Konfigurieren der ASR1000-Verschlüsselung über OTV Unicast

Inhalt

Einführung

Dieses Dokument beschreibt die grundlegenden Konfigurationssätze, mit denen die Overlay Transport Virtualization (OTV) mit IPSec-Verschlüsselung aufgerufen wird. Für die Verschlüsselung über OTV sind keine zusätzlichen Konfigurationen vom OTV-Ende erforderlich. Sie müssen nur verstehen, wie OTV und IPSEC gleichzeitig existieren.

Um die Verschlüsselung über OTV hinzuzufügen, müssen Sie zusätzlich zur OTV PDU einen ESP-Header (Encapsulating Security Payload) hinzufügen. Für die ASR1000 Edge Devices (ED) kann eine Verschlüsselung auf zwei Arten erfolgen: (i) IPSec (ii) GETVPN.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASR1000 Router für Edge-Geräte (ED)
- Core (ISP Cloud)
- Catalyst 2960 Switches als Access Switch an beiden Standorten

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.

Hintergrundinformationen

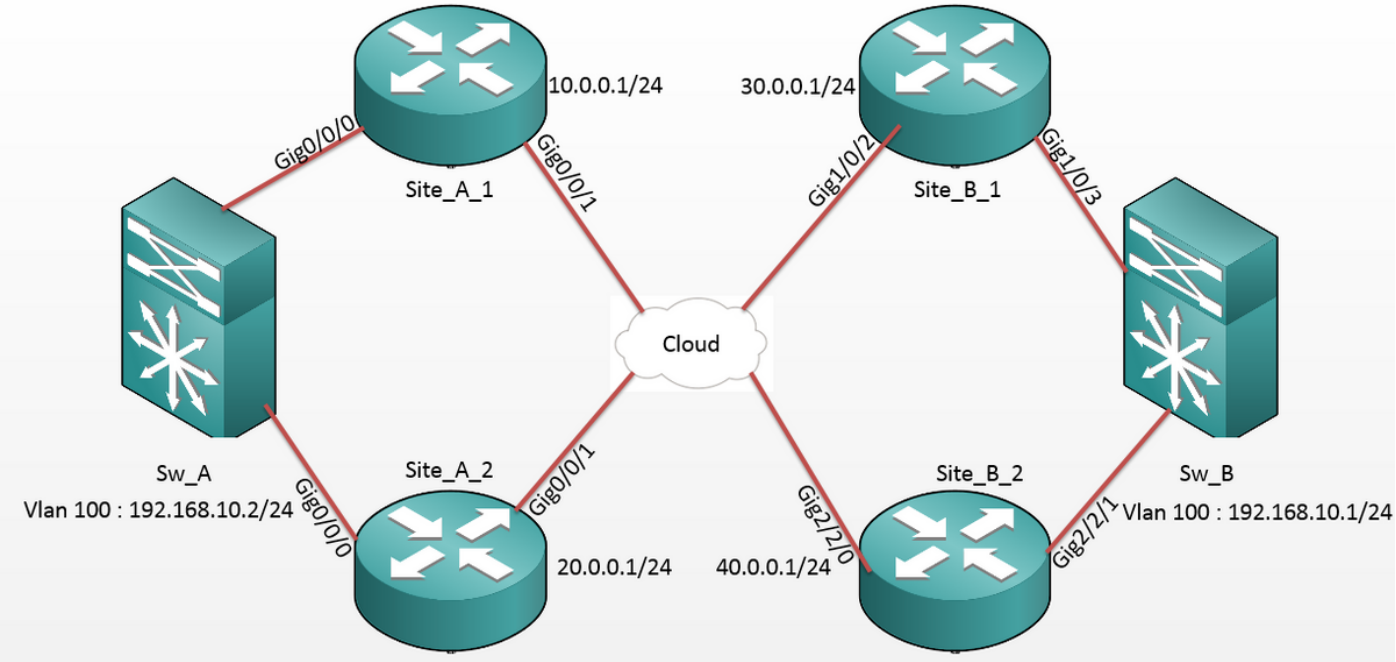
Es wird davon ausgegangen, dass die Benutzer dieses Dokuments über die grundlegenden Funktionen und Konfigurationen von OTV Bescheid wissen.

Sie können auch die folgenden Dokumente für die gleiche Weise befolgen:

- OTV-Unicast-Konfiguration
- OTV-Multicast-Konfiguration

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Standort A: ED-Konfigurationen:

```
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
```

Standort B: ED-Konfigurationen:

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Überprüfen Sie, ob die MAC-Adresse des internen VLAN-Hosts (in diesem Fall die SVI auf den Catalyst-Switches der Serie 2960) in den OTV-Routing-Tabellen erfasst wurde.
2. Überprüfen Sie, ob die Verschlüsselungsverschlüsse und die Decap-Dateien für den Overlay (OTV-Datenverkehr)-Datenverkehr ausgeführt werden.

Wenn das OTV nach der Konfiguration der Crypto Map auf der Join-Schnittstelle aktiviert ist, überprüfen Sie den aktiven Forwarder für die lokalen VLANs (in diesem Fall VLAN 100 und 101). Dies zeigt, dass Site_A_1 und Site_B_2 die aktiven Forwarder für die selbst erstellten VLANs sind, da Sie die Datenverkehrsverschlüsselung für Pings testen, die von VLAN 100 auf Site A bis VLAN 100 auf Site B initiiert wurden:

```
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
```

Um zu überprüfen, ob die Pakete tatsächlich auf einem der ED-Geräte gekapselt und entkapselt werden, sollten Sie überprüfen, ob die IPSec-Sitzung aktiv ist und ob die Zählerwerte in den Krypto-Sitzungen vorhanden sind, um sicherzustellen, dass die Pakete tatsächlich verschlüsselt und entschlüsselt werden. Um zu überprüfen, ob die IPSec-Sitzung aktiv ist, da sie nur aktiviert wird, wenn ein Datenverkehr durchfließt, überprüfen Sie die Ausgabe von **show crypto isakmp sa**. Hier werden nur die Ausgänge für die aktiven Forwarder überprüft. Dies sollte jedoch den aktiven Status auf allen EDs anzeigen, damit OTV over Encryption funktioniert.

```
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
```

Um zu überprüfen, ob die Pakete verschlüsselt und entschlüsselt werden, müssen Sie zunächst wissen, was in den Ausgaben der **Anzeige** der **Verschlüsselungssitzungsdetails** zu erwarten ist. Wenn Sie also das ICMP-Echo-Paket vom Sw_A-Switch zum Sw_B initiieren, wird Folgendes erwartet:

- Das ICMP-Echo verlässt den Standort_A_1 ED, der der aktive Forwarder für das VLAN 100 ist, jedoch muss die OTV-Payload gekapselt werden (ICMP-Echo + MPLS + GRE).
- Sobald das ICMP-Echo den Standort_B_2 ED erreicht hat, der der aktive Forwarder für VLAN 100 ist, muss die OTV-Nutzlast entkapselt werden (ICMP Echo + MPLS + GRE).
- Wenn der Standort_B_2 ED die ICMP-Echo-Antwort von Sw_B erhält, muss er die OTV-Payload erneut kapseln (ICMP Echo + MPLS + GRE).
- Sobald die ICMP-Echo-Antwort den Standort_A_1 ED erreicht hat, muss ich erneut die OTV-Payload **entkapseln** (ICMP-Echo + MPLS + GRE).

Erwarten Sie nach den erfolgreichen Pings von Sw_A nach Sw_B, dass im Abschnitt "Enc" (Verschlüsseln) und "dec" (Dezimalstellen) der **Ausgabe** von **Verschlüsselungssitzungsdetails** auf beiden aktiven Weiterleitungs-EDs eine Erhöhung von 5 Zählern angezeigt wird.

Jetzt prüfen Sie das Gleiche über die LEDs:

```
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
```

Dieser Konfigurationsleitfaden kann die erforderlichen Konfigurationsdetails mithilfe von IPSec für die Dual-Homed-Einrichtung des Unicast-Core-Kerns vermitteln.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.