ASR 1000 encryptie via OTV Unicast configureren

Inhoud

Inleiding

Dit document beschrijft de basisverzameling configuraties die worden gebruikt om OTV-virtualisatie (Overlay Transport Virtualization) op te zetten met IPSec-encryptie. Voor versleuteling via OTV hebt u geen extra configuraties nodig van de OTV-kant. U hoeft alleen maar te begrijpen hoe OTV en IPSEC naast elkaar bestaan.

Om encryptie via OTV toe te voegen, moet u een Encapsulating Security Payload (ESP)-header bovenop OTV PDU toevoegen. U kunt encryptie op de ASR 1000 Edge-apparaten (ED) op twee manieren realiseren: (i) IPSec (ii) GETVPN.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASR 1000 routers voor Edge-apparaten (ED)
- Core (ISP Cloud)
- Catalyst 2960-switches als de toegangsswitch op één van beide locaties

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.

Achtergrondinformatie

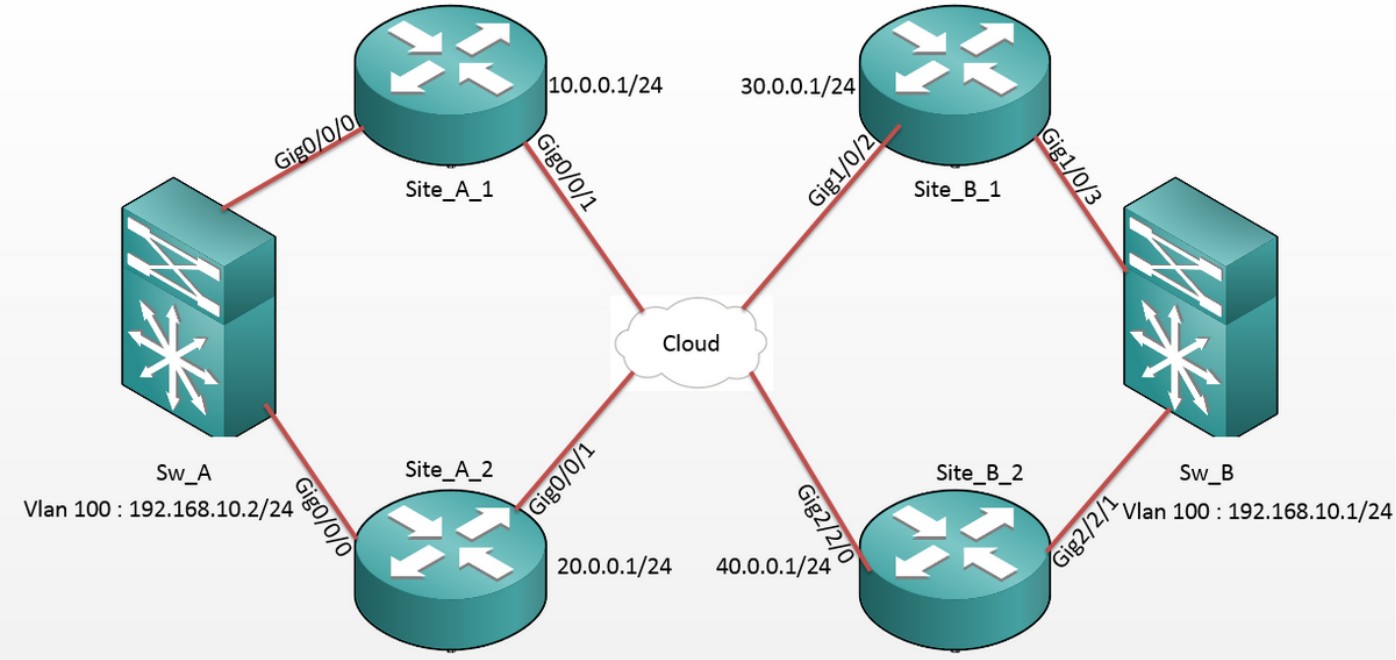
De basisfuncties en de configuraties van OTV worden geacht bekend te zijn bij de gebruikers van dit document.

U kunt deze documenten ook voor hetzelfde gebruiken:

- Configuratie OTV Unicast
- Configuratie OTV-multicast

Configureren

Netwerkdiagram



Configuraties

Site A: ED-configuraties:

```
Site_A_1#show run
Building configuration...
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
crypto isakmp policy 10
 hash md5
 authentication pre-share
```

```
Site_A_2#show run
Building configuration...
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
crypto isakmp policy 10
 hash md5
 authentication pre-share
```

```
crypto isakmp key cisco address 30.0.0.1
crypto isakmp key cisco address 40.0.0.1
!
crypto ipsec transform-set tset esp-aes
esp-md5-hmac
 mode tunnel
!
crypto map cmap 1 ipsec-isakmp
 set peer 30.0.0.1
 set transform-set tset
 match address cryptoacl
crypto map cmap 3 ipsec-isakmp
 set peer 40.0.0.1
 set transform-set tset
 match address cryptoacl3
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/1
 otv adjacency-server unicast-only
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 no ip address
service instance 99 ethernet
 encapsulation dot1q 99
```

```
crypto isakmp key cisco address 30.0.0.1
crypto isakmp key cisco address 40.0.0.1
!
crypto ipsec transform-set tset esp-aes
esp-md5-hmac
 mode tunnel
!
crypto map cmap 2 ipsec-isakmp
 set peer 30.0.0.1
 set transform-set tset
 match address cryptoacl2
crypto map cmap 3 ipsec-isakmp
 set peer 40.0.0.1
 set transform-set tset
 match address cryptoacl3
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/1
 otv use-adjacency-server 10.0.0.1 30.0.0.1
unicast-only
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 no ip address
service instance 99 ethernet
```

```
 bridge-domain 99
 !
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
 crypto map cmap
!
ip access-list extended cryptoacl
 permit gre host 10.0.0.1 host 30.0.0.1
ip access-list extended cryptoacl3
 permit gre host 10.0.0.1 host 40.0.0.1
```

```
 encapsulation dot1q 99
 bridge-domain 99
 !
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet0/0/1
 ip address 20.0.0.1 255.255.255.0
 crypto map cmap
!
ip access-list extended cryptoacl2
 permit gre host 20.0.0.1 host 30.0.0.1
ip access-list extended cryptoacl3
 permit gre host 20.0.0.1 host 40.0.0.1
```

Site B: ED-configuraties:

```
Site_B_1#sh run
Building configuration...
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco address 10.0.0.1
crypto isakmp key cisco address 20.0.0.1
```

```
Site_B_2#sh run
Building configuration...
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco address 10.0.0.1
crypto isakmp key cisco address 20.0.0.1
```

```
!
crypto ipsec transform-set tset esp-aes esp-md5-hmac
 mode tunnel
!
crypto map cmap 1 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set tset
 match address cryptoacl
crypto map cmap 2 ipsec-isakmp
 set peer 20.0.0.1
 set transform-set tset
 match address cryptoacl2
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/2
 otv use-adjacency-server 10.0.0.1 unicast-only
 otv adjacency-server unicast-only
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet1/0/3
 no ip address
service instance 99 ethernet
 encapsulation dot1q 99
```

```
!
crypto ipsec transform-set tset esp-aes esp-md5-hmac
 mode tunnel
!
crypto map cmap 1 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set tset
 match address cryptoacl
crypto map cmap 2 ipsec-isakmp
 set peer 20.0.0.1
 set transform-set tset
 match address cryptoacl2
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet2/2/0
 otv use-adjacency-server 10.0.0.1 30.0.0.1 unicast-only
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet2/2/1
 no ip address
 service instance 99 ethernet
 encapsulation dot1q 99
 bridge-domain 99
```

```
 bridge-domain 99
 !
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet1/0/2
 ip address 30.0.0.1 255.255.255.0
crypto map cmap
!
ip access-list extended cryptoacl
 permit gre host 30.0.0.1 host 10.0.0.1
ip access-list extended cryptoacl2
 permit gre host 30.0.0.1 host 20.0.0.1
```

```
 !
 service instance 100 ethernet
 encapsulation dot1q 100
 bridge-domain 100
 !
 service instance 101 ethernet
 encapsulation dot1q 101
 bridge-domain 101
 !
!
interface GigabitEthernet2/2/0
 ip address 40.0.0.1 255.255.255.0
 crypto map cmap
!
ip access-list extended cryptoacl
 permit gre host 40.0.0.1 host 10.0.0.1
ip access-list extended cryptoacl2
 permit gre host 40.0.0.1 host 20.0.0.1
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Controleer of het MAC-adres van de interne VLAN-host (in dit geval de SVI op de Catalyst-schakelaar van 2960) op de OTV-routetabellen is geleerd.
2. Controleer of de crypto-encap's en decap worden uitgevoerd voor het Overlay-verkeer (OTV-verkeer).

Zodra de OTV omhoog komt nadat u de crypto kaart op de verenigingsinterface vormt, controleer de actieve expediteur voor de lokale VLAN (in dit geval VLAN 100 en 101). Dit toont aan dat Site_A_1 en Site_B_2 de actieve expediteurs voor de zelfs VLAN's zijn aangezien u de verkeersencryptie voor pings zal testen die van VLAN 100 op Site A tot VLAN 100 op Site B wordt geïnitieerd:

```
Site_A_1#show otv vlan

Key:  SI - Service Instance, NA - Non AED, NFC - Not Forward Capable.
```

```
Overlay 99 VLAN Configuration Information

 Inst VLAN BD   Auth ED             State                Site If(s)

 0    100  100  *Site_A_1           active               Gi0/0/0:SI100

 0    101  101   Site_A_2           inactive(NA)         Gi0/0/0:SI101

 0    200  200  *Site_A_1           active               Gi0/0/0:SI200

 0    201  201   Site_A_2           inactive(NA)         Gi0/0/0:SI201

 Total VLAN(s): 4

Site_B_2#show otv vlan

Key:  SI - Service Instance, NA - Non AED, NFC - Not Forward Capable.


Overlay 99 VLAN Configuration Information

 Inst VLAN BD   Auth ED             State                Site If(s)

0    100  100  *Site_B_2           active               Gi2/2/1:SI100

 0    101  101   Site_B_1           inactive(NA)         Gi2/2/1:SI101

 0    200  200  *Site_B_2           active               Gi2/2/1:SI200

 0    201  201   Site_B_1           inactive(NA)         Gi2/2/1:SI201

 Total VLAN(s): 4
```

Om te controleren of de pakketten inderdaad ingekapseld en gedecapsuleerd worden op één van beiden ED, zou u moeten controleren of de IPSec sessie actief is en de tegenwaarden in de crypto sessies om te bevestigen dat de pakketten inderdaad versleuteld en gedecrypteerd worden. Om te controleren of de IPSec-sessie actief is, aangezien deze alleen actief wordt als er verkeer doorheen stroomt, controleert u de uitvoer van **showcrypto isakmp als**. Hier worden alleen de uitgangen voor de actieve expediteurs gecontroleerd, maar dit zou de actieve status op alle ED's voor OTV over encryptie moeten tonen om te werken.

```
Site_A_1#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst             src             state          conn-id status

10.0.0.1        30.0.0.1        QM_IDLE           1008 ACTIVE

10.0.0.1        40.0.0.1        QM_IDLE           1007 ACTIVE

Site_B_2#sh crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst             src             state          conn-id status

20.0.0.1        40.0.0.1        QM_IDLE           1007 ACTIVE

10.0.0.1        40.0.0.1        QM_IDLE           1006 ACTIVE
```

Om te bevestigen of de pakketten versleuteld en gedecrypteerd worden, moet u eerst weten wat te verwachten in de uitgangen van **show crypto sessiedetails**. Wanneer u het ICMP-echopakket start van de Sw_A-schakelaar naar de Sw_B, wordt dit verwacht:

- Terwijl de ICMP-echo vertrekt van de Site_A_1 ED, die de actieve expediteur voor VLAN 100 is, moet deze de OTV-lading insluiten (ICMP Echo + MPLS + GRE)
- Wanneer de ICMP-echo de Site_B_2 ED bereikt, die de actieve expediteur voor VLAN 100 is, moet deze de OTV-lading (ICMP Echo + MPLS + GRE) decapsuleren
- Wanneer de Site_B_2 ED het ICMP Echo-antwoord van Sw_B ontvangt, moet deze de OTV-lading opnieuw inkapselen (ICMP Echo + MPLS + GRE)
- En zodra het ICMP Echo-antwoord de Site_A_1 ED bereikt zou ik de OTV-lading opnieuw moeten **decapsulseren** (ICMP Echo + MPLS + GRE)

Verwacht na de succesvolle pings van Sw_A tot Sw_B, een toename van 5 tellers onder "enc" en "dec" deel van de **show crypto sessiedetails** op zowel de actieve Fed's te zien.

Controleer dit nu ook bij de ED's:

```
Site_A_1(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

       Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/3345

       Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) 4607998/3291 <<<< 10 counter before ping

Site_A_1(config-if)#do show crypto session detail | section dec

       Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4608000/3343

       Inbound:  #pkts dec'ed 18 drop 0 life (KB/Sec) 4607997/3289 <<<< 18 counter before ping

Site_B_2(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

       Outbound: #pkts enc'ed 18 drop 0 life (KB/Sec) 4607997/3295 <<<< 18 counter before ping

       Outbound: #pkts enc'ed 9 drop 0 life (KB/Sec) 4607999/3295

Site_B_2(config-if)#do show crypto session detail | section dec

       Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) 4607998/3293 <<<< 10 counter before ping

       Inbound:  #pkts dec'ed 1 drop 0 life (KB/Sec) 4607999/3293

Sw_A(config)#do ping 192.168.10.1 source vlan 100


Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.10.2

!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/10 ms

Sw_A(config)#

Site_A_1(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

       Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/3339

       Outbound: #pkts enc'ed 15 drop 0 life (KB/Sec) 4607997/3284 <<<< 15 counter after ping
(After ICMP Echo)

Site_A_1(config-if)#do show crypto session detail | section dec

       Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 4608000/3338

       Inbound:  #pkts dec'ed 23 drop 0 life (KB/Sec) 4607997/3283 <<<< 23 counter after ping
(After ICMP Echo Reply)

Site_B_2(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

       Outbound: #pkts enc'ed 23 drop 0 life (KB/Sec) 4607997/3282 <<<< 23 counter after ping
(After ICMP Echo Reply)

       Outbound: #pkts enc'ed 9 drop 0 life (KB/Sec) 4607999/3282

Site_B_2(config-if)#do show crypto session detail | section dec

       Inbound:  #pkts dec'ed 15 drop 0 life (KB/Sec) 4607997/3281 <<<< 15 counter after ping
(After ICMP Echo)

       Inbound:  #pkts dec'ed 1 drop 0 life (KB/Sec) 4607999/3281
```

Deze configuratiehandleiding kan de vereiste configuratiegegevens met het gebruik van IPSec voor de Unicast kern dubbele homed instelling overbrengen.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.