Configurazione delle interfacce ASA Virtual Tunnel in uno scenario con doppio ISP

Sommario

Introduzione

In questo documento viene descritto come configurare le VTI (Virtual Tunnel Interface) tra due appliance ASA (Adaptive Security Appliance) con il protocollo IKEv2 (Internet Key Exchange versione 2) per garantire una connettività sicura tra due branch. Entrambe le filiali dispongono di due collegamenti ISP per un'elevata disponibilità e il bilanciamento del carico. Il protocollo Border Gateway Protocol (BGP) viene stabilito sui tunnel per scambiare le informazioni di routing interno. Questa funzione è stata introdotta nell'appliance ASA versione 9.8(1). L'implementazione VTI ASA è compatibile con l'implementazione VTI disponibile sui router IOS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- protocollo BGP

Componenti usati

Le informazioni di questo documento si basano sui firewall ASAv con software 9.8(1)6.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Differenze tra VTI e mappa crittografica

- La mappa crittografica è una funzionalità di output dell'interfaccia. Per inviare il traffico attraverso il tunnel basato su mappa crittografica, il traffico deve essere indirizzato all'interfaccia con connessione Internet (tradizionalmente chiamata interfaccia esterna) e deve essere confrontato con un ACL crittografico. D'altra parte, VTI è un'interfaccia logica. Il tunnel verso ogni peer VPN è rappresentato da un VTI diverso. Se il routing punta verso la VTI, il pacchetto verrà crittografato e inviato al peer corrispondente.

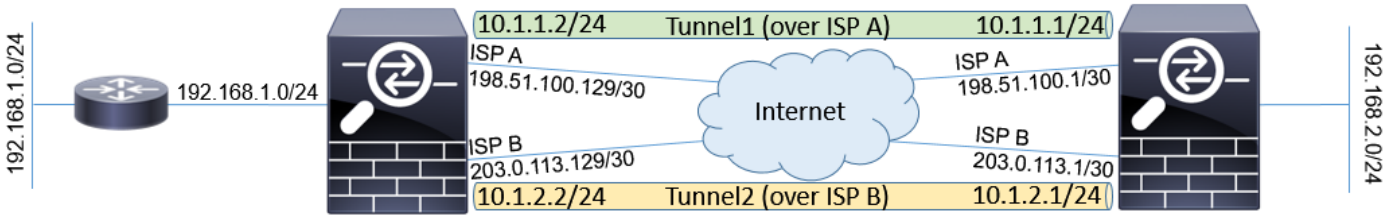
- Il VTI elimina la necessità di utilizzare gli elenchi degli accessi crittografati e le regole di esenzione NAT (Network Address Translation).

- L'elenco di controllo di accesso (ACL) delle mappe crittografiche non consente la sovrapposizione di voci. VTI è una VPN basata su route e al traffico VPN vengono applicate regole di routing regolari, che semplificano la configurazione e i processi di risoluzione dei problemi.

- La mappa crittografica impedisce automaticamente l'invio del traffico tra i siti in testo non crittografato se il tunnel non è attivo. VTI non protegge automaticamente da esso. È necessario aggiungere route null per garantire la stessa funzionalità.

Configurazione

Esempio di rete



Configurazioni

Nota: questo esempio non è adatto per uno scenario in cui l'ASA è un membro di un sistema autonomo indipendente e ha peer BGP con reti ISP. Copre la topologia in cui l'ASA ha due collegamenti ISP indipendenti con indirizzi pubblici di diversi sistemi autonomi. In questo caso, l'ISP può implementare una protezione anti-spoofing che verifica se i pacchetti ricevuti non provengono da un IP pubblico appartenente a un altro ISP. In questa configurazione, vengono adottate le misure appropriate per evitare questa condizione.

1. Parametri comuni di crittografia e autenticazione. Per informazioni sui parametri di crittografia consigliati, visitare il sito Web all'indirizzo: https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

   Su entrambe le appliance 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. Configurare il profilo IPSec. Una delle parti deve essere l'iniziatore e l'altra deve rispondere alla negoziazione IKEv2:

   ASA sinistra:

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

   Diritto ASA:

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

3. Abilitare il protocollo IKEv2 su entrambe le interfacce ISP.

   Entrambe le appliance ASA:

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

4. Configurare la chiave già condivisa per l'autenticazione reciproca delle appliance ASA:

   ASA sinistra:

```
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 *****
```

   Diritto 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. Configurare le interfacce ISP:

   ASA sinistra:
   ```
   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
   !
   ```
   Diritto 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. Il collegamento primario è l'interfaccia ISP A. L'ISP B è secondario. La disponibilità del collegamento primario viene rilevata quando si invia una richiesta ping ICMP a un host su Internet. Nell'esempio, le appliance ASA usano le altre interfacce ISP-A come destinazione del ping:

   ASA sinistra:
   ```
   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
   ```
   Diritto 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 primaria viene sempre stabilita sull'ISP A. La VTI secondaria viene stabilita sull'ISP B. Sono necessari percorsi statici verso la destinazione del tunnel. In questo modo, i pacchetti crittografati vengono lasciati dall'interfaccia fisica corretta per evitare che l'ISP perda la protezione contro lo spoofing:

   ASA sinistra:

```
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
```

Diritto 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. Configurazione VTI:

ASA sinistra:

```
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
```

Diritto 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. Configurazione BGP. Il tunnel associato all'ISP A è un server primario. I prefissi annunciati sul tunnel formato sull'ISP B hanno una preferenza locale inferiore, che li rende meno preferiti dalla tabella di routing:

ASA sinistra:

```
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
```

Diritto 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. (Facoltativo) Per annunciare una rete aggiuntiva dietro l'appliance ASA sinistra che non è collegata direttamente ad essa, è possibile configurare la ridistribuzione statica del percorso:

    ASA sinistra:

    ```
    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. (Facoltativo) Il traffico può essere bilanciato in base al carico tra i tunnel in base alla destinazione del pacchetto. Nell'esempio, il percorso verso la rete 192.168.10.0/24 è preferito al tunnel di backup (tunnel ISP B)

    ASA sinistra:

    ```
    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. Per evitare che il traffico tra i siti venga inviato in testo non crittografato a Internet se i tunnel non sono attivi, è necessario aggiungere route Null. Tutti gli indirizzi RFC1918 sono stati aggiunti per semplicità:

    Entrambe le appliance 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. (Facoltativo) Per impostazione predefinita, il processo ASA BGP invia pacchetti keepalive una volta ogni 60 secondi. Se la risposta keepalive non viene ricevuta dal peer per 180 secondi, viene dichiarata inattiva. Per velocizzare il rilevamento degli errori dei router adiacenti, è possibile configurare i timer BGP. Nell'esempio, i pacchetti keepalive vengono inviati ogni 10 secondi e i pacchetti adiacenti vengono dichiarati inattivi dopo 30 secondi.

```
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
```

Verifica

Verificare se il tunnel IKEv2 è attivo:

```
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
```

Verificare lo stato di vicinato 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
```

Verificare le route ricevute da BGP. Le route contrassegnate con "**>**" vengono installate nella tabella di routing:

```
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
```

Risoluzione dei problemi

Debug utilizzati per risolvere i problemi relativi al protocollo IKEv2:

```
debug crypto ikev2 protocol 4
debug crypto ikev2 platform 4
```

Per ulteriori informazioni sulla risoluzione dei problemi relativi al protocollo IKEv2: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

Per ulteriori informazioni sulla risoluzione dei problemi relativi al protocollo BGP: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Informazioni correlate

- Regole di selezione route BGP: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- Guida alla configurazione di ASA BGP: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Documentazione e supporto tecnico – Cisco Systems