

Configurar a criptografia ASR1000 por unicast OTV

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve o conjunto básico de configurações que são usadas para ativar o Overlay Transport Virtualization (OTV) com criptografia IPSec. A criptografia por OTV não exige configurações adicionais da extremidade OTV. Você só precisa entender como OTV e IPSEC coexistem.

Para adicionar criptografia sobre OTV, você precisa adicionar um cabeçalho ESP (Encapsulating Security Payload, payload de segurança de encapsulamento) sobre PDU de OTV. Você pode obter criptografia nos dispositivos ASR1000 Edge (ED) de duas maneiras: (i) IPSec (ii) GETVPN.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteadores ASR1000 para dispositivos de borda (ED)
- Núcleo (ISP Cloud)
- Switches Catalyst 2960 como o switch de acesso em qualquer local

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

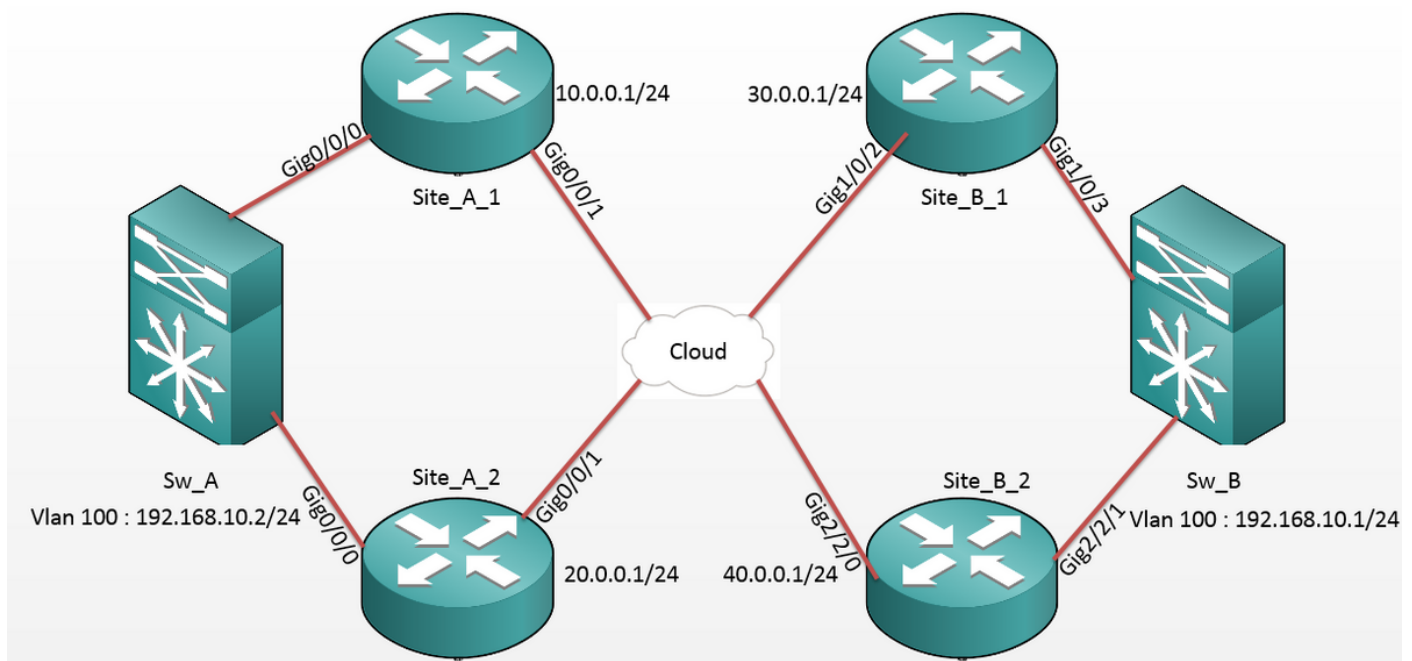
Presume-se que a funcionalidade básica e as configurações de OTV sejam conhecidas pelos usuários deste documento.

Você também pode seguir estes documentos para o mesmo:

- [Configuração unicast de OTV](#)
- [Configuração multicast de OTV](#)

Configurar

Diagrama de Rede



Configurações

Site A: Configurações 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 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

```

Local B: Configurações 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 cryptoacl1

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 cryptoacl1

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

```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Verifique se o endereço MAC do host interno da VLAN (nesse caso, o SVI no switch Catalyst 2960) foi aprendido nas tabelas de rotas OTV.
2. Verifique se os encap criptografados e decaps são executados para o tráfego de Sobreposição (tráfego OTV).

Quando o OTV for ativado depois que você configurar o mapa de criptografia na interface de união, verifique o encaminhador ativo para a VLAN local (nesse caso, VLAN 100 e 101). Isso mostra que Site_A_1 e Site_B_2 são os encaminhadores ativos para a VLAN par, já que você testará a criptografia de tráfego para pings iniciados da VLAN 100 no Site A para a VLAN 100 no 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

Para verificar se os pacotes realmente são encapsulados e desencapsulados em um dos ED, você deve verificar se a sessão IPSec está ativa e os valores do contador nas sessões de criptografia para confirmar se os pacotes estão realmente sendo criptografados e descriptografados. Para verificar se a sessão IPSec está ativa, já que ela se torna ativa somente se qualquer tráfego flui, verifique a saída de **show crypto isakmp sa**. Aqui, somente as saídas dos encaminhadores ativos são verificadas, mas isso deve mostrar o status ativo em todos os EDs para OTV sobre criptografia para funcionar.

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

Agora, para confirmar se os pacotes são criptografados e descriptografados, você precisa primeiro saber o que esperar nas saídas de **show crypto session detail**. Então, quando você inicia o pacote de eco ICMP do switch Sw_A em direção ao Sw_B, isso é esperado:

- Enquanto o eco ICMP sai do Site_A_1 ED que é o encaminhador ativo para a VLAN 100, ele terá que encapsular a carga de OTV (ICMP Echo + MPLS + GRE)
- Depois que o eco ICMP alcançar o Site_B_2 ED, que é o encaminhador ativo para a VLAN 100, ele terá que desencapsular a carga de OTV (ICMP Echo + MPLS + GRE)
- Agora, uma vez que o Site_B_2 ED recebe a Resposta de Eco ICMP de Sw_B, ele teria que encapsular novamente a carga de OTV (ICMP Echo + MPLS + GRE)
- E assim que a Resposta de Eco ICMP chegasse ao Site_A_1 ED, eu teria que **novamente desencapsular** a carga de OTV (ICMP Echo + MPLS + GRE)

Após os pings bem-sucedidos de Sw_A a Sw_B, espere um incremento de 5 contadores nas seções "enc" e "dec" da saída **show crypto session detail** em ambos os EDs do encaminhador ativo.

Agora, verifique o mesmo com os 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

Este guia de configuração é capaz de transmitir os detalhes de configuração necessários com o uso de IPSec para a configuração dual-homed do núcleo Unicast.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.