

FlexVPN a parlé dans la conception redondante de hub avec l'exemple de configuration de bloc de client de FlexVPN

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagrammes du réseau](#)

[Réseau de transport](#)

[Réseau de substitution](#)

[Configuration de base de rai et de hub](#)

[Réglage de configuration en étoile](#)

[Configuration en étoile - Bloc de configuration de client](#)

[Plaine configuration en étoile - Référence](#)

[Configuration du concentrateur](#)

[Adresses de rai](#)

[Adresse de recouvrement de hub](#)

[Acheminement](#)

[Utilisation de résumés de réseau](#)

[Tunnels de spoke-to-spoke](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un rai dans un réseau de FlexVPN avec l'utilisation du bloc de configuration de client de FlexVPN dans un scénario où les plusieurs concentrateurs sont disponibles.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- Protocoles de routage de Cisco

Composants utilisés

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

- Routeur de service intégré de gamme Cisco G2 (ISR)
- Version 15.2M de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Pour des raisons de redondance, un rai pourrait devoir se connecter aux plusieurs concentrateurs. La Redondance du côté de l'étoile permet le fonctionnement continu sans point de défaillance unique du côté concentrateur.

Les deux conceptions redondantes de hub de FlexVPN les plus communes qui utilisent la configuration en étoile sont :

- **Double approche de nuage**, où un rai a deux tunnels distincts actifs aux deux Concentrateurs à tout moment.
- **Approche de Basculement**, où un rai a un tunnel actif avec un hub à n'importe quel moment donné.

Les deux approches ont un seul ensemble d'avantages - et - des inconvénients.

Approche	Avantages	Inconvénients
Conjuguent le nuage	<ul style="list-style-type: none">• Une reprise plus rapide dans une panne, basée sur des temporisateurs de protocole de routage• Plus de possibilités pour distribuer le trafic parmi des Concentrateurs, puisque les connexions aux deux Concentrateurs sont en activité	<ul style="list-style-type: none">• Le rai met à jour la session aux deux Concentrateurs en même temps, qui consomme des ressources sur les deux Concentrateurs
Basculement	<ul style="list-style-type: none">• Configuration simple - établie dans FlexVPN• Ne compte pas sur le protocole de routage dans une panne	<ul style="list-style-type: none">• Un temps de rétablissement plus lent - basé sur Dead Peer Detection (DPD) ou (sur option) le Suivi d'objets• Tout le trafic est forcé pour voyager à un hub à la fois

Ce document décrit la deuxième approche.

Configurez

Note: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

[Diagrammes du réseau](#)

Ces diagrammes affichent les diagrammes de topologie de transport et de recouvrement.

Réseau de transport

Ce diagramme montre le réseau de transport de base qui est typiquement utilisé dans des réseaux de FlexVPN.

Réseau de substitution

Ce diagramme montre le réseau de substitution avec la Connectivité logique qui affiche comment le Basculement devrait fonctionner. Pendant le fonctionnement normal, le rai 1 et le rai 2 mettent à jour des relations avec un hub seulement.

Note: Dans le diagramme, les lignes vertes solides affichent la connexion et la direction de la version 2 primaire d'échange de clés Internet (IKE) (les sessions IKEv2)/Flex, et des lignes bleues pointillées indiquent la connexion de sauvegarde si la session d'Échange de clés Internet (IKE) à l'échouer de concentrateur principal.

L'adressage de /24 représente le groupe d'adresses allouées pour ce nuage, et pas l'adressage réel d'interface. C'est parce que le hub de FlexVPN alloue typiquement une adresse IP dynamique pour l'interface de rai, et se fonde sur des artères insérées dynamiquement par l'intermédiaire des commandes d'artère dans le bloc d'autorisation de FlexVPN.

Configuration de base de rai et de hub

La configuration de base du hub and spoke est basée sur des documents de transfert de VPN multipoint dynamique (DMVPN) à FlexVPN. Cette configuration est décrite dans le [transfert de FlexVPN : Mouvement dur de DMVPN à FlexVPN sur le même](#) article de [périphériques](#).

Réglage de configuration en étoile

Configuration en étoile - Bloc de configuration de client

La configuration en étoile doit être étendue par le bloc de configuration de client.

En configuration de base, des plusieurs homologues sont spécifiés. Le pair avec la préférence la plus élevée (le nombre le plus peu élevé) est considéré avant d'autres.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnell
```

La configuration de tunnel doit changer afin de permettre la destination de tunnel à choisir dynamiquement, basé sur le bloc de configuration de client de FlexVPN.

```
interface Tunnell
 tunnel destination dynamic
```

Il est crucial de se souvenir que le bloc de configuration de client de FlexVPN est attaché à une interface, et pas d'IKEv2 ou du profil d'IPSec (IPsec).

Le bloc de configuration de client fournit les nombreuses options afin d'ajuster le temps et les exécutions de Basculement, qui incluent dépister l'utilisation d'objets, l'Accès direct secours, et les fonctionnalités de groupes de sauvegarde.

Avec la configuration de base, le rai se fonde sur DPDs afin de le détecter si un rai est insensible, et il déclenche une modification une fois que le pair est déclaré complètement. L'option d'utiliser DPD n'est pas rapide, en raison de la façon dont travail de DPDs. Un administrateur pourrait vouloir améliorer la configuration avec le Suivi d'objets ou les améliorations semblables.

Le pour en savoir plus, se rapportent au chapitre de **configuration de client de FlexVPN** du guide de configuration Cisco IOS, qui est joint dans la **section Informations connexes à la fin** de ce document.

Pleine configuration en étoile - Référence

```
interface Tunnell
 tunnel destination dynamic
```

[Configuration du concentrateur](#)

Tandis que la majorité de la configuration de hub demeure la même, plusieurs aspects doivent être abordés. La plupart d'entre eux concerne une situation dans lesquels ou plus de rais sont connectés à un hub, alors que d'autres restent dans les relations à un autre hub.

Adresses de rai

Puisque les rais obtiennent des adresses IP des Concentrateurs, on le désire normalement que les Concentrateurs affectent des adresses des différents sous-réseaux ou une différente partie d'un sous-réseau.

Exemple :

Hub1

```
interface Tunnell
 tunnel destination dynamic
```

Hub2

```
interface Tunnell
 tunnel destination dynamic
```

Ceci empêche la création de superposition, même si les adresses ne sont pas conduites en dehors de du nuage de FlexVPN, qui pourrait altérer le dépannage.

Adresse de recouvrement de hub

Les deux Concentrateurs peuvent retenir la même adresse IP sur une interface de modèle virtuel ; cependant, ceci peut affecter le dépannage dans certains cas. Ce choix de conception le facilite pour se déployer et prévoir, puisque le rai doit avoir seulement une adresse de pair pour le Protocole BGP (Border Gateway Protocol).

Dans certains cas, il ne pourrait pas être désiré ou été nécessaire.

Acheminement

Il est que les Concentrateurs permutent des informations sur les rais qui sont connectés.

Les Concentrateurs doivent pouvoir permuter les artères spécifiques des périphériques qu'ils ont connectés, et fournir toujours un résumé aux rais.

Puisque Cisco recommande que vous utilisiez l'iBGP avec FlexVPN et DMVPN, seulement ce protocole de routage est affiché.

```
interface Tunnell
 tunnel destination dynamic
```

```
interface Tunnell
 tunnel destination dynamic
```

Cette configuration laisse :

- Auditeur dynamique des adresses assignées aux rais
- La publicité du réseau de **192.168.0.0/24**
- La publicité de la route récapitulative de **192.168.0.0/16** à tous les rais. La configuration d'aggregate-address crée une artère statique pour ce préfixe par l'intermédiaire de l'interface null0, qui est une route de suppression qui est utilisée afin d'empêcher des boucles de routage.
- Expédition des préfixes spécifiques à l'autre hub
- Client de réflecteur de route pour s'assurer que les Concentrateurs permutent les informations apprises des rais entre l'un l'autre

Ce diagramme représente l'échange de préfixe dans le BGP dans cette installation, de la perspective d'un des Concentrateurs.

Note: Dans ce diagramme, la ligne verte représente les informations fournies par des rai au hub, la ligne rouge représente les informations fournies par chaque hub aux rai (un résumé seulement), et la ligne bleue représente les préfixes permutés entre les Concentrateurs.

Utilisation de résumés de réseau

Les résumés ne pourraient pas être applicables ou désirés dans quelques scénarios. Précaution d'usage quand vous indiquez l'IP de destination dans les préfixes, parce que l'iBGP n'ignore pas le prochain saut par défaut.

Des résumés sont recommandés dans les réseaux qui changent l'état fréquemment. Par exemple, les connexions Internet instables pourraient exiger des résumés : évitez la suppression et l'ajout des préfixes, limitez le nombre de mises à jour, et permettez à la plupart des installations pour mesurer correctement.

Tunnels de spoke-to-spoke

Dans le scénario et la configuration mentionnés dans la section précédente, les rai sur différents Concentrateurs ne peuvent pas établir les tunnels directs de spoke-to-spoke. Le trafic entre les rai a connecté à différents Concentrateurs des écoulements au-dessus des périphériques centraux.

Il y a un contournement facile pour ceci. Cependant, il exige que le Protocole NHRP (Next Hop Resolution Protocol) avec le même network-id est activé entre les Concentrateurs. Ceci peut être réalisé, par exemple, si vous créez un tunnel point par point d'Encapsulation de routage générique (GRE) entre les Concentrateurs. Puis, IPsec n'est pas exigé.

Vérifiez

[L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

La **crypto** commande d'**ikev2 SA d'exposition** vous informe au sujet d'où le rai est actuellement connecté.

La **crypto** commande de **flexvpn du client ikev2 d'exposition** permet à un administrateur pour comprendre l'état actuel de l'exécution de client de FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn
```

```
Spoke2# show crypto ikev2 client flexvpn
```

Un Basculement réussi avec la configuration de **show logging** se connecte cette sortie sur le périphérique de rai :

```
Spoke2# show crypto ikev2 client flexvpn
```

Dans cette sortie, les démonter de rai du **hub 172.25.1.1**, le bloc de configuration de client de Flex_Client détecte la panne et force une connexion à **172.25.2.1** où un tunnel monte, et un rai est assigné un IP de **10.1.1.177**.

Dépannez

[L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Note: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Voici les commandes de débogage appropriées :

- **debug crypto ikev2**
- **debug radius**

Informations connexes

- [FlexVPN et guide de configuration de version 2 d'échange de clés Internet \(IKE\), Cisco IOS version 15 M&T](#)
- [Support et documentation techniques - Cisco Systems](#)