Configurar a criptografia ASR1000 sobre o unicast OTV

Índice

Introdução

Este documento descreve o grupo básico de configurações que são usadas para trazer acima para overlay a virtualização do transporte (OTV) com criptografia IPSec. A criptografia sobre OTV não exige nenhuma configurações adicional da extremidade OTV. Você apenas precisa de compreender como OTV e o IPSEC coexistem.

A fim adicionar a criptografia sobre OTV, você precisa de adicionar um encabeçamento do Encapsulating Security Payload (ESP) sobre OTV PDU. Você pode conseguir a criptografia nos dispositivos de ponta ASR1000 (ED) com duas maneiras: (i) IPsec (ii) GETVPN.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Roteadores ASR1000 para os dispositivos de ponta (ED)
- Núcleo (nuvem ISP)
- Catalyst 2960 Switch como o switch de acesso em um ou outro local

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

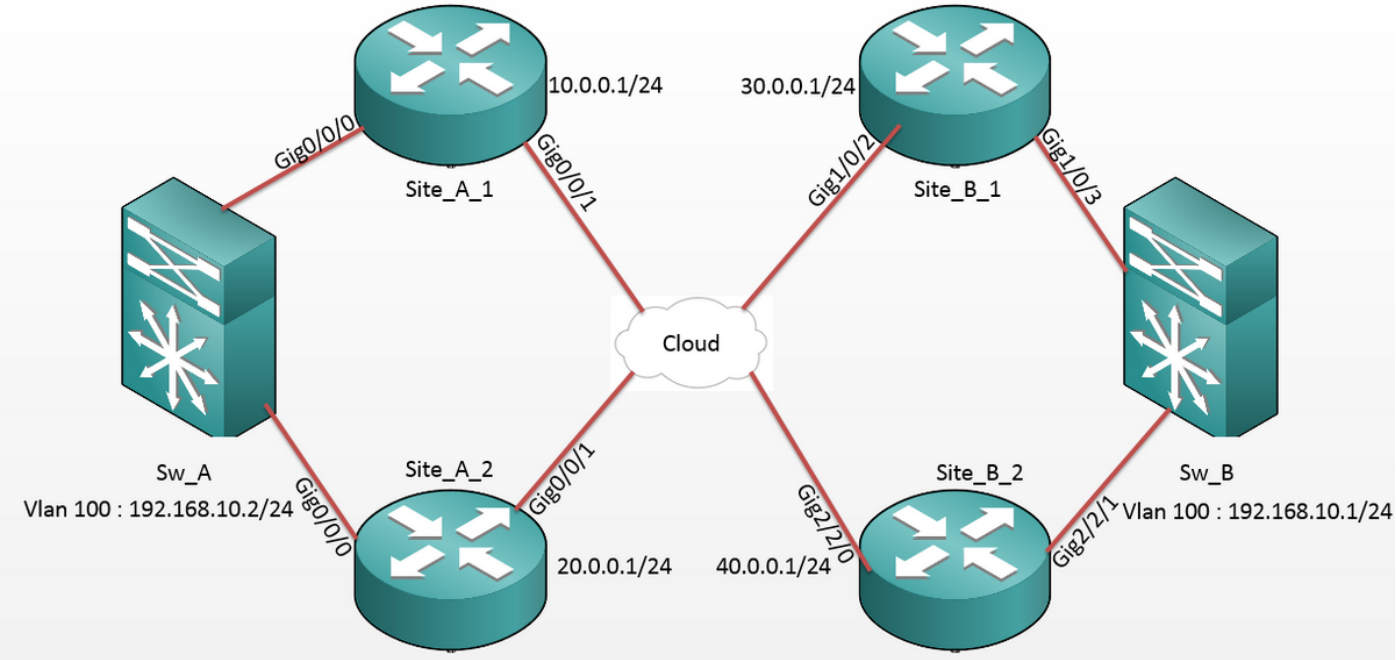
A funcionalidade básica e as configurações de OTV são presumidas ser sabidas pelos usuários deste documento.

Você pode igualmente seguir estes documentos para o mesmos:

- Configuração do unicast OTV
- Configuração do Multicast OTV

Configurar

Diagrama de Rede



Configurações

Situe 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 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
```

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 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
```

Verificar

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

1. Verifique se o MAC address do host interno VLAN (neste caso o SVI nos 2960 interruptores do catalizador) foi aprendido nas tabelas de rota OTV.
2. Verifique se o encap e os decap criptos estão executados para o tráfego da folha de prova (tráfego OTV).

Uma vez que o OTV vem acima depois que você configura o crypto map na relação da junta, verifique o remetente ativo para ver se há os VLAN locais (neste caso VLAN 100 e 101). Isto mostra que Site_A_1 e Site_B_2 são os remetentes ativos para os VLAN uniformes desde que você testará a criptografia de tráfego para os sibilos iniciados do VLAN 100 no local A ao VLAN 100 no local 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
```

A fim verificar se os pacotes obtêm certamente encapsulados e descapsulado em um ou outro ED, você deve verificar se a sessão IPSec é ativa e os valores de contador nas sessões de criptografia a fim confirmar que os pacotes estão obtendo certamente cifrados e decifrados. A fim verificar se a sessão IPSec é ativa, desde que se torna ativo somente se algum tráfego corre através, verifique a saída **isakmp cripto sa da mostra**. Aqui, somente as saídas para os remetentes ativos são verificadas, mas esta deve mostrar o status ativo em todos os ED para OTV sobre a criptografia para trabalhar.

```
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
```

Agora, a fim confirmar se os pacotes obtêm cifrados e decifrados, você precisa primeiramente de conhecer o que esperar nas saídas do **detalhe da sessão de criptografia da mostra**. Assim, quando você inicia o pacote de eco ICMP do interruptor de Sw_A para o Sw_B, isto é esperado:

- Quando o eco ICMP sair do Site_A_1 ED que é o remetente ativo para o VLAN 100, terá que encapsular o payload OTV (eco ICMP + MPLS + GRE)
- Então uma vez que o eco ICMP alcança o Site_B_2 ED que é o remetente ativo para o VLAN 100, tem que decapsulate o payload OTV (eco ICMP + MPLS + o GRE)
- Agora, uma vez que o Site_B_2 ED recebe a resposta de eco ICMP de Sw_B, teria que outra vez encapsular o payload OTV (eco ICMP + MPLS + o GRE)
- E uma vez que a resposta de eco ICMP alcança o Site_A_1 ED, eu tenho que outra vez **outra vez decapsulate o** payload OTV (eco ICMP + MPLS + o GRE)

Após os ping bem-sucedido de Sw_A a Sw_B, espere ver que um incremento dos contadores 5 sob a seção “enc” e de “dezembro” do **detalhe da sessão de criptografia da mostra** output em ambos o remetente ativo ED.

Agora, verifique o mesmos dos 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
```

Este manual de configuração pode transportar os detalhes da configuração requerida com o uso do IPsec para a instalação dual-homed do núcleo do unicast.

Troubleshooting

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