Configurez les interfaces de tunnel virtuelles ASA dans le double scénario ISP

Contenu

Introduction

Ce document décrit comment configurer VTI (tunnel virtuel Intrfaces) entre deux ASA (appliances de sécurité adaptable) avec l'utilisation d'IKEv2 (protocole de version d'échange de clés Internet (IKE) 2) pour fournir la connectivité sécurisée entre deux branchements. Chacun des deux branchements ont deux liens ISP pour les buts élevés d'availablility et d'Équilibrage de charge. La proximité de Protocole BGP (Border Gateway Protocol) est établie au-dessus des tunnels afin de permuter les informations de routage internes.
Cette caractéristique est introduite dans la version 9.8(1) ASA. L'implémentation ASA VTI est compatible avec l'implémentation VTI disponible sur des Routeurs IOS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole BGP

Composants utilisés

Les informations dans ce document sont basées sur des Pare-feu d'ASAv exécutant la version de logiciel 9.8(1)6.

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Différences entre VTI et crypto map

- Le crypto map est une caractéristique de sortie de l'interface. Afin d'envoyer le trafic par le crypto tunnel à base de cartes, le trafic doit être conduit à l'Internet faisant face à l'interface (traditionnellement appelée l'interface extérieure) et doit être apparié contre le crypto ACL. D'autre part, VTI est une interface logique. Le tunnel à chaque homologue VPN est représenté par un VTI différent. Si le routage se dirige vers VTI, le paquet sera chiffré et envoyé au pair correspondant.

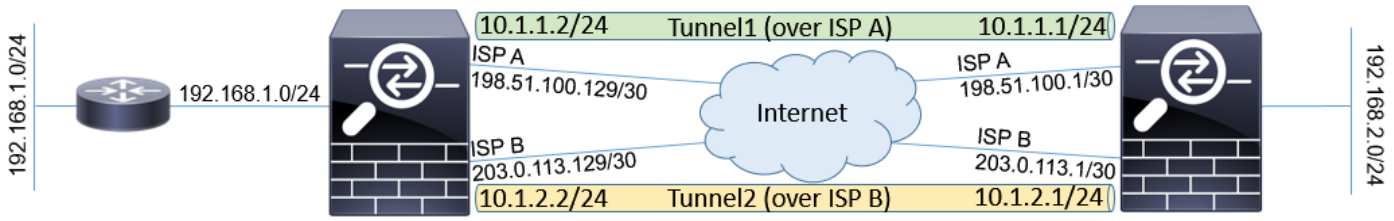
- VTI élimine la nécessité d'utiliser de cryptos règles de Listes d'accès et d'exemption de Traduction d'adresses de réseau (NAT).

- La liste de contrôle d'accès de crypto map (ACL) ne tient pas compte des entrées superposantes. VTI est un routage en fonction VPN et les règles régulières de routage s'appliquent pour le trafic VPN, qui simplifie la configuration et les processus pour dépanner.

- Le crypto map empêche automatiquement le trafic entre les sites à introduire le libellé si le tunnel est vers le bas. VTI ne se protège pas automatiquement contre lui. Des artères de null doivent être ajoutées pour assurer la fonctionnalité égale.

Configurez

Diagramme du réseau



Configurations

Note: Cet exemple n'est pas approprié au scénario où l'ASA est un membre d'Autonomous System independed et a des peerings BGP avec des réseaux ISP. Il couvre la topologie où l'ASA a deux liens d'ISP indépendant avec des annonces publiques de différents Autonomous System. Dans un tel cas, l'ISP peut déployer la protection anti-spoofing qui vérifie si les paquets reçus ne sont pas originaires de l'IP de public qui appartient à un autre ISP. Dans cette configuration, des mesures appropriées sont prises d'empêcher ceci.

1. Paramètres communs de cryptage et d'authentification. Des informations sur des paramètres cryptographiques recommandés peuvent être trouvées à : 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. Un des côtés doit être demandeur et on doit être un responder de la négociation IKEv2 :

ASA laissée :

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

Droite ASA :

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

3. Protocole de l'enable IKEv2 relatif aux 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 laissée :

```
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 *****
```

Droite 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 laissée :
```
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
!
```
   Droite 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 interface ISP A. L'ISP B est secondaire. La Disponibilité de liaison principale est dépistée avec l'utilisation de la requête ping d'ICMP à un hôte dans l'Internet, dans cet exemple l'utilisation ASA interface ISP A comme destination de ping :

   ASA laissée :
```
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
```
   Droite 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. Le VTI primaire est toujours établi au-dessus de l'ISP A. Secondary VTI est établi au-dessus d'ISP B. Static que les artères vers la destination de tunnel sont nécessaires. Ceci s'assure que le congé chiffré de paquets de l'interface physique correcte pour éviter l'anti-mystification ISP chute :

ASA laissée :

```
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
```

Droite 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 laissée :

```
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
```

Droite 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 avec ISP A est un primaire. Les préfixes annoncés au-dessus du tunnel formé au-dessus de l'ISP B ont des gens du pays-prefernce inférieurs qui les font moins préférés par la table de routage :

ASA laissée :

```
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
```

Droite 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 le réseau supplémentaire derrière l'ASA gauche qui n'est pas directement connectée à lui, la redistribution de routage statique peut être configurée :

    ASA laissée :

    ```
    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) le trafic peut être chargement équilibré entre les tunnels basés sur la destination de paquet. Dans cet exemple, l'artère vers le réseau 192.168.10.0/24 est préférée au-dessus du tunnel de sauvegarde (le tunnel d'ISP B)

    ASA laissée :

    ```
    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 empêcher le trafic entre les sites d'être introduit le libellé à l'Internet si les tunnels sont vers le bas, des artères de null doivent être ajoutées. Toutes les adresses RFC1918 ont été ajoutées pour la 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 le Keepalives une fois par seconde 60. Si la réponse de keepalive n'est pas reçue du pair pendant 180 secondes, on lui déclare complètement. Afin d'accélérer la panne de neigbor de détection, vous pouvez configurer des temporisateurs BGP. Dans cet exemple, le Keepalives est envoyé toutes les 10 secondes et le voisin est déclaré vers le bas 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
```

Vérifiez

Vérifiez si le tunnel IKEv2 est :

```
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 de proximité 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 artères reçues du BGP. Des artères identifiées par « > » 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
```

Dépannez

Debugs utilisés pour dépanner le protocole IKEv2 :

protocole 4 du debug crypto ikev2
plate-forme 4 du debug crypto ikev2

Pour plus d'informations sur dépanner le 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 dépanner le 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