

Configurez le cryptage ASR1000 au-dessus d'OTV Unicast

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

Introduction

Ce document décrit l'ensemble de base de configurations qui sont utilisées pour apporter pour recouvrir la virtualisation de transport (OTV) avec le chiffrement IPsec. Le cryptage au-dessus d'OTV n'exige aucune configuration supplémentaire de l'extrémité OTV. Vous devez juste comprendre comment OTV et IPSEC coexiste.

Afin d'ajouter le cryptage au-dessus d'OTV, vous devez ajouter une en-tête de Protocole ESP (Encapsulating Security Payload) sur OTV PDU. Vous pouvez réaliser le cryptage sur les périphériques de la périphérie ASR1000 (ED) par deux manières : (i) IPsec (ii) GETVPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Routeurs ASR1000 pour les périphériques de périphérie (ED)
- Noyau (nuage ISP)
- Le Catalyst 2960 commute comme commutateur d'accès sur l'un ou l'autre de site

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

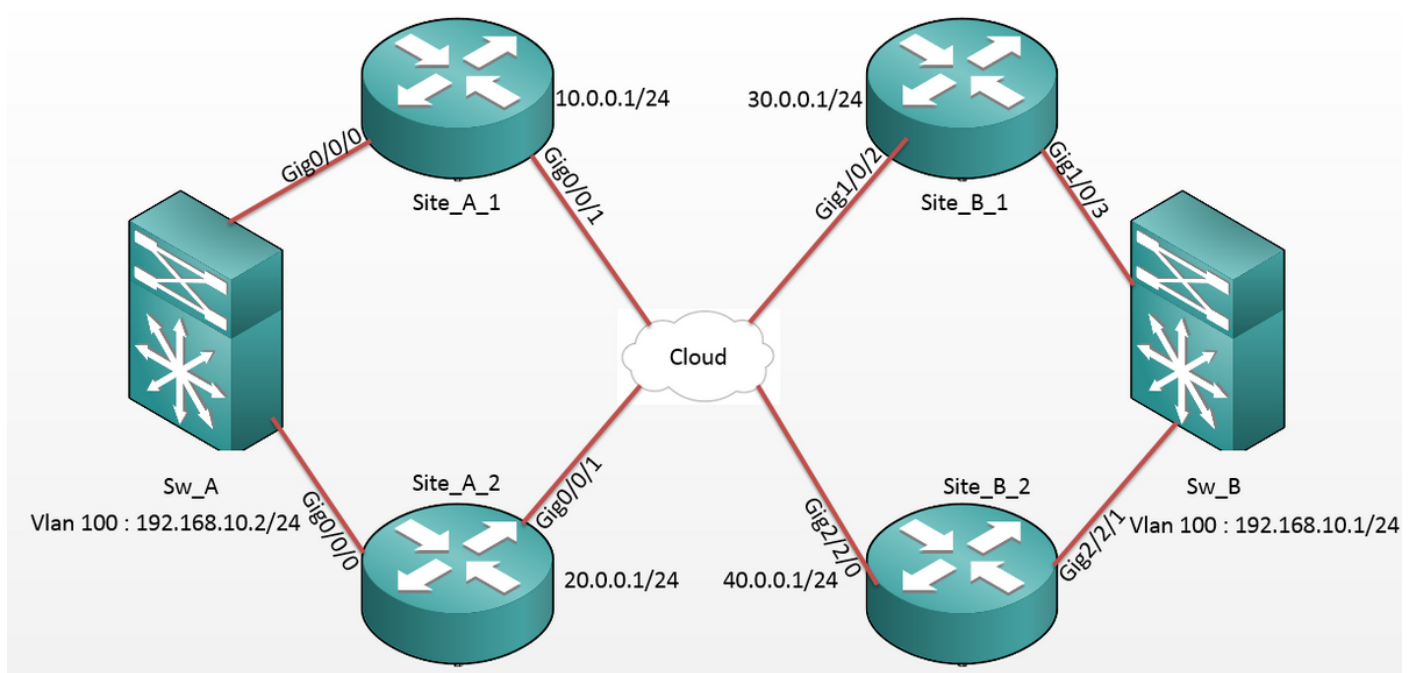
La fonctionnalité de base et les configurations d'OTV sont présumées pour être connues par les utilisateurs de ce document.

Vous pouvez également suivre ces documents pour la même chose :

- [Configuration OTV Unicast](#)
- [Configuration de Multidiffusion OTV](#)

Configurez

Diagramme du réseau



Configurations

Situez A : Configurations ED :

```
Site_A_1#show run
Building configuration...
otv site bridge-domain 99
!
otv site-identifrier 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-identifrier 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 30.0.0.1
crypto isakmp key cisco address 40.0.0.1      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 cryptoacl1
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 30.0.0.1
crypto isakmp key cisco address 40.0.0.1      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
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 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
!
!
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

```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Vérifiez si l'adresse MAC de l'hôte interne VLAN (dans ce cas le SVI sur les 2960 commutateurs de Catalyst) ont été apprises sur les tables de routage OTV.
2. Vérifiez si le cryptos encap et decap sont exécutés pour le trafic de recouvrement (le trafic OTV).

Une fois que l'OTV monte après que vous configurez le crypto map sur l'interface de joindre, vérifiez l'expéditeur actif pour les gens du pays VLAN (dans ce cas VLAN 100 et 101). Ceci prouve que Site_A_1 et Site_B_2 sont les expéditeurs actifs pour les VLAN égaux puisque vous testerez le cryptage du trafic pour des pings initiés de VLAN 100 sur le site A à 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 obtiennent en effet encapsulé et désencapsulé sur l'un ou l'autre d'ED, vous devriez vérifier si la session d'IPSec est en activité et les valeurs du compteur en cryptos sessions afin de confirmer que les paquets sont en effet obtenir chiffré et déchiffré. Afin de vérifier si la session d'IPSec est en activité, puisqu'elle devient active seulement si n'importe quel trafic traverse, vérifiez la sortie du **show crypto isakmp sa**. Ici, seulement les sorties pour les expéditeurs actifs sont vérifiées, mais ceci devrait afficher l'état active sur tous les ED pour OTV au-dessus de cryptage pour fonctionner.

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

Maintenant, afin de confirmer si les paquets obtiennent chiffré et déchiffré, vous le premier besoin de savoir quoi prévoir dans les sorties du **petit groupe de show crypto session**. Ainsi, quand vous initiez le paquet d'écho ICMP du commutateur de Sw_A vers le Sw_B, ceci est prévu :

- Tandis que les feuilles d'écho d'ICMP du Site_A_1 ED qui est l'expéditeur actif pour le VLAN 100, il devront encapsuler la charge utile OTV (écho d'ICMP + MPLS + GRE)
- Alors une fois que l'écho d'ICMP atteint le Site_B_2 ED qui est l'expéditeur actif pour VLAN 100, il devrait désencapsuler la charge utile OTV (écho d'ICMP + MPLS + GRE)
- Maintenant, une fois que le Site_B_2 ED reçoit la réponse d'écho d'ICMP de Sw_B, il devrait de nouveau encapsuler la charge utile OTV (écho d'ICMP + MPLS + GRE)
- Et une fois que la réponse d'écho d'ICMP atteint le Site_A_1 ED, je devrais de nouveau **de nouveau désencapsuler la charge utile OTV** (écho d'ICMP + MPLS + GRE)

Après les pings réussis de Sw_A à Sw_B, comptez voir qu'un incrément de 5 compteurs sous la section « P.J. » et de « décembre » du **petit groupe de show crypto session** a sorti sur chacun des deux l'expéditeur actif ED.

Maintenant, vérifiez la même chose 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
```

```
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
```

```
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 peut donner les détails exigés de configuration avec l'utilisation d'IPSec pour la principale installation dual-homed d'Unicast.

Dépannez

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