Configurazione della crittografia ASR1000 su OTV Unicast

Sommario

Introduzione

In questo documento viene descritto il set di configurazioni di base utilizzato per attivare Overlay Transport Virtualization (OTV) con crittografia IPSec. La crittografia su OTV non richiede ulteriori configurazioni dall'estremità OTV. È sufficiente comprendere la coesistenza di OTV e IPSEC.

Per aggiungere la crittografia su OTV, è necessario aggiungere un'intestazione ESP (Encapsulating Security Payload) sopra la PDU OTV. È possibile ottenere la crittografia su ASR1000 Edge Devices (ED) in due modi: (i) IPSec (ii) GETVPN.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASR 1000 router per dispositivi Edge (ED)
- Core (ISP Cloud)
- Switch Catalyst 2960 come switch di accesso su entrambi i siti

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.

Premesse

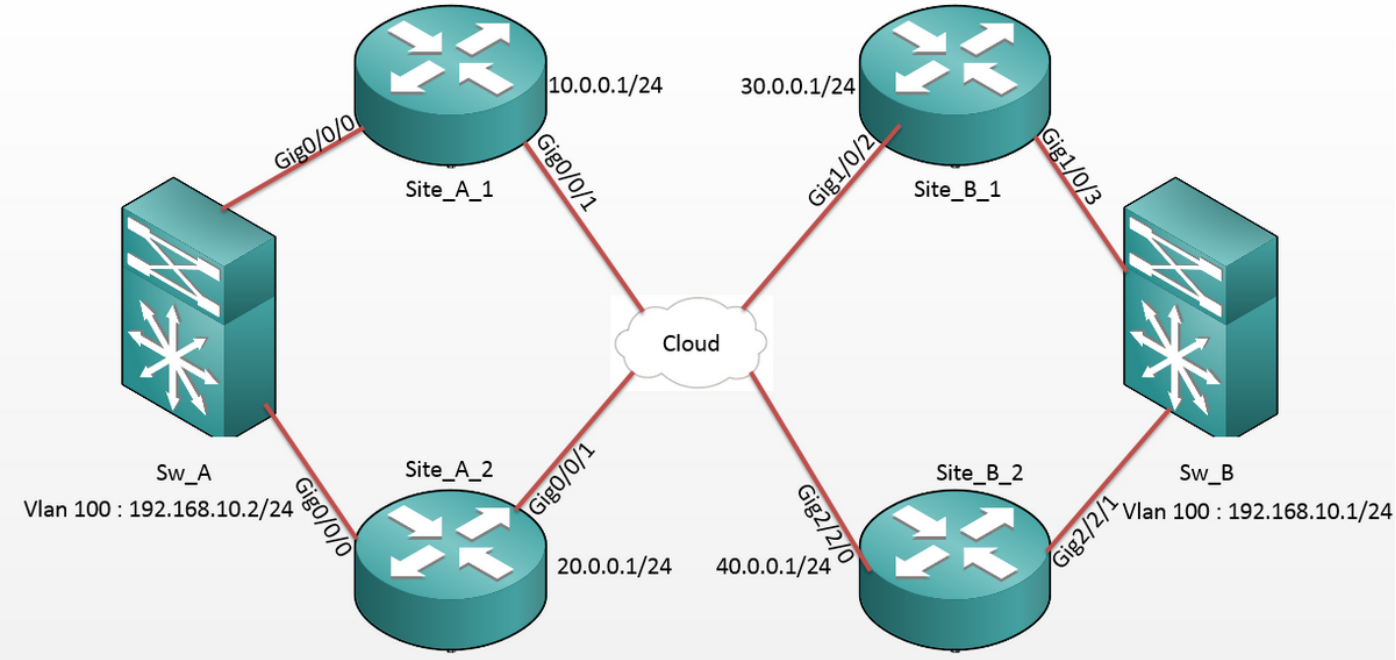
Si presume che gli utenti di questo documento conoscano le funzionalità e le configurazioni di base di OTV.

Allo stesso modo, è possibile seguire i seguenti documenti:

- Configurazione unicast OTV
- Configurazione multicast OTV

Configurazione

Esempio di rete



Configurazioni

Sito A: Configurazioni ED:

```
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
```

Sito B: Configurazioni ED:

```
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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Verificare che l'indirizzo MAC dell'host VLAN interno (in questo caso la SVI sullo switch Catalyst 2960) sia stato appreso sulle tabelle di routing OTV.
2. Verificare se la crittografia e il decap sono eseguiti per il traffico di overlay (traffico OTV).

Dopo aver configurato la mappa crittografica sull'interfaccia di join, l'OTV torna a funzionare, quindi controllare il server d'inoltro attivo per le VLAN locali (in questo caso le VLAN 100 e 101). Ciò mostra che il sito A_1 e il sito B_2 sono i server d'inoltro attivi per le VLAN pari, in quanto è possibile testare la crittografia del traffico per i ping avviati dalla VLAN 100 sul sito A alla VLAN 100 sul sito B:

```
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
```

Per verificare se i pacchetti vengono effettivamente incapsulati e decapsulati su uno dei dispositivi ED, verificare che la sessione IPSec sia attiva e che i valori dei contatori nelle sessioni crittografiche confermino che i pacchetti vengano effettivamente crittografati e decriptati. Per verificare se la sessione IPSec è attiva, in quanto diventa attiva solo se vi è traffico in transito, controllare l'output del comando **show crypto isakmp sa**. In questo caso, vengono controllati solo gli output per i server d'inoltro attivi, ma questo dovrebbe mostrare lo stato attivo su tutti gli ED affinché la crittografia OTV sia efficace.

```
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
```

Ora, per confermare se i pacchetti vengono crittografati e decriptati, è necessario sapere cosa

aspettarsi nei risultati del **comando show crypto session detail**. Quindi, quando si avvia il pacchetto echo ICMP dallo switch Sw_A al software Sw_B, è necessario:

- Mentre l'eco ICMP abbandona il sito A_1 ED, il server d'inoltro attivo per la VLAN 100, dovrà incapsulare il payload OTV (ICMP Echo + MPLS + GRE)
- Quindi, quando l'eco ICMP raggiunge il sito B_2 ED, il mittente attivo per la VLAN 100, deve decapsulare il payload OTV (ICMP Echo + MPLS + GRE)
- Ora, una volta che il sito B_2 ED riceve la risposta echo ICMP dal sito Sw_B, dovrebbe incapsulare nuovamente il payload OTV (ICMP Echo + MPLS + GRE)
- E una volta che la risposta echo ICMP raggiunge il sito A_1 ED, dovrò **decapsulare** di **nuovo** il payload OTV (ICMP Echo + MPLS + GRE)

Dopo aver eseguito correttamente i ping da Sw_A a Sw_B, prevedere un incremento di 5 contatori nelle sezioni "enc" e "dec" dell'output **show crypto session detail** su entrambi gli ED di inoltro attivi.

Ora, provate a fare lo stesso dai ED:

```
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
```

Questa guida alla configurazione è in grado di fornire i dettagli di configurazione richiesti utilizzando IPSec per l'installazione dual-homed di base Unicast.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.