Configurer une session eBGP sécurisée avec une VTI IPsec

Contenu

Introduction

Ce document décrit comment sécuriser une relation de voisinage eBGP (Border Gateway Protocol) externe avec l'utilisation d'une interface de tunnel virtuel (VTI) IPsec avec les interfaces physiques (non tunnel) pour le trafic du plan de données. Cette configuration présente les avantages suivants :

- Confidentialité totale de la session de voisinage BGP avec confidentialité des données, anti-relecture, authenticité et intégrité.
- Le trafic du plan de données n'est pas limité à la surcharge MTU (Maximum Transmission Unit) de l'interface de tunnel. Les clients peuvent envoyer des paquets MTU standard (1 500 octets) sans incidence sur les performances ni fragmentation.
- Moins de surcharge sur les routeurs de point d'extrémité puisque le chiffrement/déchiffrement SPI (Security Policy Index) est limité au trafic du plan de contrôle BGP.

L'avantage de cette configuration est que le plan de données n'est pas limité à la limitation de l'interface tunnelisée. Par conception, le trafic du plan de données n'est pas sécurisé par IPsec.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- Principes fondamentaux de la configuration et de la vérification eBGP
- Manipulation de PA (Policy Accounting) BGP à l'aide d'une route-map
- Fonctions de base de la stratégie ISAKMP (Internet Security Association and Key Management Protocol) et IPsec

Components Used

Les informations de ce document sont basées sur le logiciel Cisco IOS® Version 15.3(1.3)T, mais d'autres versions prises en charge fonctionnent. Puisque la configuration IPsec est une fonction cryptographique, assurez-vous que votre version de code contient ce jeu de fonctions.

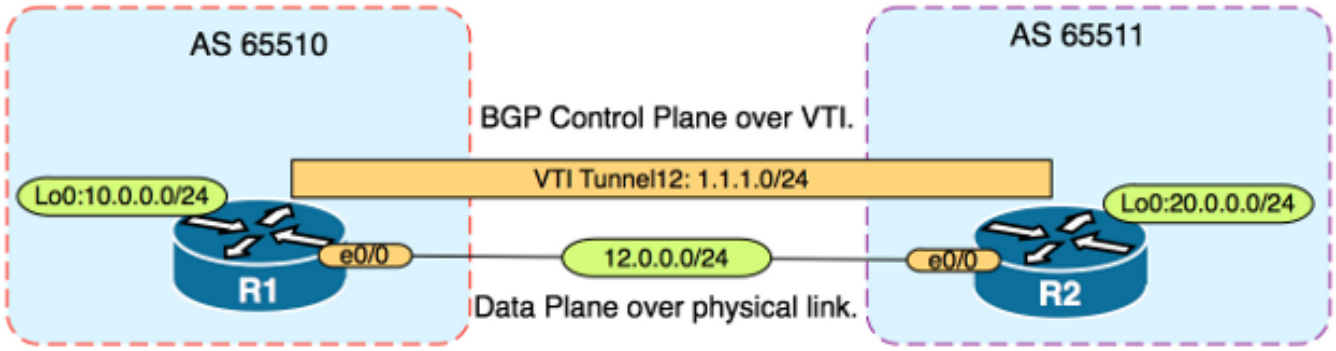
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Attention** : L'exemple de configuration de ce document utilise des algorithmes de chiffrement modestes qui peuvent ou non convenir à votre environnement. Reportez-vous au Livre blanc sur le chiffrement de nouvelle génération pour une discussion sur la sécurité relative de différentes suites de chiffrement et tailles de clé.

Configuration

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



Configurations

Procédez comme suit :

1. Configurez les paramètres IKE (Internet Key Exchange) de phase 1 sur R1 et R2 avec la clé pré-partagée sur R1 : **Note**: N'utilisez jamais les numéros de groupe DH 1, 2 ou 5 car ils sont considérés comme inférieurs. Si possible, utilisez un groupe DH avec la cryptographie elliptique (ECC), par exemple les groupes 19, 20 ou 24. Les normes AES (Advanced Encryption Standard) et SHA256 (Secure Hash Algorithm 256) doivent être considérées comme supérieures aux normes DE (Data Encryption Standard)/3DES et MD5 (Message Digest 5)/SHA1 respectivement. N'utilisez jamais le mot de passe « cisco » dans un environnement de production.**Configuration de R1**

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
```

```
R1(config-isakmp)exit

R1(config)#crypto isakmp key CISCO address 12.0.0.2
```

Configuration de R2

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```

2. Configurez le chiffrement de mot de passe de niveau 6 pour la clé pré-partagée dans la mémoire NVRAM sur R1 et R2. Cela réduit la probabilité que la clé pré-partagée stockée en texte clair ne soit pas lue si un routeur est compromis :

```
R1(config)#key config-key password-encrypt CISCOCISCO

R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```

Note: Une fois le chiffrement de mot de passe de niveau 6 activé, la configuration active n'affiche plus la version en texte clair de la clé pré-partagée :

```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```

3. Configurez les paramètres de phase 2 IKE sur R1 et R2 : **Configuration de R1**

```
R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
R1(ipsec-profile)#set pfs group19
```

Configuration de R2

```
R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET

R2(ipsec-profile)#set pfs group19
```

Note: La configuration de Perfect Forward Secrecy (PFS) est facultative mais améliore la puissance du VPN car elle force une nouvelle génération de clés symétriques dans l'établissement de l'association de sécurité IKE phase 2.

4. Configurez les interfaces de tunnel sur R1 et R2 et sécurisez-les avec le profil IPsec :

Configuration de R1

```
R1(config)#interface tunnel 12

R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0
```

```
R1(config-if)#tunnel mode ipsec ipv4

R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```

Configuration de R2

```
R2(config)#interface tunnel 12

R2(config-if)#ip address 1.1.1.2 255.255.255.0

R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```

5. Configurez BGP sur R1 et R2 et annoncez les réseaux loopback0 dans BGP : **Configuration de R1**

```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```

Configuration de R2

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```

6. Configurez une route-map sur R1 et R2 afin de modifier manuellement l'adresse IP du tronçon suivant afin qu'elle pointe vers l'interface physique et non vers le tunnel. Vous devez appliquer cette route-map dans la direction entrante. **Configuration de R1**

```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```

Configuration de R2

```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10

R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end
```

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Vérifiez que les phases 1 et 2 IKE sont terminées. Le protocole de ligne sur l'interface de tunnel virtuel (VTI) ne passe pas à actif tant que la phase IKE 2 n'est pas terminée :

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

Notez qu'avant l'application de la route-map, l'adresse IP du tronçon suivant pointe vers l'adresse IP du voisin BGP qui est l'interface de tunnel :

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

Lorsque le trafic utilise le tunnel, le MTU est limité au MTU du tunnel :

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
Success rate is 0 percent (0/5)
```

```
R1#show interfaces tunnel 12 | inc transport|line

Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

Après l'application de la route-map, l'adresse IP est remplacée par l'interface physique de R2, et non par le tunnel :

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

Modifiez le plan de données afin d'utiliser le saut suivant physique par opposition au tunnel autorise une MTU de taille standard :

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Dépannage

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