Configurer les interfaces de tunnel virtuel ASA dans un scénario de double ISP

Contenu

Introduction

Ce document décrit comment configurer VTI (Virtual Tunnel Intrfaces) entre deux ASA (Adaptive Security Appliances) à l'aide du protocole IKEv2 (Internet Key Exchange version 2) pour fournir une connectivité sécurisée entre deux filiales. Les deux filiales disposent de deux liaisons ISP pour une disponibilité élevée et un équilibrage de charge. Le voisinage BGP (Border Gateway Protocol) est établi sur les tunnels afin d'échanger des informations de routage interne.
Cette fonctionnalité est introduite dans ASA version 9.8(1). La mise en oeuvre ASA VTI est compatible avec la mise en oeuvre VTI disponible sur les routeurs IOS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- protocole BGP

Components Used

Les informations de ce document sont basées sur les pare-feu ASAv exécutant la version 9.8(1)6 du logiciel.

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.

Différences entre VTI et Crypto Map

- Crypto map est une fonction de sortie de l'interface. Afin d'envoyer le trafic via un tunnel basé sur une carte de chiffrement, le trafic doit être acheminé vers l'interface Internet orientée vers l'extérieur (traditionnellement appelée interface externe) et doit être mis en correspondance avec la liste de contrôle d'accès de chiffrement. Par contre, VTI est une interface logique. Le tunnel vers chaque homologue VPN est représenté par une VTI différente. Si le routage pointe vers VTI, le paquet sera chiffré et envoyé à l'homologue correspondant.

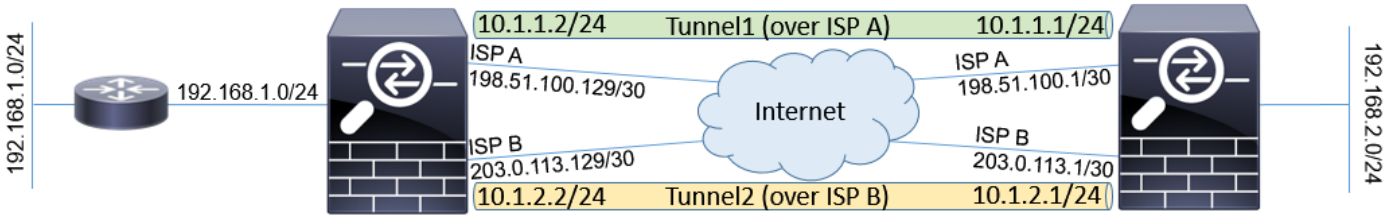
- VTI élimine la nécessité d'utiliser des listes d'accès cryptographiques et des règles d'exemption NAT (Network Address Translation).

- La liste de contrôle d'accès (ACL) crypto-map ne permet pas le chevauchement des entrées. VTI est un VPN basé sur une route et des règles de routage régulières s'appliquent au trafic VPN, ce qui simplifie la configuration et les processus de dépannage.

- La carte de chiffrement empêche automatiquement l'envoi en texte clair du trafic entre les sites en cas de panne du tunnel. VTI ne protège pas automatiquement contre elle. Des routes NULL doivent être ajoutées pour garantir une fonctionnalité égale.

Configuration

Diagramme du réseau



Configurations

Remarque : Cet exemple ne convient pas au scénario où l'ASA est membre d'un système autonome indépendant et possède des homologues BGP avec les réseaux ISP. Il couvre la topologie dans laquelle ASA a deux liaisons ISP indépendantes avec des adresses publiques de différents systèmes autonomes. Dans ce cas, le FAI peut déployer une protection anti-usurpation qui vérifie si les paquets reçus ne proviennent pas d'une adresse IP publique qui appartient à un autre FAI. Dans cette configuration, des mesures appropriées sont prises pour empêcher cela.

1. Paramètres communs de chiffrement et d'authentification. Vous trouverez des informations sur les paramètres cryptographiques recommandés à l'adresse suivante : https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

   Sur les deux ASA :

```
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 24
prf sha256
lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal PROP
protocol esp encryption aes-256
protocol esp integrity sha-256
```

2. Configurez le profil IPsec. L'une des parties doit être initiatrice et l'autre doit être responsable de la négociation IKEv2 :

   ASA est parti :

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
responder-only
```

   Droit ASA :

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
```

3. Activez le protocole IKEv2 sur les deux interfaces ISP.

   Les deux ASA :

```
crypto ikev2 enable ispa
crypto ikev2 enable ispb
```

4. Configurez la clé pré-partagée pour authentifier mutuellement les ASA :

   ASA est parti :

```
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.1 type ipsec-l2l
tunnel-group 203.0.113.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

   Droit ASA :

```
tunnel-group 198.51.100.129 type ipsec-l2l
tunnel-group 198.51.100.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.129 type ipsec-l2l
tunnel-group 203.0.113.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
```

```
ikev2 local-authentication pre-shared-key *****
```

5. Configurez les interfaces ISP :

   ASA est parti :
   ```
   interface GigabitEthernet0/1
   nameif ispa
   security-level 0
   ip address 198.51.100.129 255.255.255.252
   !
   interface GigabitEthernet0/2
   nameif ispb
   security-level 0
   ip address 203.0.113.129 255.255.255.252
   !
   ```
   Droit ASA :
   ```
   interface GigabitEthernet0/1
   nameif ispa
   security-level 0
   ip address 198.51.100.1 255.255.255.252
   !
   interface GigabitEthernet0/2
   nameif ispb
   security-level 0
   ip address 203.0.113.1 255.255.255.252
   !
   ```
6. La liaison principale est l'interface du FAI A. Le FAI B est secondaire. La disponibilité de la liaison principale est suivie avec l'utilisation de la requête ping ICMP à un hôte sur Internet, dans cet exemple, les ASA utilisent l'une de l'autre interface du FAI comme destination de la requête ping :

   ASA est parti :
   ```
   sla monitor 1
   type echo protocol ipIcmpEcho 198.51.100.1 interface ispa
   !
   sla monitor schedule 1 life forever start-time now
   !
   track 1 rtr 1 reachability
   !
   route ispa 0.0.0.0 0.0.0.0 198.51.100.130 1 track 1
   route ispb 0.0.0.0 0.0.0.0 203.0.113.130 10
   ```
   Droit ASA :
   ```
   sla monitor 1
   type echo protocol ipIcmpEcho 198.51.100.129 interface ispa
   !
   sla monitor schedule 1 life forever start-time now
   !
   track 1 rtr 1 reachability
   !
   route ispa 0.0.0.0 0.0.0.0 198.51.100.2 1 track 1
   route ispb 0.0.0.0 0.0.0.0 203.0.113.2 10
   ```
7. La VTI principale est toujours établie sur le FAI A. Le VTI secondaire est établi sur le FAI B. Des routes statiques vers la destination du tunnel sont nécessaires. Cela garantit que les paquets chiffrés quittent l'interface physique correcte pour éviter les pertes d'anti-usurpation du FAI :

   ASA est parti :

```
route ispa 198.51.100.1 255.255.255.255 198.51.100.130 1
route ispb 203.0.113.1 255.255.255.255 203.0.113.130 1
```

Droit ASA :

```
route ispa 198.51.100.129 255.255.255.255 198.51.100.2 1
route ispb 203.0.113.129 255.255.255.255 203.0.113.2 1
```

8. Configuration VTI :

ASA est parti :

```
interface Tunnel1
nameif tuna
ip address 10.1.1.2 255.255.255.0
tunnel source interface ispa
tunnel destination 198.51.100.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
!
interface Tunnel2
nameif tunb
ip address 10.1.2.2 255.255.255.0
tunnel source interface ispb
tunnel destination 203.0.113.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

Droit ASA :

```
interface Tunnel1
nameif tuna
ip address 10.1.1.1 255.255.255.0
tunnel source interface ispa
tunnel destination 198.51.100.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
!
interface Tunnel2
nameif tunb
ip address 10.1.2.1 255.255.255.0
tunnel source interface ispb
tunnel destination 203.0.113.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile PROF
```

9. Configuration BGP. Le tunnel associé au FAI A est un tunnel principal. Les préfixes annoncés sur le tunnel formé par le FAI B ont une préférence locale plus faible, ce qui les rend moins préférables par la table de routage :

ASA est parti :

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.1 remote-as 65000
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 next-hop-self
neighbor 10.1.2.1 remote-as 65000
neighbor 10.1.2.1 activate
neighbor 10.1.2.1 next-hop-self
neighbor 10.1.2.1 route-map BACKUP out
network 192.168.1.0
```

```
no auto-summary
no synchronization
exit-address-family
```

Droit ASA :

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.2 remote-as 65000
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 next-hop-self
neighbor 10.1.2.2 remote-as 65000
neighbor 10.1.2.2 activate
neighbor 10.1.2.2 next-hop-self
neighbor 10.1.2.2 route-map BACKUP out
network 192.168.2.0
no auto-summary
no synchronization
exit-address-family
```

10. (Facultatif) Afin d'annoncer un réseau supplémentaire derrière l'ASA gauche qui n'est pas directement connecté à celui-ci, la redistribution de route statique peut être configurée :

    ASA est parti :

    ```
    route inside 192.168.10.0 255.255.255.0 192.168.1.100 1
    !
    prefix-list REDISTRIBUTE_LOCAL seq 10 permit 192.168.10.0/24
    !
    route-map REDISTRIBUTE_LOCAL permit 10
    match ip address prefix-list REDISTRIBUTE_LOCAL
    !
    router bgp 65000
    address-family ipv4 unicast
    redistribute static route-map REDISTRIBUTE_LOCAL
    ```

11. (Facultatif) La charge du trafic peut être équilibrée entre les tunnels en fonction de la destination du paquet. Dans cet exemple, la route vers le réseau 192.168.10.0/24 est préférée au tunnel de secours (tunnel ISP B)

    ASA est parti :

    ```
    route-map BACKUP permit 5
    match ip address prefix-list REDISTRIBUTE_LOCAL
    set local-preference 200
    !
    route-map BACKUP permit 10
    set local-preference 80
    ```

12. Pour éviter que le trafic entre les sites ne soit envoyé en texte clair sur Internet si les tunnels sont en panne, des routes Null doivent être ajoutées. Toutes les adresses RFC1918 ont été ajoutées pour plus de simplicité :

    Les deux ASA :

    ```
    route Null0 10.0.0.0 255.0.0.0 250
    route Null0 172.16.0.0 255.240.0.0 250
    route Null0 192.168.0.0 255.255.0.0 250
    ```

13. (Facultatif) Par défaut, le processus BGP ASA envoie des keepalives une fois toutes les 60

secondes. Si la réponse keepalive n'est pas reçue de l'homologue pendant 180 secondes, elle est déclarée morte. Afin d'accélérer l'échec du voisin de détection, vous pouvez configurer des temporisateurs BGP. Dans cet exemple, les keepalives sont envoyées toutes les 10 secondes et le voisin est déclaré désactivé après 30 secondes.

```
router bgp 65000
address-family ipv4 unicast
neighbor 10.1.1.2 timers 10 30
neighbor 10.1.2.2 timers 10 30
exit-address-family
```

Vérification

Vérifiez si le tunnel IKEv2 est actif :

```
ASA-right(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:32538, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
836052177 198.51.100.1/500 198.51.100.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/7 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xc6623962/0x5c4a3bce

IKEv2 SAs:

Session-id:1711, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
832833529 203.0.113.1/500 203.0.113.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/29 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x2e3715af/0xc20e22b4
```

Vérifiez l'état du voisinage BGP :

```
ASA-right(config)# show bgp summary
BGP router identifier 203.0.113.1, local AS number 65000
BGP table version is 29, main routing table version 29
3 network entries using 600 bytes of memory
5 path entries using 400 bytes of memory
5/3 BGP path/bestpath attribute entries using 1040 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2040 total bytes of memory
BGP activity 25/22 prefixes, 69/64 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.2 4 65000 6 5 29 0 0 00:00:51 2
10.1.2.2 4 65000 7 6 29 0 0 00:01:20 2
```

Vérifiez les routes reçues du protocole BGP. Les routes marquées de ">" sont installées dans la table de routage :

```
ASA-right(config)# show bgp

BGP table version is 29, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*>i192.168.1.0 10.1.1.2 0 100 0 i
* i 10.1.2.2 0 80 0 i
*> 192.168.2.0 0.0.0.0 0 32768 i
* i192.168.10.0 10.1.1.2 0 100 0 ?
*>i 10.1.2.2 0 200 0 ?

Verify routing table:

ASA-right(config)# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.51.100.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.2, ispa
S 10.0.0.0 255.0.0.0 is directly connected, Null0
C 10.1.1.0 255.255.255.0 is directly connected, tuna
L 10.1.1.1 255.255.255.255 is directly connected, tuna
C 10.1.2.0 255.255.255.0 is directly connected, tunb
L 10.1.2.1 255.255.255.255 is directly connected, tunb
S 172.16.0.0 255.240.0.0 is directly connected, Null0
S 192.168.0.0 255.255.0.0 is directly connected, Null0
B 192.168.1.0 255.255.255.0 [200/0] via 10.1.1.2, 00:02:06
C 192.168.2.0 255.255.255.0 is directly connected, inside
L 192.168.2.1 255.255.255.255 is directly connected, inside
B 192.168.10.0 255.255.255.0 [200/0] via 10.1.2.2, 00:02:35
C 198.51.100.0 255.255.255.252 is directly connected, ispa
L 198.51.100.1 255.255.255.255 is directly connected, ispa
S 198.51.100.129 255.255.255.255 [1/0] via 198.51.100.2, ispa
C 203.0.113.0 255.255.255.252 is directly connected, ispb
L 203.0.113.1 255.255.255.255 is directly connected, ispb
S 203.0.113.129 255.255.255.255 [1/0] via 203.0.113.2, ispb
```

Dépannage

Débogues utilisés pour dépanner le protocole IKEv2 :

debug crypto ikev2 protocol 4
debug crypto ikev2 plate-forme 4

Pour plus d'informations sur le dépannage du protocole IKEv2 : https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

Pour plus d'informations sur le dépannage du protocole BGP : https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Informations connexes

- Règles de sélection de route BGP : https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- Guide de configuration BGP ASA : https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Support et documentation techniques - Cisco Systems