Configuración del cifrado ASR1000 sobre OTV Unicast

Contenido

Introducción

Este documento describe el conjunto básico de configuraciones que se utilizan para activar Overlay Transport Virtualization (OTV) con cifrado IPSec. El cifrado sobre OTV no requiere ninguna configuración adicional del extremo OTV. Solo tiene que entender cómo coexisten OTV e IPSEC.

Para agregar cifrado a través de OTV, debe agregar un encabezado de carga útil de seguridad de encapsulación (ESP) a la parte superior de la PDU de OTV. Puede lograr el cifrado en los dispositivos periféricos ASR1000 (ED) de dos maneras: i) IPSec ii) GETVPN.

Prerequisites

Requirements

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 ASR 1000 para dispositivos periféricos (ED)
- Núcleo (nube ISP)
- Switches Catalyst 2960 como switch de acceso en cualquier sitio

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

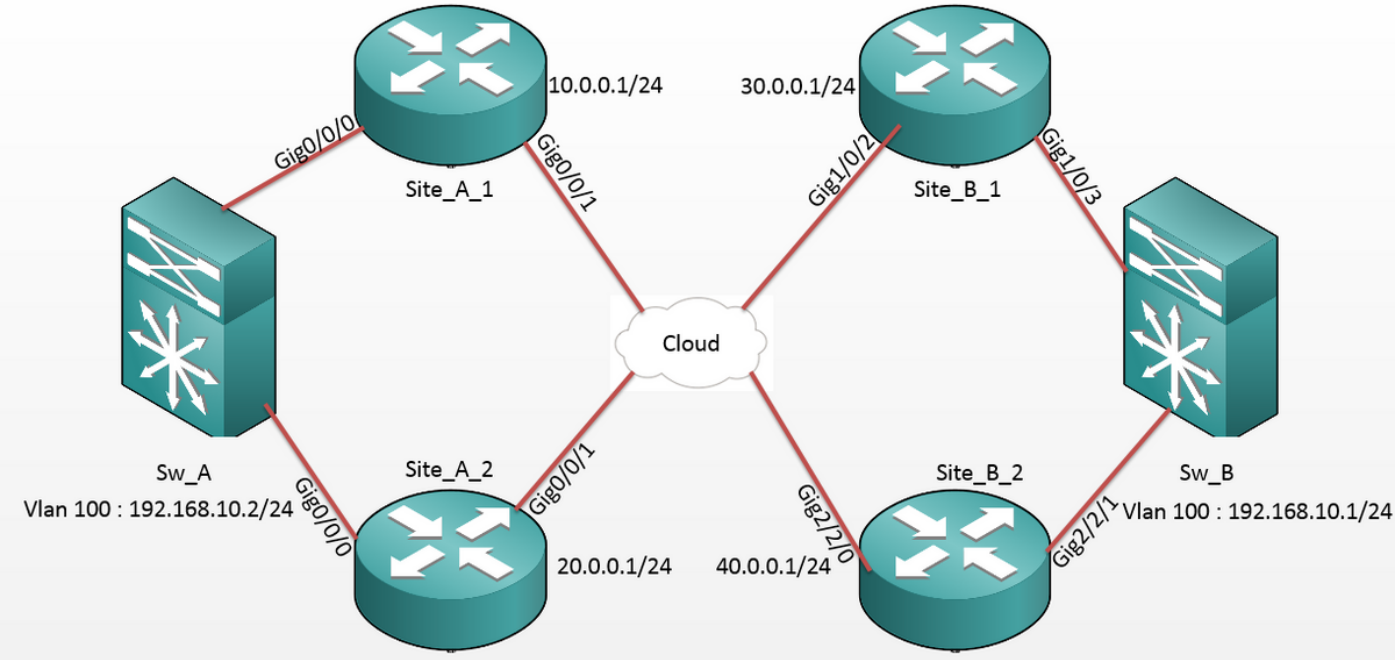
Se supone que los usuarios de este documento conocen la funcionalidad básica y las configuraciones de OTV.

También puede seguir estos documentos para lo mismo:

- Configuración de unidifusión OTV
- Configuración de multidifusión de OTV

Configurar

Diagrama de la red



Configuraciones

Sitio 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. Verifique si la dirección MAC del host VLAN interno (en este caso, la SVI en los switches Catalyst 2960) se ha aprendido en las tablas de ruta OTV.
2. Compruebe si se realizan los encapsulados y los decap criptográficos para el tráfico Overlay (OTV traffic).

Una vez que el OTV aparece después de configurar el mapa crypto en la interfaz de unión, verifique el reenviador activo para las VLAN locales (en este caso VLAN 100 y 101). Esto muestra que Site_A_1 y Site_B_2 son los reenviadores activos para las VLAN pares ya que probará el cifrado del tráfico para los pings iniciados desde VLAN 100 en el Sitio A a 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 verificar si los paquetes realmente se encapsulan y se desencapsulan en cualquiera de los ED, debe verificar si la sesión IPSec está activa y los valores de contador en las sesiones crypto para confirmar que los paquetes están efectivamente cifrados y descifrados. Para verificar si la sesión IPSec está activa, ya que se activa solamente si fluye tráfico, verifique el resultado de **show crypto isakmp sa**. Aquí, sólo se comprueban los resultados de los reenviadores activos, pero esto debería mostrar el estado activo en todos los ED para que OTV sobre cifrado funcione.

```
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
```

Ahora, para confirmar si los paquetes se cifran y descifran, primero debe saber qué esperar en los resultados de **show crypto session detail**. Por lo tanto, cuando se inicia el paquete de eco ICMP

del switch Sw_A hacia el Sw_B, se espera esto:

- Mientras el eco ICMP sale del ED Site_A_1 que es el reenviador activo para la VLAN 100, tendrá que encapsular la carga útil OTV (eco ICMP + MPLS + GRE)
- Luego, una vez que el eco ICMP llega al ED Site_B_2, que es el reenviador activo para VLAN 100, tendría que desencapsular la carga útil OTV (eco ICMP + MPLS + GRE)
- Ahora, una vez que el ED Site_B_2 recibe la respuesta de eco ICMP de Sw_B, tendría que encapsular de nuevo la carga útil de OTV (eco ICMP + MPLS + GRE)
- Y una vez que la Respuesta de eco ICMP llega al ED Site_A_1, tendría que **volver** a **desencapsular** la carga útil de OTV (ICMP Echo + MPLS + GRE)

Después de los pings exitosos de Sw_A a Sw_B, espere ver un incremento de 5 contadores en la sección "enc" y "dec" de la salida **show crypto session detail** en ambos ED del reenviador activo.

Ahora, verifique 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

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
```

Esta guía de configuración puede transmitir los detalles de configuración requeridos con el uso de IPSec para la configuración de doble reposición de núcleo unidifusión.

Troubleshoot

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