ASA virtuele tunnelinterfaces configureren in dubbel ISP-scenario

Inhoud

Inleiding

Dit document beschrijft hoe u VTI (Virtual Tunnel Interfaces) tussen twee ASA's (adaptieve security applicaties) kunt configureren met gebruik van IKEv2 (Internet Key Exchange versie 2)-protocol om beveiligde connectiviteit tussen twee takken te waarborgen. Beide takken hebben twee ISP-links voor doeleinden van hoge beschikbaarheid en taakverdeling. Border Gateway Protocol (BGP) buurship wordt over de tunnels tot stand gebracht om informatie over de interne routering uit te wisselen.
Deze optie wordt toegevoegd in ASA versie 9.8(1). ASA VTI-implementatie is compatibel met VTI-implementatie beschikbaar op IOS-routers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- BGP-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op ASAv-firewalls met een softwareversie van 9.8(1)6.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

Verschillen tussen VTI en Crypto Map

- Crypto map is een uitvoerkenmerk van de interface. Om het verkeer door een op crypto kaart gebaseerde tunnel te kunnen doorsturen, moet het verkeer naar de interface op het internet worden geleid (traditioneel externe interface genoemd) en moet het zijn afgestemd op crypto ACL. Aan de andere kant is VTI een logische interface. Tunnel naar elke VPN-peer wordt weergegeven door een andere VTI. Als de routing naar VTI wijst, wordt het pakket versleuteld en naar de corresponderende peer verzonden.

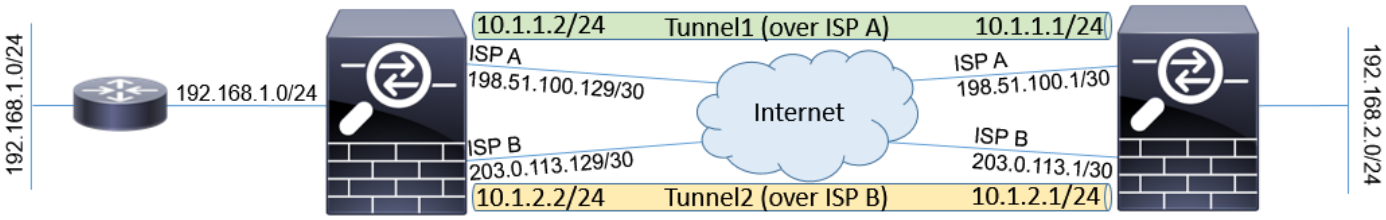
- VTI heft de noodzaak op om crypto toegangslijsten en NAT-vrijstellingsregels (Network Address Translation) te gebruiken.

- Crypto map Access Control List (ACL) maakt geen overlappende items mogelijk. VTI is een route gebaseerd VPN en de regelmatige routingregels zijn van toepassing op het VPN-verkeer, dat configuratie en processen voor probleemoplossing vereenvoudigt.

- Crypto map voorkomt automatisch verkeer tussen plaatsen die in klcleartext worden verstuurd als tunnel is neergedaald. VTI biedt niet automatisch bescherming tegen VTI. Er moeten volledige routes worden toegevoegd om gelijke functionaliteit te waarborgen.

Configureren

Netwerkdiagram



Configuraties

Opmerking: Dit voorbeeld is niet geschikt voor het scenario waarin de ASA lid is van een onafhankelijk autonoom systeem en de BGP-prestaties met ISP-netwerken heeft. Het bestrijkt de topologie waar ASA twee onafhankelijke ISP banden met openbare adressen van verschillende autonome systemen heeft. In dat geval kan ISP anti-spoofing bescherming implementeren die controleert of de ontvangen pakketten niet zijn afgeleid van openbare IP die aan een andere ISP toebehoort. In deze situatie worden passende maatregelen genomen om dit te voorkomen.

1. Gemeenschappelijke encryptie- en authenticatieparameters. Informatie over aanbevolen cryptografische parameters is te vinden op: https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

Op beide ASA's:

```
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. Configuratie van het IPsec-profiel. Een van de partijen moet het initiatief nemen en je moet een responder zijn van de IKEv2-onderhandelingen:

ASA links:

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

ASA recht:

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

3. Schakel IKEv2-protocol in op beide ISP-interfaces.

Beide ASA's:

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

4. Configureer de voorgedeelde toets om de ASA's wederzijds te authentiseren:

ASA links:

```
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 *****
```

ASA recht:

```
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. Configuratie van de interfaces van ISP:

   ASA links:
```
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
!
```
   ASA recht:
```
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. De primaire verbinding is ISP A interface. ISP B is secundair. De primaire verbinding beschikbaarheid wordt gevolgd door gebruik van ICMP ping verzoek aan een gastheer in het internet, in dit voorbeeld gebruiken de ASA's elkaar interface van ISP A als ping bestemming:

   ASA links:
```
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
```
   ASA recht:
```
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. Het primaire VTI wordt altijd ingesteld via de secundaire VTI van ISP A. is ingesteld via ISP B. Statische routes naar tunnelbestemming zijn nodig. Dit waarborgt dat de versleutelde pakketten niet via de juiste fysieke interface worden verzonden om door ISP tegen spoofing gerichte druppels te voorkomen:

ASA links:

```
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
```

ASA recht:

```
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. VTI-configuratie:

ASA links:

```
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
```

ASA recht:

```
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. BGP-configuratie. De tunnel die bij ISP A is gekoppeld, is een primaire. Prefixes die over de tunnel worden geadverteerd die over ISP B wordt gevormd hebben een lagere lokale voorkeur, wat hen minder liever maakt door de routingtabel:

ASA links:

```
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
```

ASA recht:

```
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. (Optioneel) Om extra netwerk achter links ASA te adverteren dat er niet direct op is aangesloten, kan de statische routeherverdeling worden geconfigureerd:

    ASA links:

    ```
    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. (Optioneel) Het verkeer kan tussen de tunnels worden geladen op basis van de pakketbestemming. In dit voorbeeld wordt de route naar het 192.168.10.0/24 netwerk de voorkeur gegeven boven reservetunnel (ISP B tunnel)

    ASA links:

    ```
    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. Om te voorkomen dat het verkeer tussen sites als er tunnels uitvallen, in duidelijke tekst naar het internet wordt verstuurd, moeten er volledige routes worden toegevoegd. Alle RFC1918-adressen werden toegevoegd voor eenvoud:

    Beide ASA's:

    ```
    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. (Optioneel) Standaard wordt het ASA BGP-proces één keer per 60 seconden uitgevoerd. Als de aanhoudende respons 180 seconden lang niet van de peer wordt ontvangen, wordt hij dood verklaard. Om de detectie buurfout te versnellen kunt u BGP timers configureren. In dit voorbeeld worden de keepalives elke 10 seconden verstuurd en de buur wordt na 30 seconden gedeclareerd.

```
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
```

Verifiëren

Controleer of de IKEv2-tunnel is opgezet:

```
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
```

Controleer de BGP-buurtstatus:

```
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
```

Controleer de van BGP ontvangen routes. Routes die zijn gemarkeerd met ">" worden geïnstalleerd in de routingtabel:

```
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
```

Problemen oplossen

Debugs die zijn gebruikt voor het oplossen van IKEv2-protocol:

debug van crypto ikev2 - protocol 4
debug van crypto ikev2 - platform 4

Voor meer informatie over het oplossen van IKEv2-protocol:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

Voor meer informatie over het oplossen van problemen BGP-protocol:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Gerelateerde informatie

- BGP-regels voor routeselectie:
  https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- ASA BGP-configuratiehandleiding:
  https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Technische ondersteuning en documentatie – Cisco Systems