèle de configuration qui inclut tous les paramètres nécessaires pour une connexion VPN, tels que l'attribution d'adresse IP, la source du tunnel et les paramètres IPsec. Dans cette interface, la commande est configurée pour emprunter une adresse IP,`ip unnumbered`généralement à partir d'un bouclage au lieu de configurer une adresse IP spécifique comme source du tunnel. Cela permet au même modèle d'être utilisé par chaque rayon, permettant à chaque rayon d'utiliser sa propre adresse IP source.

- Interface d'accès virtuel : Il s'agit d'interfaces créées dynamiquement qui héritent leurs paramètres de l'interface de modèle virtuelle. Chaque fois qu'une nouvelle connexion VPN est établie, une nouvelle interface d'accès virtuelle est créée sur la base du modèle virtuel. Cela signifie que chaque session VPN a sa propre interface unique, ce qui simplifie la gestion et l'évolutivité.

- Protocoles de routage dynamique: Il fonctionne avec des protocoles de routage tels que OSPF, EIGRP et BGP sur des tunnels VPN. Les informations de routage sont ainsi mises à jour automatiquement, ce qui est important pour les grands réseaux dynamiques.

- IKEv2 annonce les routes en permettant au serveur FlexVPN de transmettre les attributs réseau au client, qui installe ces routes sur l'interface du tunnel. Le client communique également ses propres réseaux au serveur lors de l'échange du mode de configuration, ce qui active les mises à jour de route aux deux extrémités.

- Le protocole NHRP (Next Hop Resolution Protocol) est un protocole de résolution d'adresse dynamique utilisé dans les topologies Hub and Spoke pour mapper des adresses IP publiques à des points d'extrémité VPN privés. Il permet aux satellites de découvrir d'autres IP de satellites pour une communication directe.

Politique d'autorisation

Une stratégie d'autorisation IKEv2 pour FlexVPN peut être configurée pour contrôler divers aspects de la connexion VPN. Une stratégie d'autorisation IKEv2 définit la stratégie d'autorisation locale et contient des attributs locaux et/ou distants :

- Les attributs locaux, tels que le routage et le transfert VPN (VRF) et la stratégie QOS, sont appliqués localement.
- Les attributs distants, tels que les routes, sont transmis à l'homologue via le mode de configuration.
- Utilisez la commande crypto ikev2 authorization policy pour définir la stratégie locale.
- La stratégie d'autorisation IKEv2 est référencée à partir du profil IKEv2 via la commande AAA authorization.

Ce tableau présente les paramètres clés pouvant être configurés dans le cadre de la stratégie d'autorisation IKEv2.

Paramètre	Description

AAA	Intégration aux serveurs AAA pour valider les informations d'identification des utilisateurs, autoriser l'accès et créer un compte pour l'utilisation. La stratégie peut spécifier si la validation est effectuée localement sur le routeur ou à distance, par exemple via un serveur RADIUS.
Configuration du client	Transmet les paramètres de configuration au client, tels que les valeurs de délai d'inactivité, les messages de veille, l'affectation de serveurs DNS et WINS, etc.
Configuration spécifique au client	Permet différentes configurations pour différents clients en fonction de leur identité ou de leur appartenance à un groupe.
Ensemble de routages	Cette configuration permet à certains trafics de passer par le tunnel VPN. Ceci effectue l'injection de route qui est poussée vers le client VPN lors d'une connexion réussie.

FlexVPN et autres technologies

FlexVPN offre une gamme d'avantages qui en font un choix attrayant pour les environnements réseau modernes. En fournissant une structure unifiée, FlexVPN simplifie la configuration et la gestion, améliore la sécurité, prend en charge l'évolutivité, assure l'interopérabilité et réduit la complexité.

	Crypto-carte	Réseaux RPV multipoint dynamique (DMVPN)	FlexVPN
Routage dynamique	Non	Oui	Oui
Connexion directe satellite-satellite dynamique	Non	Oui	Oui
VPN d’accès à distance	Oui	Non	Oui
Push de configuration	Non	Non	Oui
Configuration homologue-homologue	Non	Non	Oui
Qualité de service pair à pair	Non	Oui	Oui
Intégration du serveur AAA	Non	Non	Oui

Diagramme du réseau

FlexVPN permet la création de tunnels entre les périphériques, établissant la communication entre le concentrateur et les satellites. Il permet également la création de tunnels pour la communication directe entre les rayons et la connexion pour les utilisateurs VPN d'accès à distance, comme illustré dans le schéma.

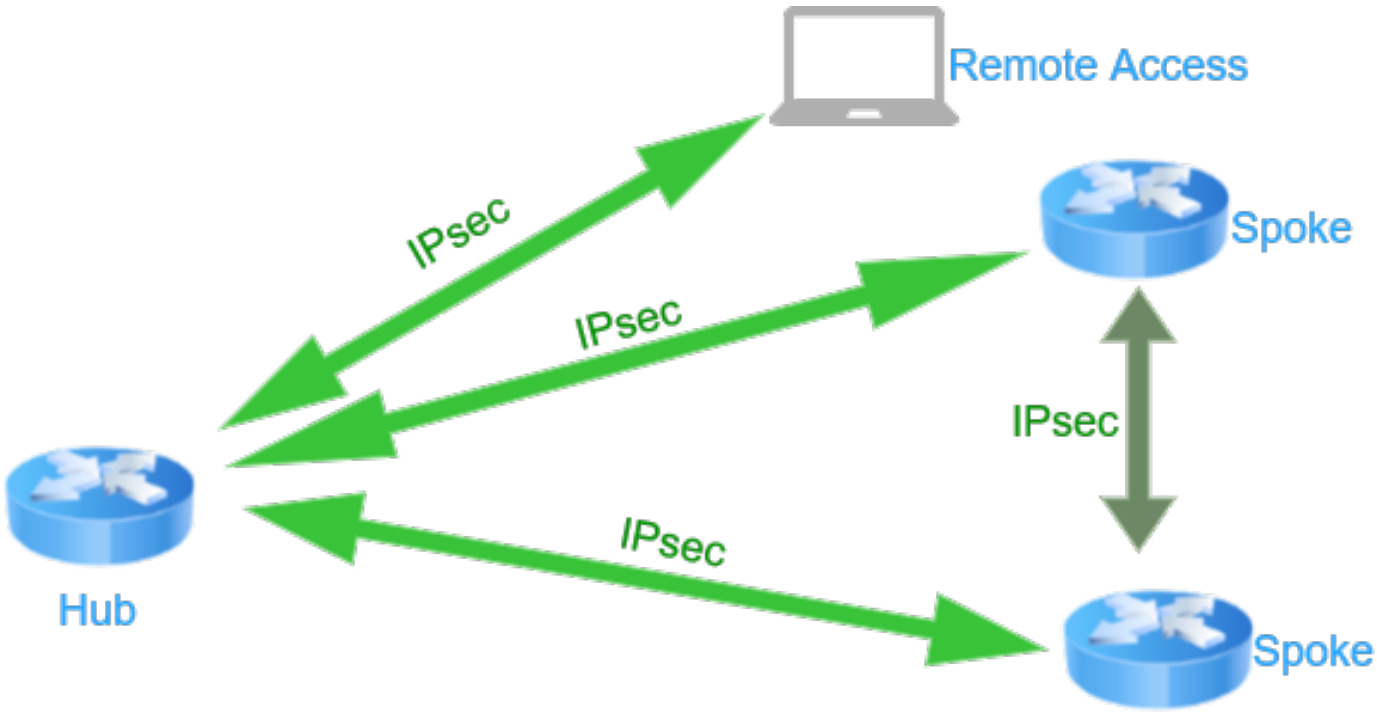
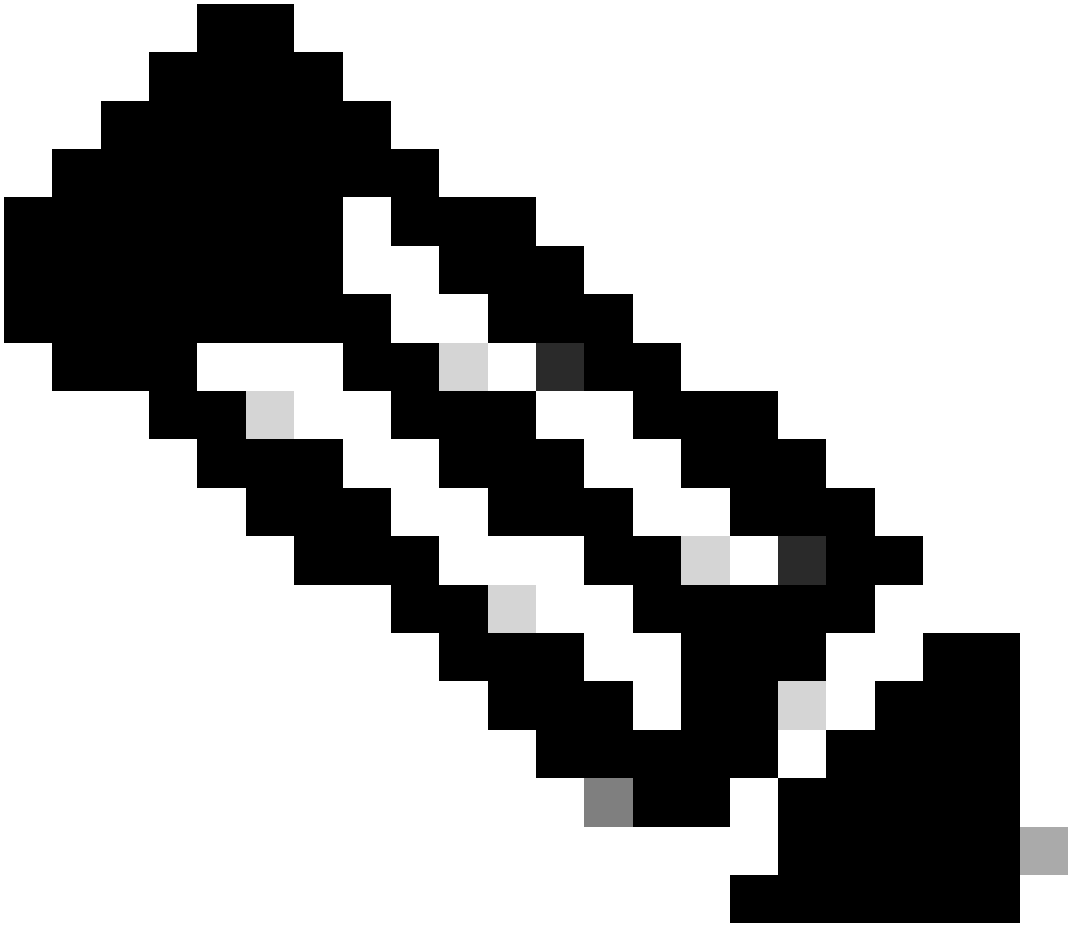


Schéma FlexVPN



Remarque : La configuration du VPN d'accès à distance n'est pas traitée dans ce guide. Pour plus d'informations sur sa configuration, reportez-vous au guide :

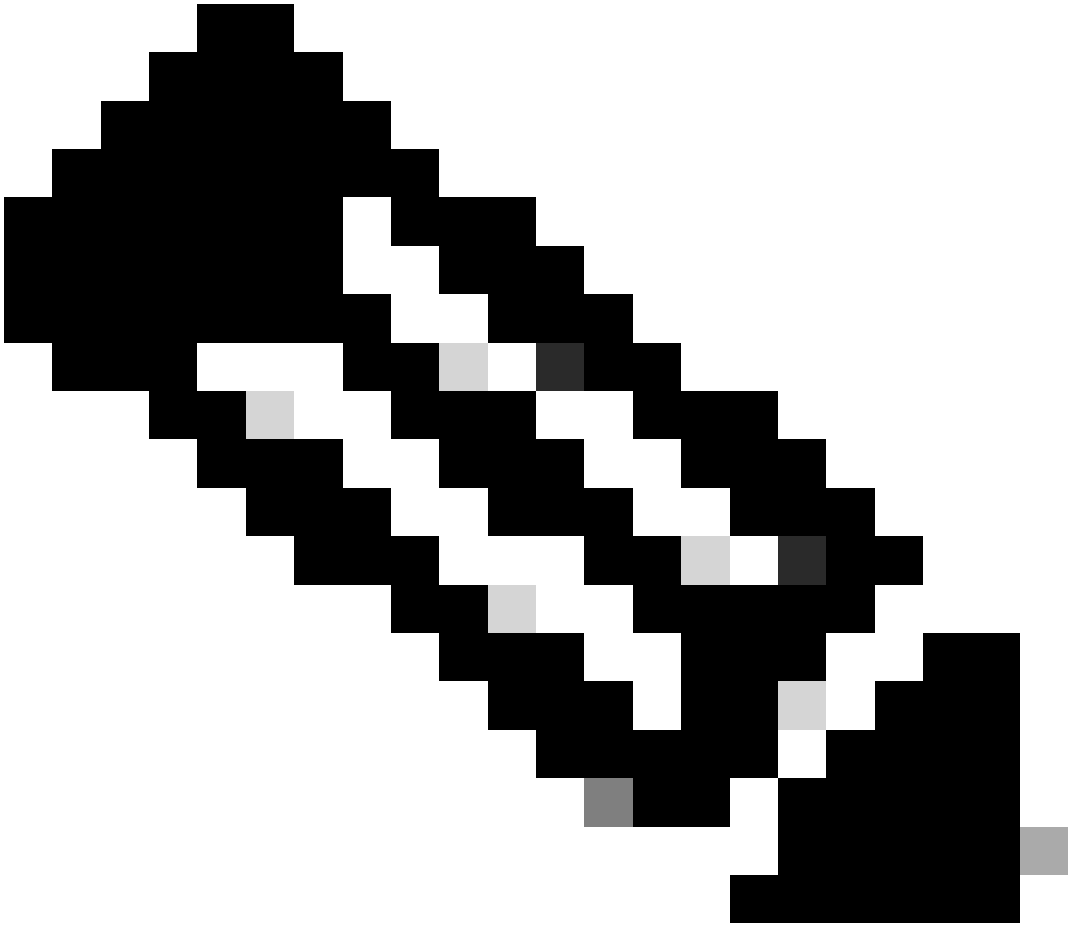
Configuration de la tête de réseau FlexVPN pour l'accès à distance IKEv2 Secure Client (AnyConnect) à l'aide de la base de données utilisateur locale

Configurer

FlexVPN se caractérise par la simplicité de sa configuration. Cette simplicité est évidente dans les blocs de configuration cohérents utilisés pour différents types de VPN. FlexVPN fournit des blocs de configuration simples qui sont généralement applicables, avec des configurations facultatives ou des étapes supplémentaires disponibles en fonction des caractéristiques ou exigences spécifiques de la topologie :

- Proposition IKEv2 : Définit les algorithmes utilisés dans la négociation de l'association de sécurité IKEv2. Une fois créée, joignez cette proposition à une stratégie IKEv2 pour qu'elle soit sélectionnée lors de la négociation.

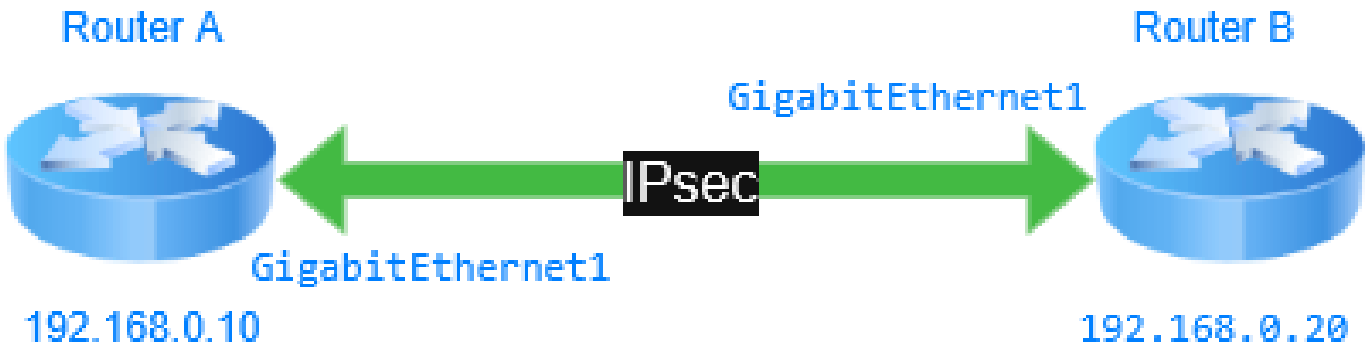
- Stratégie IKEv2 : Relie la proposition à une instance VRF (Virtual Routing and Forwarding) ou à une adresse IP locale. Lien de stratégie vers la proposition IKEv2.
- Porte-clés IKEv2 : Spécifie les clés prépartagées (PSK), qui peuvent être asymétriques si elles sont utilisées pour l'authentification homologue.
- Trustpoint (facultatif) : Configure les attributs d'identité et d'autorité de certification (CA) pour l'authentification homologue lors de l'utilisation de l'infrastructure à clé publique (PKI) comme méthode d'authentification.
- Intégration AAA (facultatif) : FlexVPN intègre des serveurs AAA, tels que des serveurs Cisco ISE (Identity Services Engine) ou RADIUS comme méthode d'authentification.
- Profil IKEv2 : Stocke les paramètres non négociables de l'association de sécurité IKE, tels que l'adresse de l'homologue VPN et les méthodes d'authentification. Il n'existe pas de profil IKEv2 par défaut. Vous devez donc en configurer un et l'associer à un profil IPsec sur l'initiateur. Si l'authentification PSK est utilisée, le profil IKEv2 fait référence au porte-clés IKEv2. Si l'authentification PKI ou la méthode d'authentification AAA est utilisée, elle fait référence ici.
- Jeu de transformation IPsec : Spécifie une combinaison d'algorithmes acceptable pour la SA IPsec.
- Profil IPsec : Regroupe les paramètres FlexVPN dans un profil unique qui peut être appliqué à une interface. Ce profil fait référence au jeu de transformation IPsec et au profil IKEv2.



Remarque : Les exemples de configuration utilisent des clés pré-partagées pour fournir une démonstration simple de la configuration et de la simplicité de FlexVPN. Bien que les clés pré-partagées puissent être utilisées pour un déploiement facile et des topologies de petite taille, les méthodes AAA ou PKI sont plus adaptées aux topologies de grande taille.

Configuration FlexVPN site à site

La topologie FlexVPN site à site est conçue pour les connexions VPN directes entre deux sites. Chaque site est équipé d'une interface de tunnel qui établit un canal sécurisé sur lequel le trafic peut circuler. La configuration explique comment établir une connexion VPN directe entre deux sites, comme le montre le schéma.



Diagramme_site_à_site

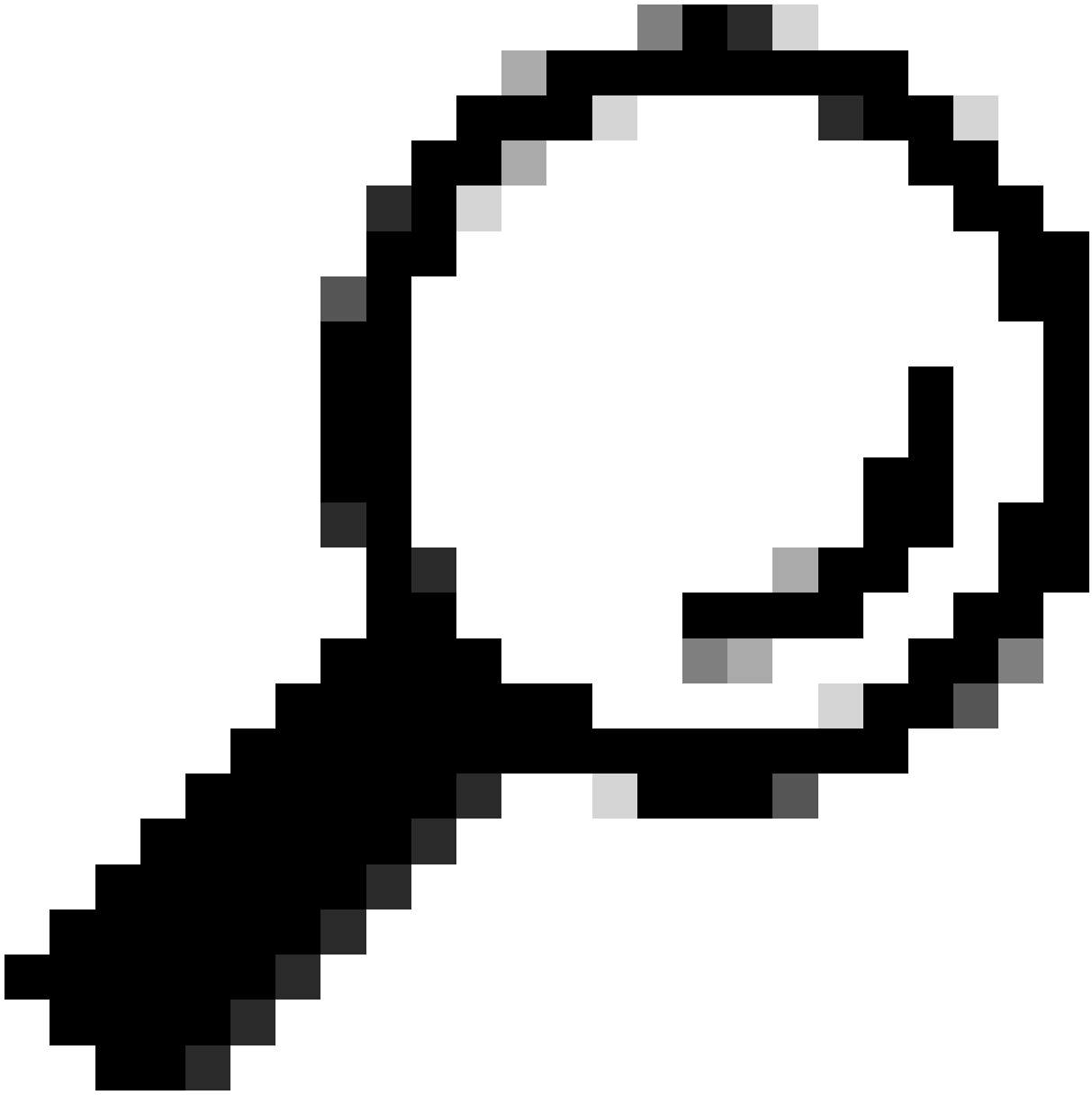
Étape 1 : Configuration du routeur A

a. Définir une proposition et une politique IKEv2.

b. Configurez un trousseau de clés et entrez un Pre-Shared Key qui est utilisé pour authentifier l'homologue.

c. Créez un IKEv2 profile et attribuez le 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
!
```



Conseil : Cette **IKEv2 Smart Defaults** fonctionnalité réduit la configurationFlexVPNen couvrant la plupart des cas d'utilisation. Vous pouvez personnaliser **IKEv2 Smart Defaults** pour des cas d'utilisation spécifiques, bien que Cisco ne recommande pas cette pratique.

d. Créez un Transport Set et définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

e. Créez un **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. Configurez l'interface du tunnel.

```
!
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. Configurez le routage dynamique pour annoncer l'interface du tunnel. Ensuite, il peut annoncer les autres réseaux qui doivent passer par le tunnel.

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

Étape 2 : Configuration du routeur B

a. Définir une proposition et une politique IKEv2.

b. Configurez un keyring et entrez un Pre-Shared Key qui est utilisé pour authentifier l'homologue.

c. Créez un IKEv2 profile et attribuez le 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. Créez un Transport Set et définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

e. Créez un profil IKEv2 IPsec profile et attribuez-lui le jeu de transformation et le profil IKEv2 précédemment créés.

```
!
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. Configurez le 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. Configurez le routage dynamique pour annoncer l'interface du tunnel. Ensuite, il peut annoncer les autres réseaux qui doivent passer par le tunnel.

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

Vérifier

- Utilisez la commande show ip interface brief pour examiner l'état de l'interface du tunnel et vérifier que le tunnel est dans un état up/up.

<#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. Utilisez la commande show crypto ikev2 sa pour confirmer que la connexion sécurisée entre les routeurs est établie.

<#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
```

- Utilisez la commande show crypto ipsec sa pour confirmer que le trafic est chiffré et passe par le tunnel en vérifiant que les compteurs encaps et decaps sont incrémentés.

<#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
```

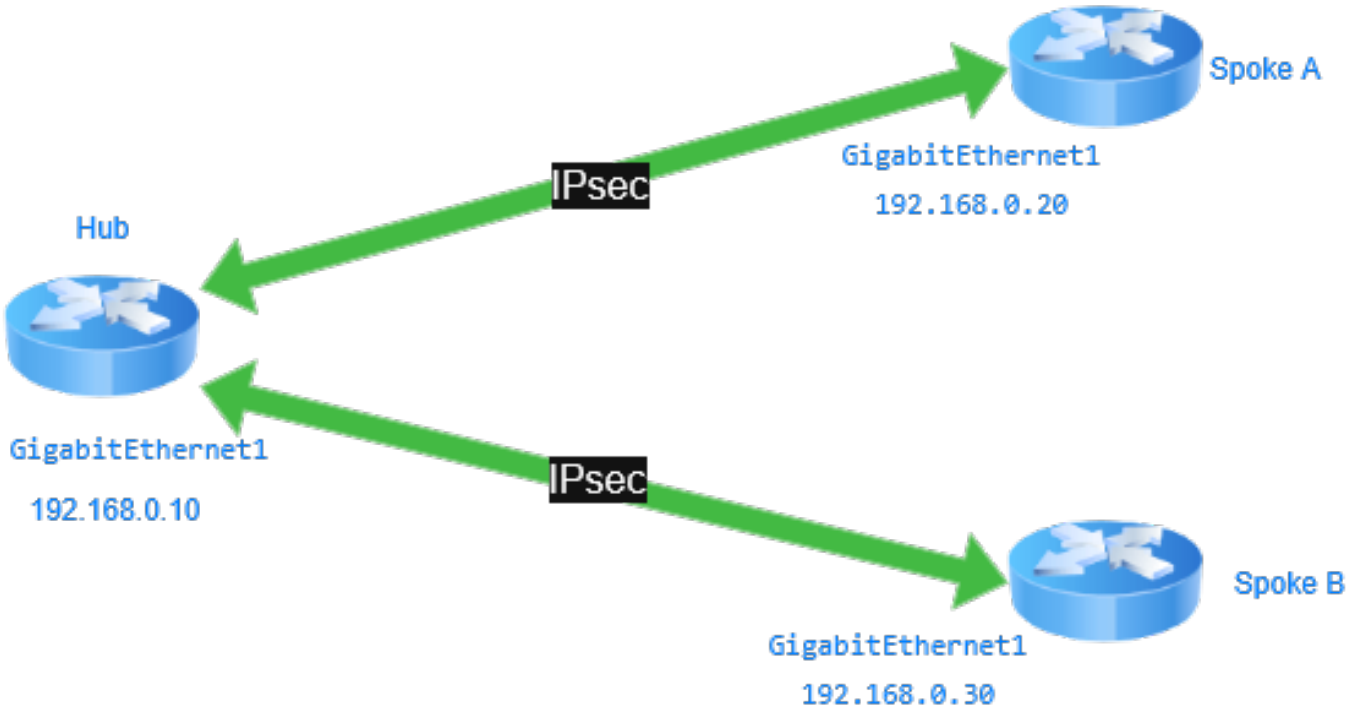
```
sa timing: remaining key lifetime (k/sec): (4607991/3137)

         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- Utilisez la commande show ip eigrp neighbors pour confirmer que la contiguïté EIGRP est établie avec l'autre site.

```
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
```

FlexVPN Hub-and-Spoke

Dans la topologie en étoile, plusieurs routeurs en étoile se connectent à un routeur central. Cette configuration est optimale pour les scénarios dans lesquels les rayons communiquent principalement avec le concentrateur. Dans FlexVPN, les tunnels dynamiques peuvent être configurés pour améliorer l'efficacité des communications. Le concentrateur utilise le routage IKEv2 pour distribuer les routes vers les routeurs en étoile, garantissant ainsi une connectivité transparente. Comme il est référencé dans le schéma, la configuration explique la connexion VPN entre un concentrateur et un satellite et comment le concentrateur est configuré pour établir une connexion dynamique avec plusieurs satellites et il est capable d'ajouter davantage de satellites.



Diagramme_Hub_and_Spoke

Étape 1 : Configuration du concentrateur

a. Définir une proposition et une politique IKEv2.

b. Configurez un keyring et entrez un Pre-Shared Key qui est utilisé pour authentifier les rayons.

```
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. Activez les services AAA sur le routeur concentrateur, puis définissez une liste d'autorisations réseau nomméeFlexAuthqui spécifie les stratégies à partir de la configuration du périphérique local.

```
!
aaa new-model
```

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

d. Définissez unIP address poolnomFlexPool, qui contient les adresses 10.1.1.2 à 10.1.1.254. Ce pool est utilisé pour attribuer automatiquement une adresse IP à l'interface de tunnel des rayons.

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

e. Définissez une liste de contrôle d'accès IP standard nomméeFlexTrafficet autorisant le réseau 10.10.1.0/24. Cette liste de contrôle d'accès définit les réseaux qui sont poussés vers les rayons FlexVPN pour les atteindre via le tunnel.

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

La liste d'accès et le pool d'adresses IP sont référencés dans le **IKEv2 Authorization Policy**.

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

f. Créez un IKEv2 profilegroupe, attribuez-lui le groupe d'autorisations keyring et AAA.

```
!
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. Créez un Transport Setfichier, définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

h. Créez un IPsec profile, affectez le IKEv2 profile et le Transport Set précédemment créé.

```
!
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. Configurez le **virtual-template 1** as **type tunnel**. Référencez l'interface en tant queIP unnumbered addresset appliquez la **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
!
```

Étape 2 : Configuration du rayon

a. Définir une proposition et une politique IKEv2.

b. Configurez un porte-clés et entrez une clé prépartagée utilisée pour l'authentification auprès du concentrateur.

```
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. Activez les services AAA sur le routeur concentrateur, puis définissez une liste d'autorisations réseau nommée **FlexAuth** qui spécifie les stratégies de la configuration du périphérique local. Ensuite, configurez la stratégie de configuration de mode pour pousser l'adresse IP et les routes vers les rayons FlexVPN.

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

d. Définissez une liste de contrôle d’accès IP standard nommée **FlexTraffic** et autorisant le réseau 10.20.2.0/24. Cette liste de contrôle d’accès définit les réseaux partagés par ce rayon à traverser le tunnel.

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

La liste d'accès est attribuée dans le **IKEv2 Authorization Policy**.

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

e. Créez un IKEv2 profilegroupe d'autorisation, attribuez-lui le groupe d'autorisation keyring et AAA.

```
!
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. Créez un jeu d'objets à transporter et définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

g. Créez un profil IPsec, attribuez le profil IKEv2 et le jeu d'objets à transporter précédemment créés.

```
!
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. Configurez l'interface du tunnel avec la propriété de l'adresse IP négociée, qui est obtenue à partir du pool qu'elle a configuré sur le concentrateur.

```
!
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
!
```

Vérifier

Utilisez la commande show ip interface brief pour examiner l'état du tunnel, du modèle virtuel et de l'accès virtuel :

- Sur le concentrateur, le modèle virtuel a un état up/down qui est normal. Un accès virtuel est créé pour chaque satellite qui établit une connexion avec le concentrateur et affiche un état up/up.
- Sur le satellite, l'interface du tunnel a reçu une adresse IP et affiche un état up/up.

<#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
```

- Utilisez la commande show crypto ikev2 sa pour confirmer que la connexion sécurisée entre le concentrateur et le satellite est établie.

<#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
```

- Utilisez la commande show crypto ipsec sa pour confirmer que le trafic est chiffré et passe par le tunnel en vérifiant que les compteurs encaps et decaps sont incrémentés.

<#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:
```

- Utilisez la commande show ip route pour vérifier que les routes ont été poussées vers les rayons :
  - La route pour 10.1.1.1/32 a été diffusée via les données utiles de configuration IKEv2 en raison de l'instruction d'interface de la route set dans la configuration du concentrateur.
  - La route pour 10.10.1.0/24 a été diffusée via des données utiles de configuration IKEv2 en raison de l'instruction route set access-list FlexTraffic dans la configuration du concentrateur.

<#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
```

- Utilisez la commande ping pour vérifier la connectivité aux réseaux annoncés.

<#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#
```

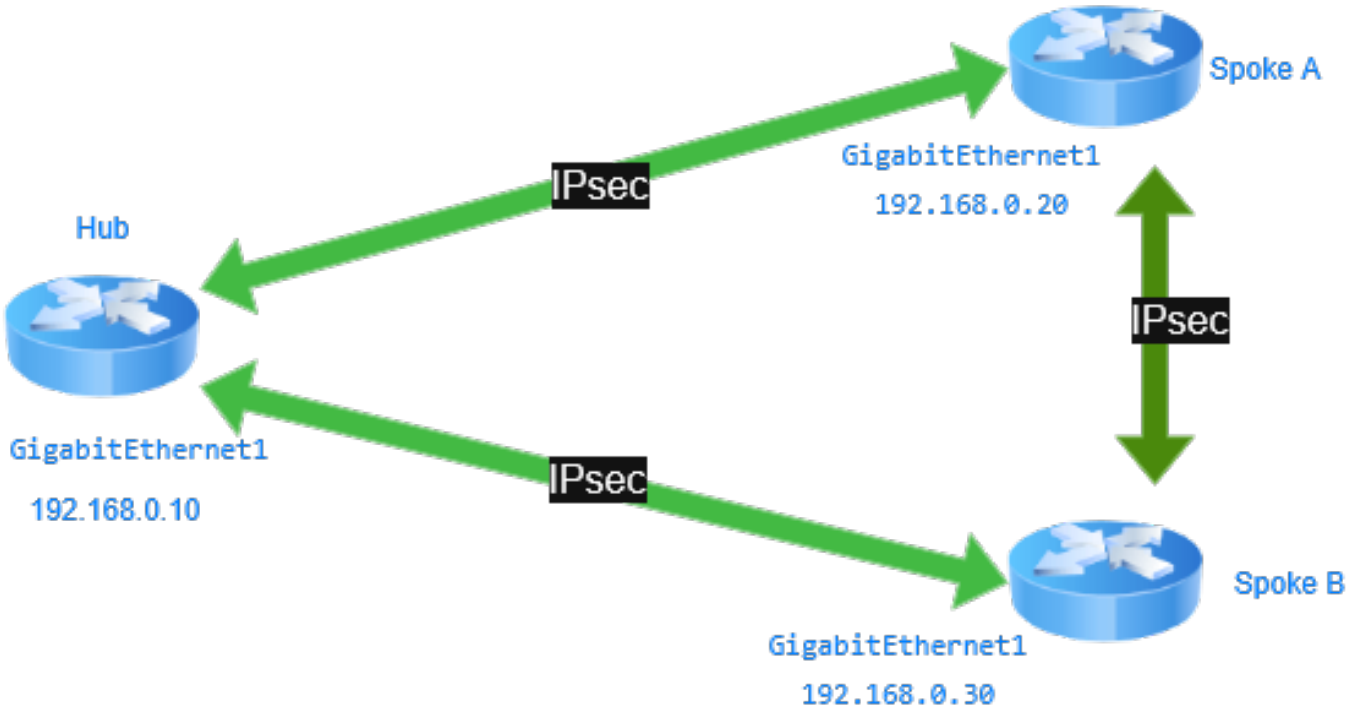
```
ping 10.10.1.10
```

```
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
```

FlexVPN satellite à satellite

FlexVPN dans une topologie Hub and Spoke avec connectivité Spoke to Spoke permet une communication VPN dynamique, évolutive et sécurisée. Le concentrateur agit comme un point de contrôle centralisé où NHRP permet aux rayons d'interroger le concentrateur pour d'autres adresses IP de rayons, permettant des tunnels IPsec rayon à rayon directs pour une communication efficace et une latence réduite.

Sur le concentrateur, la **ip nhrp redirect** commande est utilisée pour avertir les rayons qu'une communication directe entre les rayons est possible, optimisant ainsi le flux de trafic en contournant le concentrateur pour le trafic du plan de données. Sur les rayons, la **ip nhrp shortcut** commande leur permet d'établir dynamiquement des tunnels directs avec d'autres rayons après avoir reçu la redirection du concentrateur. Le schéma fait référence au trafic entre le concentrateur et le satellite, et à la communication satellite à satellite.



Diagramme_Spoke_to_Spoke

Étape 1 : Configuration du concentrateur

a. Définition des stratégies et des profils IKEv2

b. Configurez un keyring et entrez un Pre-Shared Key qui est utilisé pour authentifier les rayons.

```
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. Activez les services AAA sur le routeur concentrateur, puis définissez une liste d'autorisations réseau nommée qui spécifie les stratégies à partir de la configuration du périphérique local, **FlexAuth** puis configurez la stratégie de configuration du mode pour transmettre l'adresse IP et les routes vers les rayons FlexVPN.

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

d. Définissez unIP address poolnom **FlexPool**, qui contient les adresses 10.1.1.2 à 10.1.1.254. Ce pool est utilisé pour attribuer automatiquement une adresse IP à l'interface de tunnel des rayons.

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

e. Définissez une liste de contrôle d'accès IP standard nomméeFlexTrafficet autorisant le réseau 10.0.0.0/8. Cette liste de contrôle d'accès définit les réseaux qui sont envoyés aux rayons FlexVPN, y compris les réseaux pour les autres rayons connectés au concentrateur, afin que les rayons sachent que ces réseaux sont d'abord atteints via le concentrateur.

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

La liste d'accès et IP address pool sont attribuées dans la **IKEv2 Authorization Policy**.

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

f. Créez un IKEv2 profilegroupe, attribuez-lui les autorisations keyring et AAA.

```
!
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. Créez un Transport Set et définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

h. Créez un IPsec profilefichier, attribuez le fichier IKEv2 profile et le fichier Transport Set précédemment créé.

```
!
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. Configurez le **virtual-template 1** as **type tunnel**. Référencez l'interface en tant que **IP unnumbered address** et appliquez la **IPsec profile**.

La **ip nhrp redirect** commande est configurée sur le modèle virtuel pour informer les rayons d'établir une connexion directe avec d'autres rayons pour atteindre leurs réseaux.

```
!
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
!
```

Étape 2 : Configuration Spoke A

a. Définition des stratégies et des profils IKEv2

b. Configurez un keyring et entrez un Pre-Shared Key qui est utilisé pour authentifier les rayons.

```
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. Activez les services AAA sur le routeur concentrateur, puis définissez une liste d'autorisations réseau nommée **FlexAuth** qui spécifie les stratégies de la configuration du périphérique local. Ensuite, configurez la stratégie de configuration de mode pour pousser l'adresse IP et les routes vers les rayons FlexVPN.

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

d. Définissez une liste de contrôle d’accès IP standard nommée **FlexTraffic** et autorisant le réseau 10.20.2.0/24. Cette liste de contrôle d’accès définit les réseaux partagés par ce rayon à traverser le tunnel.

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

La liste d'accès est attribuée dans le **IKEv2 Authorization Policy.**

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

e. Créez un IKEv2 profilegroupe d'autorisation, attribuez-lui le groupe d'autorisation keyring et AAA.

```
!
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. Créez un Transport Set et définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

g. Créez un profil IPsec, attribuez le profil IKEv2 et le jeu d'objets à transporter précédemment créés.

```
!
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. Configurez l'interface de tunnel et le modèle virtuel. Spécifiez **Virtual-Template1** pour les dVTI qui sont créés pour prendre en charge **NHRP shortcuts**. En outre, définissezTunnel0en tant qu'adresse non numérotée sur levirtual-template.

La **ip nhrp shortcut** commande est configurée sur les rayons pour leur permettre d'établir dynamiquement des tunnels directs vers d'autres rayons en fonction des messages de redirection NHRP du concentrateur.

```
!
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
!
```

Étape 3 : Configuration satellite B

a. Définition des stratégies et des profils IKEv2

b. Configurez un keyring et entrez un Pre-Shared Key qui est utilisé pour authentifier les rayons.

```
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. Activez les services AAA sur le routeur concentrateur, puis définissez une liste d'autorisations réseau nommée qui spécifie les stratégies à partir de la configuration du périphérique local, **FlexAuth** puis configurez la stratégie de configuration du mode pour transmettre l'adresse IP et les routes vers les rayons FlexVPN.

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

d. Définissez une liste de contrôle d’accès IP standard nommée **FlexTraffic** et autorisant le réseau 10.30.3.0/24. Cette liste de contrôle d’accès définit les réseaux partagés par ce rayon à traverser le tunnel.

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

La liste d'accès est référencée dans la IKEv2 Authorization Policy.

```
!
```

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

e. Créez un IKEv2 profilegroupe d'autorisation, attribuez-lui le groupe d'autorisation keyring et AAA.

```
!
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. Créez un Transport Set et définissez les algorithmes de chiffrement et de hachage utilisés pour protéger les données.

g. Créez un IPsec profilefichier, attribuez le fichier IKEv2 profile et le fichier Transport Set précédemment créé.

```
!
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. Configurez les tunnel interface et virtual template. Spécifiez **Virtual-Template1** pour les dVTI créés pour prendre en charge NHRP shortcuts. En outre, définissezTunnel0en tant qu'adresse non numérotée sur levirtual-template.

La **ip nhrp shortcut** commande est configurée sur les rayons pour leur permettre d'établir dynamiquement des tunnels directs vers d'autres rayons en fonction des messages de redirection NHRP du concentrateur.

```
!
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
!
```

Vérifier

Utilisez la commande show ip interface brief pour examiner l'état du tunnel, du modèle virtuel et de l'accès virtuel. Maintenant, il s'agit de la connexion directe de rayon à rayon :

- Sur les rayons, le modèle virtuel a un état up/down qui est normal. Un accès virtuel est créé pour la connexion en état up/up.

<#root>

```
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
```

- Utilisez la commande show crypto ikev2 sa pour confirmer que la connexion sécurisée entre chaque périphérique est établie.
- Utilisez la commande show crypto ipsec sa pour confirmer que le trafic est chiffré et passe par le tunnel en vérifiant que les compteurs encaps et decaps sont incrémentés.
- Utilisez la commande show ip nhrp pour vérifier la redirection du trafic entre les rayons.
  <#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
```

Utilisez la commande show ip route pour vérifier que les routes ont été poussées vers le rayon :

- Les deux routes associées à l'interface Virtual-Access1 sont nouvelles et associées aux raccourcis NHRP.
- Le caractère % indique un remplacement de tronçon suivant.

<#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
```

- Utilisez la commande ping pour vérifier la connectivité aux réseaux annoncés.

<#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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. Utilisez ces commandes pour déboguer le processus de négociation de tunnel :

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

Les débogages NHRP peuvent vous aider à dépanner les connexions satellite à satellite.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.