Exemple de configuration de protocole EIGRP sur SVTI, DVTI et IKEv2 FlexVPN avec la commande « IP[v6] Unnumbered »

Contenu

Introduction

Ce document décrit comment configurer le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) dans un certain nombre de scénarios courants sur Cisco IOS®. Afin d'accepter une contiguïté de voisinage EIGRP, Cisco IOS doit obtenir le paquet HELLO EIGRP à partir d'une adresse IP dans le même sous-réseau. Il est possible de désactiver cette vérification avec la commande **ip unnumbered**.

La première partie de l'article présente une défaillance EIGRP lorsqu'il reçoit un paquet qui n'est pas dans le même sous-réseau.

Un autre exemple illustre l'utilisation de la commande **ip unnumbered** qui désactive cette vérification et permet au protocole EIGRP de former une contiguïté entre des homologues appartenant à des sous-réseaux différents.

Cet article présente également un déploiement FlexVPN Hub and Spoke avec une adresse IP envoyée par le serveur. Dans ce scénario, la vérification des sous-réseaux est désactivée pour la

commande **ip address negotiation** et pour la commande **ip unnumbered**. La commande **ip unnumbered** est principalement utilisée pour les interfaces de type point à point (P2P), ce qui fait de FlexVPN un ajustement parfait puisqu'elle est basée sur une architecture P2P.

Enfin, un scénario IPv6 est présenté, ainsi que des différences pour les interfaces de tunnel virtuel statique (SVTI) et les interfaces de tunnel virtuel dynamique (DVTI). Il y a de légers changements de comportement lorsque vous comparez les scénarios IPv6 à IPv4.

En outre, les modifications entre les versions 15.1 et 15.3 de Cisco IOS sont présentées (ID de bogue Cisco CSCtx45062).

La commande **ip unnumbered** est toujours nécessaire pour DVTI. En effet, les adresses IP configurées de manière statique sur une interface de modèle virtuel ne sont jamais clonées à une interface d'accès virtuel. En outre, une interface sans adresse IP configurée ne peut pas établir de contiguïté de protocole de routage dynamique. La commande **ip unnumbered** n'est pas nécessaire pour SVTI, mais sans ce sous-réseau, la vérification est effectuée lorsque la contiguïté du protocole de routage dynamique est établie. De même, la commande **ipv6 unnumbered** n'est pas nécessaire pour les scénarios IPV6 en raison des adresses link-local utilisées pour créer des contiguïtés EIGRP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN sur Cisco IOS
- Configuration FlexVPN sur Cisco IOS

Components Used

Les informations de ce document sont basées sur la version 15.3T de Cisco IOS.

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. If your network is live, make sure that you understand the potential impact of any command.

EIGRP sur un segment Ethernet avec différents sous-réseaux

Topologie: Routeur 1 (R1) (e0/0 : 10.0.0.1/24)—(e0/1 : 10.0.1.2/24) Routeur 2 (R2)

R1:

```
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

router eigrp 100
network 10.0.0.1 0.0.0.0
```

R2:

```
interface Ethernet0/0
ip address 10.0.1.2 255.255.255.0

router eigrp 100
network 10.0.1.2 0.0.0.0
```

R1 affiche :

```
*Mar 3 16:39:34.873: EIGRP: Received HELLO on Ethernet0/0 nbr 10.0.1.2
*Mar 3 16:39:34.873:   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
*Mar 3 16:39:34.873: EIGRP-IPv4(100): Neighbor 10.0.1.2 not on common subnet
for Ethernet0/0
```

Cisco IOS ne forme pas de contiguïté, ce qui est attendu. Pour plus d'informations à ce sujet, référez-vous à Que signifient les messages EIGRP « Not On Common Subnet » ? article.

EIGRP sur le segment SVTI avec différents sous-réseaux

La même situation se produit lorsque vous utilisez des interfaces de tunnel virtuel (VTI) (tunnel GRE (Generic Routing Encapsulation)).

Topologie: R1(Tun1) : 172.16.0.1/24)—(Tun1 : 172.17.0.2/24) R2

R1:

```
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

interface Tunnel1
 ip address 172.16.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.2

router eigrp 100
 network 172.16.0.1 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R2:

```
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0

interface Tunnel1
 ip address 172.17.0.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.1

router eigrp 100
 network 172.17.0.2 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R1 affiche :

```
*Mar  3 16:41:52.167: EIGRP: Received HELLO on Tunnel1 nbr 172.17.0.2
*Mar  3 16:41:52.167:   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
*Mar  3 16:41:52.167: EIGRP-IPv4(100): Neighbor 172.17.0.2 not on common subnet
for Tunnel1
```

C'est un comportement attendu.

Utiliser la commande IP Unnumbered

Cet exemple montre comment utiliser la commande **ip unnumbered** qui désactive la vérification et permet l'établissement d'une session EIGRP entre des homologues de différents sous-réseaux.

La topologie est similaire à l'exemple précédent, mais les adresses des tunnels sont maintenant définies via la commande **ip unnumbered** qui pointe vers les boucles :

Topologie: R1(Tun1) : 172.16.0.1/24)—(Tun1 : 172.17.0.2/24) R2

```
R1:
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

interface Loopback0
 ip address 172.16.0.1 255.255.255.0

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.2

router eigrp 100
 network 172.16.0.1 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1

R2:
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0

interface Loopback0
 ip address 172.17.0.2 255.255.255.0

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.1

router eigrp 100
 network 172.17.0.2 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R1 affiche :

```
*Mar  3 16:50:39.046: EIGRP: Received HELLO on Tunnel1 nbr 172.17.0.2
*Mar  3 16:50:39.046:   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
*Mar  3 16:50:39.046: EIGRP: New peer 172.17.0.2
*Mar  3 16:50:39.046: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 172.17.0.2
(Tunnel1) is up: new adjacency
```

```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                           (sec)         (ms)       Cnt Num
0   172.17.0.2              Tu1               12 00:00:07    7  1434  0  13

R1#show ip route eigrp
     172.17.0.0/24 is subnetted, 1 subnets
D        172.17.0.0 [90/27008000] via 172.17.0.2, 00:00:05, Tunnel1

R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.0.0.1         YES manual up                    up
Loopback0                172.16.0.1      YES manual up                    up
Tunnel1                    172.16.0.1      YES TFTP  up                     up
```

R2 est similaire à ceci.

Après avoir modifié la commande **ip unnumbered** en une configuration d'adresse IP spécifique, aucune contiguïté EIGRP ne se forme.

EIGRP sur segment SVTI à DVTI avec différents sous-réseaux

Cet exemple utilise également la commande ip unnumbered. Les règles mentionnées précédemment s'appliquent également à DVTI.

Topologie: R1(Tun1) : 172.16.0.1/24)—(Modèle virtuel : 172.17.0.2/24) R2

L'exemple précédent est modifié ici afin d'utiliser DVTI au lieu de SVTI. En outre, la protection de tunnel est ajoutée dans cet exemple.

R1:

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set TS esp-des esp-md5-hmac
!
crypto ipsec profile prof
 set transform-set TS
!
interface Loopback0
 ip address 172.16.0.1 255.255.255.0
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile prof
!
router eigrp 100
 network 172.16.0.1 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R2:

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp profile profLAN
  keyring default
  match identity address 10.0.0.1 255.255.255.255
   virtual-template 1
!
crypto ipsec transform-set TS esp-des esp-md5-hmac
!
crypto ipsec profile profLAN
 set transform-set TS
 set isakmp-profile profLAN

interface Loopback0
 ip address 172.17.0.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile profLAN
!
!
router eigrp 100
 network 172.17.0.2 0.0.0.0
 passive-interface default
 no passive-interface Virtual-Template1
```

Tout fonctionne comme prévu :

```
R1#show crypto session
Crypto session current status
Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
 IKEv1 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map


R1#show crypto ipsec sa
interface: Tunnel1
   Crypto map tag: Tunnel1-head-0, local addr 10.0.0.1
  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 10.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 89, #pkts encrypt: 89, #pkts digest: 89
   #pkts decaps: 91, #pkts decrypt: 91, #pkts verify: 91


R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
0   172.17.0.2              Tu1               13 00:06:31    7  1434  0  19
```

```
R1#show ip route eigrp
     172.17.0.0/24 is subnetted, 1 subnets
D        172.17.0.0 [90/27008000] via 172.17.0.2, 00:06:35, Tunnel1
```

```
R2#show crypto session
Crypto session current status
Interface: Virtual-Access1
Profile: profLAN
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
 IKEv1 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
```

```
R2#show crypto ipsec sa
interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 10.0.0.2
  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 10.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 107, #pkts encrypt: 107, #pkts digest: 107
   #pkts decaps: 105, #pkts decrypt: 105, #pkts verify: 105
```

```
R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
0   172.16.0.1              Vi1               13 00:07:41   11   200  0  16
```

```
R2#show ip route eigrp
     172.16.0.0/24 is subnetted, 1 subnets
D        172.16.0.0 [90/1433600] via 172.16.0.1, 00:07:44, Virtual-Access1
```

Comme pour les exemples précédents, lorsque vous essayez de configurer 172.16.0.1 et 172.17.0.2 directement sous les interfaces de tunnel, EIGRP échoue avec exactement la même erreur que précédemment.

EIGRP sur IKEv2 Flex VPN avec différents sous-réseaux

Voici l'exemple de configuration du concentrateur et de la plate-forme FlexVPN. Le serveur envoie l’adresse IP via le mode de configuration du client.

Topologie: R1(e0/0) : 172.16.0.1/24)—(e0/1 : 172.16.0.2/24) R2

Configuration du concentrateur (R1) :

```
aaa new-model
aaa authorization network LOCALIKEv2 local
```

```
crypto ikev2 authorization policy AUTHOR-POLICY
 pool POOL
!
crypto ikev2 keyring KEYRING
 peer R2
 address 172.16.0.2
 pre-shared-key CISCO
 !

crypto ikev2 profile default
 match identity remote key-id FLEX
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list LOCALIKEv2 AUTHOR-POLICY
 virtual-template 1

interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 172.16.0.1 255.255.255.0

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
!
router eigrp 1
 network 1.1.1.1 0.0.0.0
 passive-interface default
 no passive-interface Virtual-Template1
!
ip local pool POOL 192.168.0.1 192.168.0.10
```

Configuration du satellite :

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

crypto ikev2 authorization policy FLEX
 route set interface
!
!
!
crypto ikev2 keyring KEYRING
 peer R1
 address 172.16.0.1
 pre-shared-key CISCO
 !
!
!
crypto ikev2 profile default
 match identity remote address 172.16.0.1 255.255.255.255
 identity local key-id FLEX
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
```

```
 aaa authorization group psk list FLEX FLEX

interface Loopback0
 ip address 2.2.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 172.16.0.2 255.255.255.0

interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default

router eigrp 1
 network 0.0.0.0
 passive-interface default
 no passive-interface Tunnel0
```

Le satellite utilise SVTI afin de se connecter au concentrateur qui utilise DVTI pour tous les rayons. Étant donné que le protocole EIGRP n'est pas aussi flexible que le protocole OSPF (Open Shortest Path First) et qu'il n'est pas possible de le configurer sous l'interface (SVTI ou DVTI), le **réseau 0.0.0.0** est utilisé sur le satellite afin de s'assurer que le protocole EIGRP est activé sur l'interface **Tun0**. Une interface passive est utilisée afin de s'assurer que la contiguïté est formée uniquement sur l'interface **Tun0**.

Pour ce déploiement, il est également nécessaire de configurer **ip unnumbered** sur le concentrateur. Lorsque vous configurez manuellement une adresse IP sous l'interface de modèle virtuel, elle n'est pas clonée à l'interface d'accès virtuel. Ensuite, aucune adresse IP n'est attribuée à l'interface d'accès virtuel et la contiguïté EIGRP ne se forme pas. C'est pourquoi la commande **ip unnumbered** est toujours requise pour les interfaces DVTI afin de former une contiguïté EIGRP.

Dans cet exemple, une contiguïté EIGRP est construite entre 1.1.1.1 et 192.168.0.9.

Test sur le concentrateur :

```
R1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            172.16.0.1      YES NVRAM  up                    up
Ethernet0/1            unassigned      YES NVRAM  administratively down down
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
Loopback0              1.1.1.1         YES manual up                    up
Virtual-Access1        1.1.1.1         YES unset  up                    up
Virtual-Template1      1.1.1.1         YES manual up                    down

R1#show crypto session
Crypto session current status

Interface: Virtual-Access1
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
 IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map

R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address            Interface              Hold Uptime   SRTT   RTO  Q  Seq
```

```
                                          (sec)         (ms)       Cnt Num
0   192.168.0.9          Vi1                  10 01:28:49   12  1494  0  13

R1#show ip route eigrp
....
Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/27008000] via 192.168.0.9, 01:28:52, Virtual-Access1
```

Du point de vue de Spoke, la commande **ip address négocié** fonctionne de la même manière que la commande **ip address unnumbered**, et la vérification du sous-réseau est désactivée.

Test sur le satellite :

```
R2#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            172.16.0.2      YES NVRAM  up                    up
Ethernet0/1            unassigned      YES NVRAM  administratively down down
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
Loopback0              2.2.2.2         YES NVRAM  up                    up
Tunnel0                192.168.0.9     YES NVRAM  up                    up

R2#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 IKEv2 SA: local 172.16.0.2/500 remote 172.16.0.1/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map

R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address            Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   1.1.1.1            Tu0                      14 01:30:18   15  1434  0  14

R2#show ip route eigrp
....
     1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 1.1.1.1, 01:30:21
```

Mode de configuration du routage

Internet Key Exchange version 2 (IKEv2) est une autre option. Il est possible d'utiliser le mode de configuration afin de transmettre des routes. Dans ce scénario, EIGRP et la commande **ip unnumbered** ne sont pas nécessaires.

Vous pouvez modifier l'exemple précédent afin de configurer le concentrateur pour envoyer cette

route via le mode de configuration :

```
crypto ikev2 authorization policy AUTHOR-POLICY
 pool POOL
 route set access-list SPLIT

ip access-list standard SPLIT
 permit 1.1.1.0 0.0.0.255
```

Le Spoke voit 1.1.1.1 comme statique, pas EIGRP :

```
R2#show ip route
....
     1.0.0.0/24 is subnetted, 1 subnets
S        1.1.1.0 is directly connected, Tunnel0
```

Le même processus fonctionne dans la direction opposée. Le satellite envoie une route au concentrateur :

```
crypto ikev2 authorization policy FLEX
 route set access-list SPLIT

ip access-list standard SPLIT
 permit 2.2.2.0 0.0.0.255
```

Le concentrateur le considère comme statique (pas EIGRP) :

```
R1#show ip route
....
     2.0.0.0/24 is subnetted, 1 subnets
S        2.2.2.0 is directly connected, Virtual-Access1
```

Dans ce scénario, le protocole de routage dynamique et la commande **ip unnumbered** ne sont pas nécessaires.

IPV6 EIGRP sur le segment SVTI avec différents sous-réseaux

Pour IPv6, la situation est différente. En effet, les adresses link-local IPv6 (FE80::/10) sont utilisées afin de créer une contiguïté EIGRP ou OSPF. Les adresses link-local valides appartiennent toujours au même sous-réseau, il n'est donc pas nécessaire d'utiliser la commande **ipv6 unnumbered** pour cela.

La topologie ici est identique à celle de l'exemple précédent, à ceci près que toutes les adresses IPv4 sont remplacées par des adresses IPv6.

Configuration de R1 :

```
interface Tunnel1
 no ip address
 ipv6 address FE80:1::1 link-local
 ipv6 address 2001:1::1/64
```

```
 ipv6 enable
 ipv6 eigrp 100
 tunnel source Ethernet0/0
 tunnel mode gre ipv6
 tunnel destination 2001::2

interface Loopback0
 description Simulate LAN
 no ip address
 ipv6 address 2001:100::1/64
 ipv6 enable
 ipv6 eigrp 100

interface Ethernet0/0
 no ip address
 ipv6 address 2001::1/64
 ipv6 enable

ipv6 router eigrp 100
```

Configuration de R2 :

```
interface Tunnel1
 no ip address
 ipv6 address FE80:2::2 link-local
 ipv6 address 2001:2::2/64
 ipv6 enable
 ipv6 eigrp 100
 tunnel source Ethernet0/0
 tunnel mode gre ipv6
 tunnel destination 2001::1

interface Loopback0
 description Simulate LAN
 no ip address
 ipv6 address 2001:200::1/64
 ipv6 enable
 ipv6 eigrp 100

interface Ethernet0/0
 no ip address
 ipv6 address 2001::2/64
 ipv6 enable

ipv6 router eigrp 100
```

Les adresses de tunnel se trouvent dans différents sous-réseaux (2001:1::1/64 et 2001:2::2/64), mais ce n'est pas important. Les adresses link-local sont utilisées afin de créer une contiguïté. Avec ces adresses, il réussit toujours.

Sur R1 :

```
R1#show ipv6 int brief
Ethernet0/0            [up/up]
   FE80::A8BB:CCFF:FE00:6400
   2001::1
Loopback0              [up/up]
   FE80::A8BB:CCFF:FE00:6400
   2001:100::1
Tunnel1                [up/up]
   FE80:1::1
```

```
   2001:1::1

R1#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(100)
H   Address             Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                               (sec)         (ms)       Cnt Num
0   Link-local address: Tu1                      12 00:13:58  821  4926  0  17
    FE80:2::2

R1#show ipv6 route eigrp
...
D   2001:2::/64 [90/28160000]
    via FE80:2::2, Tunnel1
D   2001:200::/64 [90/27008000]
    via FE80:2::2, Tunnel1
```

Sur R2 :

```
R2#show ipv6 int brief
Ethernet0/0            [up/up]
   FE80::A8BB:CCFF:FE00:6500
   2001::2
Loopback0              [up/up]
   FE80::A8BB:CCFF:FE00:6500
   2001:200::1
Tunnel1                [up/up]
   FE80:2::2
   2001:2::2

R2#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(100)
H   Address             Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                               (sec)         (ms)       Cnt Num
0   Link-local address: Tu1                      14 00:15:31   21  1470  0  18
   FE80:1::1

R2#show ipv6 route eigrp
...
D   2001:1::/64 [90/28160000]
    via FE80:1::1, Tunnel1
D   2001:100::/64 [90/27008000]
    via FE80:1::1, Tunnel1
```

Le réseau IPv6 homologue est installé par le processus EIGRP. Sur R1, le réseau 2001:2::/64 est installé et ce réseau est un sous-réseau différent de 2001:1::/64. Il en va de même pour R2. Par exemple, 2001::1/64 est installé, qui est un sous-réseau pour son adresse IP homologue. Il n'est pas nécessaire d'utiliser la commande **ipv6 unnumbered** ici. En outre, la commande **ipv6 address** n'est pas nécessaire sur l'interface de tunnel afin d'établir la contiguïté EIGRP, car les adresses link-local sont utilisées (et elles sont générées automatiquement lorsque vous activez IPv6 avec la commande **ipv6 enable**).

IPV6 EIGRP sur IKEv2 Flex VPN avec différents sous-réseaux

La configuration DVTI pour IPv6 est différente de celle pour IPv4 : il n'est plus possible de configurer une adresse IP statique.

```
R1(config)#interface Virtual-Template2 type tunnel
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address ?
 autoconfig  Obtain address using autoconfiguration
 dhcp        Obtain a ipv6 address using dhcp
 negotiated  IPv6 Address negotiated via IKEv2 Modeconfig

R1(config-if)#ipv6 address
```

Ceci est attendu, car une adresse statique n'est jamais clonée à une interface d'accès virtuel. C'est pourquoi la commande **ipv6 unnumbered** est recommandée pour la configuration du concentrateur et la commande **ipv6 address négocié** est recommandée pour la configuration de Spoke.

La topologie est identique à celle de l'exemple précédent, sauf que toutes les adresses IPv4 sont remplacées par des adresses IPv6.

Configuration du concentrateur (R1) :

```
aaa authorization network LOCALIKEv2 local

crypto ikev2 authorization policy AUTHOR-POLICY
 ipv6 pool POOL

crypto ikev2 keyring KEYRING
 peer R2
 address 2001::2/64
 pre-shared-key CISCO

crypto ikev2 profile default
 match identity remote key-id FLEX
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list LOCALIKEv2 AUTHOR-POLICY
 virtual-template 1

interface Loopback0
 no ip address
 ipv6 address 2001:100::1/64
 ipv6 enable
 ipv6 eigrp 100

interface Ethernet0/0
 no ip address
 ipv6 address 2001::1/64
 ipv6 enable

interface Virtual-Template1 type tunnel
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 eigrp 100
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile default

ipv6 local pool POOL 2001:10::/64 64
ipv6 router eigrp 100
 eigrp router-id 1.1.1.1
```

Configuration du satellite (R2) :

```
aaa authorization network FLEX local

crypto ikev2 authorization policy FLEX
 route set interface

crypto ikev2 keyring KEYRING
 peer R1
 address 2001::1/64
 pre-shared-key CISCO

crypto ikev2 profile default
 match identity remote address 2001::1/64
 identity local key-id FLEX
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list FLEX FLEX

interface Tunnel0
 no ip address
 ipv6 address negotiated
 ipv6 enable
 ipv6 eigrp 100
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2001::1
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001::2/64
 ipv6 enable

ipv6 router eigrp 100
 eigrp router-id 2.2.2.2
```

Vérification :

```
R2#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(100)
H   Address             Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                (sec)         (ms)       Cnt Num
0   Link-local address: Tu0                      11 00:12:32   17  1440  0  12
   FE80::A8BB:CCFF:FE00:6500

R2#show ipv6 route eigrp
....
D   2001:100::/64 [90/27008000]
    via FE80::A8BB:CCFF:FE00:6500, Tunnel0

R2#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
```

```
Uptime: 00:13:17
Session status: UP-ACTIVE
Peer: 2001::1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 2001::1
     Desc: (none)
 IKEv2 SA: local 2001::2/500
         remote 2001::1/500 Active
         Capabilities:(none) connid:1 lifetime:23:46:43
 IPSEC FLOW: permit ipv6 ::/0 ::/0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 190 drop 0 life (KB/Sec) 4271090/2803
       Outbound: #pkts enc'ed 194 drop 0 life (KB/Sec) 4271096/2803

R2#ping 2001:100::1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2001:100::1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/5 ms

R2#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:13:27
Session status: UP-ACTIVE
Peer: 2001::1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 2001::1
     Desc: (none)
 IKEv2 SA: local 2001::2/500
         remote 2001::1/500 Active
         Capabilities:(none) connid:1 lifetime:23:46:33
 IPSEC FLOW: permit ipv6 ::/0 ::/0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 292 drop 0 life (KB/Sec) 4271071/2792
       Outbound: #pkts enc'ed 296 drop 0 life (KB/Sec) 4271082/2792
```

Pour DVTI, IPv6 ne peut pas être configuré manuellement. La commande **ipv6 unnumbered** est recommandée pour le concentrateur et la commande **ipv6 address négocié** est recommandée sur le satellite.

Ce scénario présente la commande **ipv6 unnumbered** pour DVTI. Il est important de noter que, pour IPv6 par opposition à IPv4, la commande **ipv6 unnumbered** sur l'interface virtual-template n'est pas nécessaire. La raison en est la même que pour le scénario SVTI IPv6 : l'adresse ipv6 link-local est utilisée pour créer la contiguïté. L'interface d'accès virtuel, qui est clonée à partir du modèle virtuel, hérite de l'adresse link-local IPv6, ce qui est suffisant pour créer une contiguïté EIGRP.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Caveats connus

ID de bogue Cisco CSCtx45062 FlexVPN : Eigrp ne doit pas vérifier les sous-réseaux courants si les adresses IP du tunnel sont /32.

Ce bogue et cette correction ne sont pas spécifiques à FlexVPN. Entrez cette commande avant d'implémenter le correctif (version 15.1 du logiciel) :

```
R2(config-if)#do show run int tun1
Building configuration...

Current configuration : 165 bytes

interface Tunnel1
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.1
 tunnel protection ipsec profile prof1

R2(config-if)#ip address 192.168.200.1 255.255.255.255
Bad mask /32 for address 192.168.200.1
```

Entrez cette commande après le correctif (logiciel 15.3) :

```
R2(config-if)#do show run int tun1
Building configuration...

Current configuration : 165 bytes

interface Tunnel1
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.1
 tunnel protection ipsec profile prof1

R2(config-if)#ip address 192.168.200.1 255.255.255.255
R2(config-if)#
*Jun 14 18:01:12.395: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.100.1 (Tunnel1) is up: new adjacency
```

Il y a en fait deux modifications dans la version 15.3 du logiciel :

- **Le masque de réseau /32** est accepté pour toutes les adresses IP.
- Il n'existe aucune vérification de sous-réseau pour un voisin EIGRP lorsque vous utilisez l'adresse **/32**.

Résumé

Le comportement EIGRP est modifié par la commande **ip unnumbered**. Il désactive les vérifications pour le même sous-réseau alors qu'il établit une contiguïté EIGRP.

Il est également important de se rappeler que lorsque vous utilisez des DVTIs configurées de manière statique sur le modèle virtuel, il n'est pas cloné à l'accès virtuel. C'est pourquoi la commande **ip unnumbered** est nécessaire.

Pour FlexVPN, il n'est pas nécessaire d'utiliser la commande **ip unnumbered** lorsque vous utilisez l'adresse négociée sur le client. Mais il est important de l'utiliser sur le concentrateur lorsque vous utilisez le protocole EIGRP. Lorsque vous utilisez le mode de configuration pour le routage, le protocole EIGRP n'est pas nécessaire.

Pour SVTI, IPv6 utilise des adresses link-local pour la contiguïté et il n'est pas nécessaire d'utiliser la commande **ipv6 unnumbered**.

Pour DVTI, IPv6 ne peut pas être configuré manuellement. La commande **ipv6 unnumbered** est recommandée pour le concentrateur et la commande **ipv6 address négocié** est recommandée sur le satellite.

Informations connexes

- Guide de configuration de Cisco IOS 15.3 FlexVPN
- Références des commandes de Cisco IOS 15.3
- Support et documentation techniques - Cisco Systems