Konfigurieren von ASA Virtual Tunnel-Schnittstellen in Dual ISP-Szenario

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie VTI (Virtual Tunnel Interfaces) zwischen zwei ASAs (Adaptive Security Appliances) mithilfe des IKEv2 (Internet Key Exchange Version 2)-Protokolls konfiguriert werden, um sichere Verbindungen zwischen zwei Zweigstellen zu ermöglichen. Beide Zweigstellen verfügen über zwei ISP-Verbindungen, um hohe Verfügbarkeit und Load Balancing zu ermöglichen. Die Border Gateway Protocol (BGP)-Nachbarschaft wird über die Tunnel eingerichtet, um interne Routing-Informationen auszutauschen.
Diese Funktion wurde in ASA Version 9.8(1) eingeführt. Die ASA VTI-Implementierung ist mit der VTI-Implementierung kompatibel, die auf IOS-Routern verfügbar ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- BGP-Protokoll

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf ASAv-Firewalls mit der Softwareversion 9.8(1)6.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Unterschiede zwischen VTI und Crypto Map

- Crypto Map ist eine Ausgabefunktion der Schnittstelle. Um den Datenverkehr über einen auf der Crypto Map basierenden Tunnel zu senden, muss der Datenverkehr an die Schnittstelle mit Internetanbindung (üblicherweise als externe Schnittstelle bezeichnet) weitergeleitet und mit der Crypto ACL abgeglichen werden. Andererseits ist VTI eine logische Schnittstelle. Tunnel zu jedem VPN-Peer wird durch ein anderes VTI dargestellt. Wenn das Routing auf VTI zeigt, wird das Paket verschlüsselt und an den entsprechenden Peer gesendet.

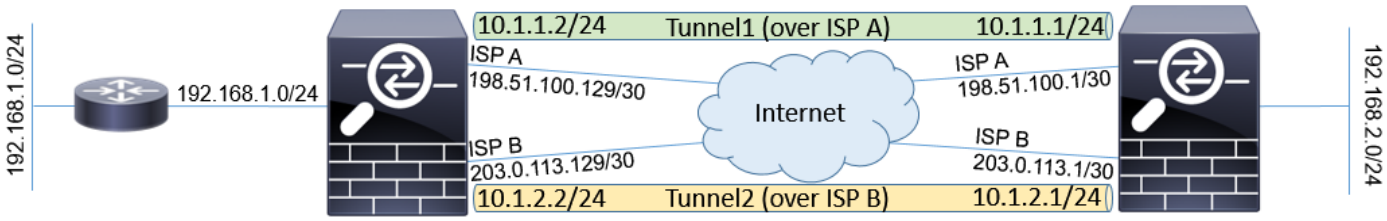
- VTI macht die Verwendung von Crypto Access-Listen und NAT-Befreiungsregeln (Network Address Translation) überflüssig.

- Die Zugriffskontrollliste (ACL, Crypto Map Access Control List) erlaubt keine überlappenden Einträge. VTI ist ein routen-basiertes VPN, und für den VPN-Datenverkehr gelten reguläre Routing-Regeln, was die Konfiguration und die Prozesse zur Fehlerbehebung vereinfacht.

- Die Crypto Map verhindert automatisch, dass Datenverkehr zwischen Standorten im Klartext gesendet wird, wenn der Tunnel ausgefallen ist. VTI schützt nicht automatisch davor. Null-Routen müssen hinzugefügt werden, um die gleiche Funktionalität zu gewährleisten.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Hinweis: Dieses Beispiel eignet sich nicht für Szenarien, in denen die ASA Mitglied eines unabhängigen autonomen Systems ist und BGP-Peers mit ISP-Netzwerken hat. Sie deckt die Topologie ab, in der ASA über zwei unabhängige ISP-Verbindungen mit öffentlichen Adressen verschiedener autonomer Systeme verfügt. In diesem Fall kann der ISP Anti-Spoofing-Schutz bereitstellen, der überprüft, ob die empfangenen Pakete nicht von einer öffentlichen IP stammen, die zu einem anderen ISP gehört. In dieser Konfiguration werden geeignete Maßnahmen ergriffen, um dies zu verhindern.

1. Gemeinsame Verschlüsselungs- und Authentifizierungsparameter. Informationen zu empfohlenen kryptografischen Parametern finden Sie unter:

https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

Auf beiden ASAs:

```
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. Konfigurieren Sie das IPsec-Profil. Eine der Seiten muss Initiator sein und eine Antwort auf die IKEv2-Aushandlung sein:

ASA links:

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

ASA rechts:

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

3. Aktivieren Sie das IKEv2-Protokoll auf beiden ISP-Schnittstellen.

Beide ASAs:

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

4. Konfigurieren Sie den Pre-Shared Key, um die ASAs gegenseitig zu authentifizieren:

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 rechts:

```
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. Konfigurieren Sie die ISP-Schnittstellen:

   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 rechts:
```
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. Die primäre Verbindung ist die ISP-A-Schnittstelle. ISP B ist sekundär. Die Verfügbarkeit der primären Verbindung wird mithilfe einer ICMP-Ping-Anfrage an einen Host im Internet nachverfolgt. In diesem Beispiel verwenden die ASAs die andere ISP-A-Schnittstelle als Ping-Ziel:

   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 rechts:
```
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. Das primäre VTI wird immer über den ISP A eingerichtet. Über ISP B wird ein sekundäres VTI eingerichtet. Statische Routen zum Tunnelziel sind erforderlich. Dadurch wird sichergestellt, dass die verschlüsselten Pakete von der richtigen physischen Schnittstelle

ausgehen, um Verwerfen von Anti-Spoofing-Angriffen durch den ISP zu vermeiden:

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 rechts:

```
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-Konfiguration:

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 rechts:

```
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-Konfiguration. Der dem ISP A zugeordnete Tunnel ist ein primäres. Präfixe, die über den über ISP B gebildeten Tunnel angekündigt werden, weisen eine niedrigere lokale Präferenz auf, was sie von der Routing-Tabelle weniger bevorzugt:

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 rechts:

```
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. (Optional) Um weitere, hinter der linken ASA verborgene Netzwerke anzukündigen, die nicht direkt mit ihr verbunden sind, kann die statische Weiterverteilung konfiguriert werden:

    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. (Optional) Je nach Paketziel kann ein Lastenausgleich für den Datenverkehr zwischen den Tunneln erfolgen. In diesem Beispiel wird die Route zum Netzwerk 192.168.10.0/24 gegenüber dem Backup-Tunnel (ISP B-Tunnel) bevorzugt.

    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. Um zu verhindern, dass Datenverkehr zwischen Standorten im Klartext an das Internet gesendet wird, wenn Tunnel ausfallen, müssen Null-Routen hinzugefügt werden. Alle RFC1918-Adressen wurden zur Vereinfachung hinzugefügt:

    Beide ASAs:

    ```
    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. (Optional) Standardmäßig sendet der ASA-BGP-Prozess Keepalives einmal pro 60 Sekunden. Wenn die Keepalive-Antwort 180 Sekunden lang nicht vom Peer empfangen wird, wird sie für tot erklärt. Um den Nachbar-Fehler zu beschleunigen, können Sie BGP-Timer konfigurieren. In diesem Beispiel werden die Keepalives alle 10 Sekunden gesendet, und der Nachbar wird nach 30 Sekunden deklariert.

```
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
```

Überprüfen

Überprüfen Sie, ob der IKEv2-Tunnel aktiv ist:

```
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
```

BGP-Nachbarschaftsstatus überprüfen:

```
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
```

Überprüfen der vom BGP empfangenen Routen Die mit ">" gekennzeichneten Routen werden in der Routing-Tabelle installiert:

```
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
```

Fehlerbehebung

Debugger zur Fehlerbehebung für das IKEv2-Protokoll:

debuggen crypto ikev2 protocol 4
debuggen crypto ikev2 plattform 4

Weitere Informationen zur Fehlerbehebung für das IKEv2-Protokoll finden Sie unter: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

Weitere Informationen zur Fehlerbehebung im BGP-Protokoll finden Sie unter: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Zugehörige Informationen

- BGP-Routenauswahlregeln: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- ASA BGP-Konfigurationsleitfaden: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Technischer Support und Dokumentation - Cisco Systems