Cifrado de la configuración ASR1000 sobre el unicast OTV

Contenido

Introducción

Este documento describe el conjunto básico de las configuraciones que se utilizan para traer para arriba para cubrir la virtualización del transporte (OTV) con la encripción de IPSec. El cifrado sobre OTV no requiere ninguna configuraciones adicional del extremo OTV. Usted apenas necesita entender cómo coexiste OTV y el IPSEC.

Para agregar el cifrado sobre OTV, usted necesita agregar una encabezado del Encapsulating Security Payload (ESP) encima de OTV PDU. Usted puede alcanzar el cifrado en los dispositivos de borde ASR1000 (ED) con dos maneras: (i) IPSec (ii) GETVPN.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers ASR1000 para los dispositivos de borde (ED)
- Base (nube ISP)
- Catalyst 2960 Switch como el switch de acceso en cualquier sitio

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

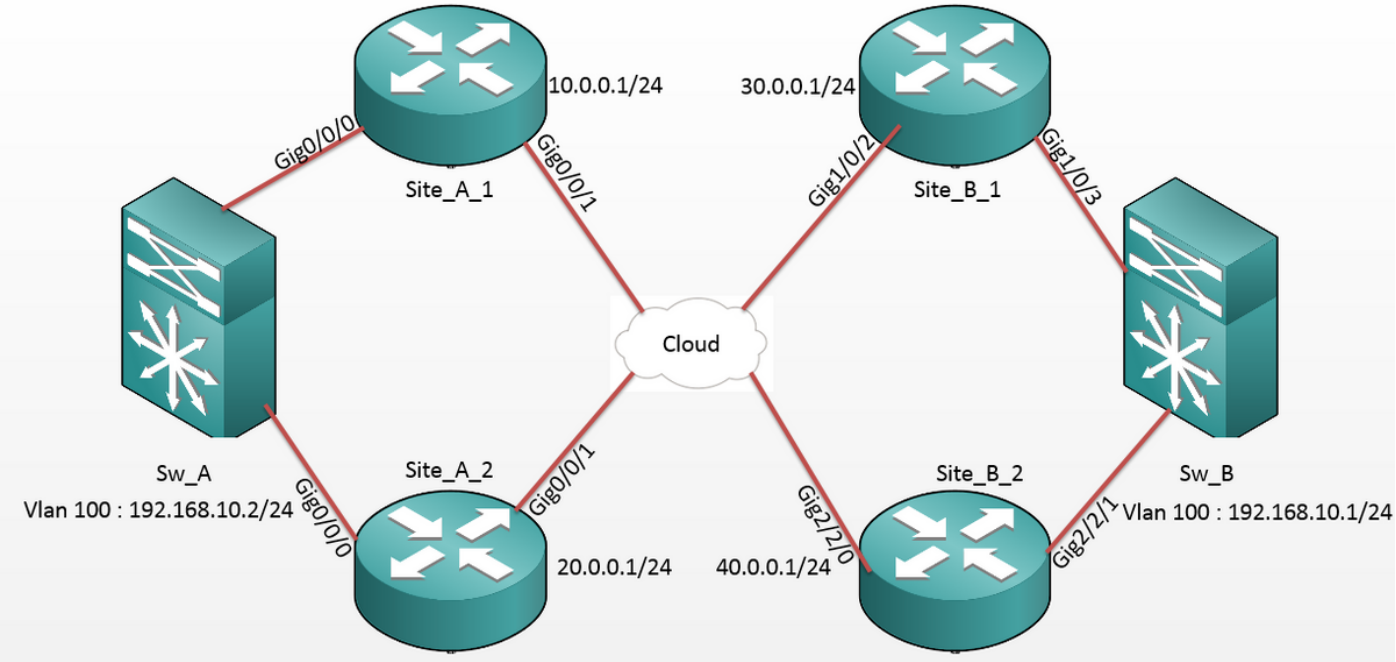
La funcionalidad básica y las configuraciones de OTV se suponen para ser sabidas por los usuarios de este documento.

Usted puede también seguir estos documentos para lo mismo:

- Configuración del unicast OTV
- Configuración del Multicast OTV

Configurar

Diagrama de la red



Configuraciones

Localice A: Configuraciones 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
```

Sitio B: Configuraciones 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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

1. Marque si la dirección MAC del host interno del VLA N (en este caso el SVI en el switch de Catalyst 2960) se ha aprendido en las tablas de ruta OTV.
2. Marque si los encap y los decap crypto se realizan para el tráfico del recubrimiento (tráfico OTV).

Una vez que sube el OTV después de que usted configure la correspondencia de criptografía en la interfaz del unido, marque el promotor activo para el VLA N local (en este caso VLAN 100 y 101). Esto muestra que Site_A_1 y Site_B_2 son los promotores activos para incluso el VLA N puesto que usted probará la encripción del tráfico para los ping iniciados del VLAN 100 en el sitio A al VLAN 100 en el sitio 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 marcar si los paquetes consiguen de hecho encapsulados y decapsulated en cualquier ED, usted debe marcar si sesión IPSec son activos y los valores de contador en las sesiones de criptografía para confirmar que los paquetes están consiguiendo de hecho cifrados y desencriptados. Para marcar si sesión IPSec es activo, puesto que llega a ser activo solamente si algún tráfico atraviesa, marque la salida **isakmp crypto sa de la demostración**. Aquí, solamente las salidas para los promotores activos se marcan, pero ésta debe mostrar el estado activo en todos los ED para OTV sobre el cifrado para trabajar.

```
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
```

Ahora, para confirmar si los paquetes consiguen cifrados y desencriptados, usted primero necesita conocer qué esperar en las salidas del **detalle de la sesión de criptografía de la demostración**. Así pues, cuando usted inicia el paquete de eco ICMP del Switch de Sw_A hacia el Sw_B, se espera esto:

- Mientras que el eco ICMP se va del Site_A_1 ED que es el promotor activo para el VLAN 100, tendrá que encapsular el payload OTV (eco ICMP + MPLS + GRE)
- Entonces una vez que el eco ICMP alcanza el Site_B_2 ED que es el promotor activo para el VLAN 100, tuvo que decapsulate el payload OTV (eco ICMP + MPLS + el GRE)
- Ahora, una vez que el Site_B_2 ED recibe la respuesta de eco ICMP de Sw_B, tendría que otra vez encapsular el payload OTV (eco ICMP + MPLS + el GRE)
- Y una vez que la respuesta de eco ICMP alcanza el Site_A_1 ED, tuve que otra vez **otra vez decapsulate el** payload OTV (eco ICMP + MPLS + el GRE)

Después de los ping exitosos de Sw_A a Sw_B, espere ver que un incremento de 5 contadores bajo sección “enc” y de “diciembre” del **detalle de la sesión de criptografía de la demostración** hiciera salir en ambos el promotor activo ED.

Ahora, marque lo mismo de los 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
```

Esta guía de configuración puede transportar los detalles de la configuración necesaria con el uso del IPSec para la configuración dual-homed de la base del unicast.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.