Configurer le chiffrement ASR1000 sur monodiffusion OTV

Contenu

Introduction

Ce document décrit l'ensemble de configurations de base utilisées pour activer Overlay Transport Virtualization (OTV) avec le chiffrement IPSec. Le chiffrement sur OTV ne nécessite aucune configuration supplémentaire de l'extrémité OTV. Il vous suffit de comprendre comment OTV et IPSEC coexistent.

Pour ajouter le chiffrement sur OTV, vous devez ajouter un en-tête ESP (Encapsulating Security Payload) au-dessus de l'unité de données de protocole OTV. Vous pouvez réaliser le chiffrement sur les périphériques Edge ASR1000 (ED) de deux manières : i) IPSec ii) GETVPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs ASR1000 pour périphériques Edge (ED)
- Noyau (cloud ISP)
- Commutateurs Catalyst 2960 comme commutateur d'accès sur l'un ou l'autre site

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

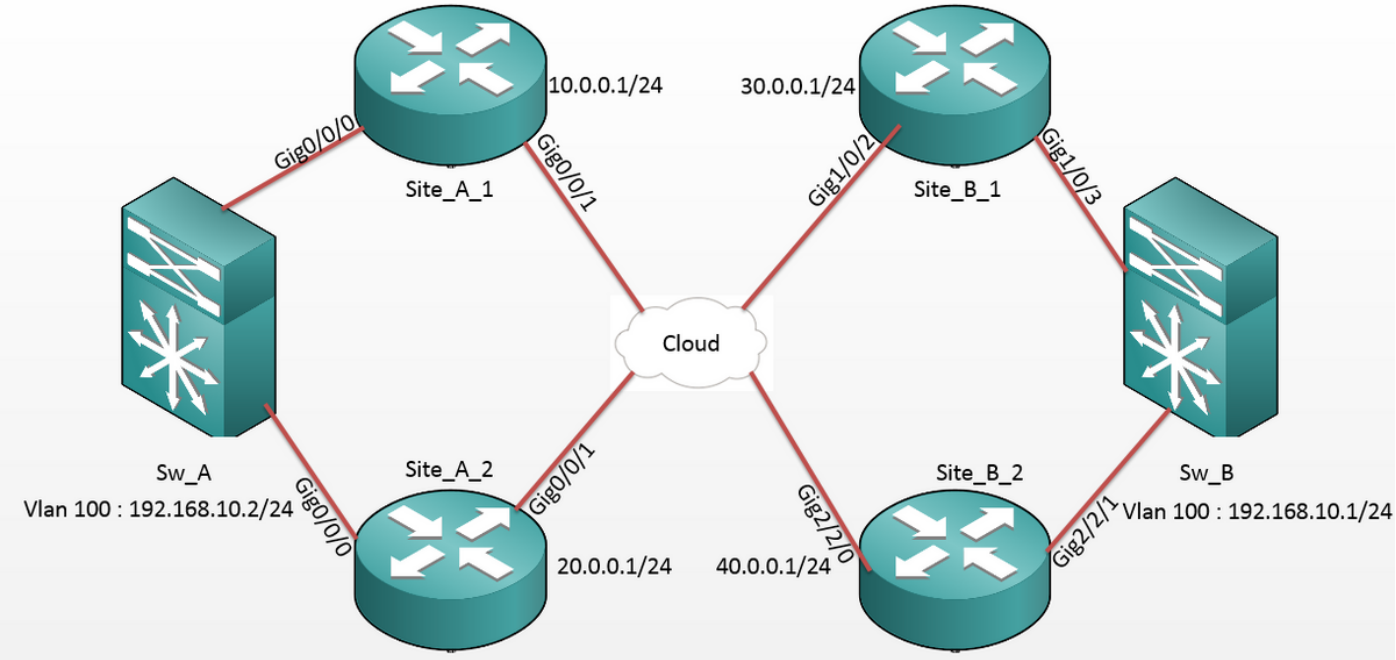
Les fonctionnalités et configurations de base d'OTV sont supposées être connues des utilisateurs de ce document.

Vous pouvez également suivre ces documents pour la même raison :

- Configuration de monodiffusion OTV
- Configuration de multidiffusion OTV

Configuration

Diagramme du réseau



Configurations

Site A : Configurations 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
```

Site B : Configurations 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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Vérifiez si l'adresse MAC de l'hôte VLAN interne (dans ce cas, l'interface SVI du commutateur Catalyst 2960) a été apprise sur les tables de routage OTV.
2. Vérifiez si les crypto encap et les decap sont effectués pour le trafic de superposition (trafic OTV).

Une fois que l'OTV s'affiche après avoir configuré la carte de chiffrement sur l'interface de jointure, vérifiez le redirecteur actif pour les VLAN locaux (dans ce cas les VLAN 100 et 101). Ceci montre que Site_A_1 et Site_B_2 sont les redirecteurs actifs des VLAN pairs puisque vous testerez le chiffrement du trafic pour les requêtes ping initiées à partir du VLAN 100 sur le Site A vers le VLAN 100 sur le Site 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
```

Afin de vérifier si les paquets sont effectivement encapsulés et décapsulés sur l'un ou l'autre ED, vous devez vérifier si la session IPSec est active et les valeurs de compteur dans les sessions de chiffrement afin de confirmer que les paquets sont effectivement cryptés et décryptés. Afin de vérifier si la session IPSec est active, puisqu'elle devient active uniquement si un trafic passe, vérifiez la sortie de **show crypto isakmp sa**. Ici, seules les sorties des redirecteurs actifs sont vérifiées, mais cela devrait indiquer l'état actif sur tous les ED pour que OTV sur le cryptage fonctionne.

```
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
```

Maintenant, afin de confirmer si les paquets sont cryptés et décryptés, vous devez d'abord savoir à quoi vous attendre dans les sorties de **show crypto session detail**. Ainsi, lorsque vous lancez le paquet d'écho ICMP à partir du commutateur Sw_A vers le commutateur Sw_B, ceci est attendu :

- Bien que l'écho ICMP quitte le site A_1 ED qui est le redirecteur actif pour le VLAN 100, il devra encapsuler la charge utile OTV (ICMP Echo + MPLS + GRE)
- Ensuite, une fois que l'écho ICMP atteint le site B_2 ED qui est le redirecteur actif pour VLAN 100, il devra décapsuler la charge utile OTV (ICMP Echo + MPLS + GRE)
- Maintenant, une fois que le Site_B_2 ED reçoit la réponse d'écho ICMP de Sw_B, il doit à nouveau encapsuler la charge utile OTV (ICMP Echo + MPLS + GRE)
- Et une fois que la réponse d'écho ICMP atteint le site A_1 ED, je devrais à nouveau **décapsuler** la charge utile OTV (ICMP Echo + MPLS + GRE)

Après les requêtes ping réussies de Sw_A à Sw_B, attendez-vous à voir un incrément de 5 compteurs sous la section « enc ” et “ dec ” de la sortie **show crypto session detail** sur les deux ED du redirecteur actif.

Maintenant, vérifiez la même chose à partir des 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
```

Ce guide de configuration est capable de transmettre les détails de configuration requis avec l'utilisation d'IPSec pour la configuration à double résidence principale de monodiffusion.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.