

OTV 유니캐스트를 통한 ASR1000 암호화 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 IPSec 암호화를 사용하는 OTV(Overlay Transport Virtualization)를 실행하는 데 사용되는 기본 컨피그레이션 집합을 설명합니다. OTV를 통한 암호화에서는 OTV 측의 추가 컨피그레이션이 필요하지 않습니다. OTV와 IPSEC이 어떻게 공존하는지 이해하기만 하면 됩니다.

OTV를 통한 암호화를 추가하려면 OTV PDU 위에 ESP(Encapsulating Security Payload) 헤더를 추가해야 합니다. 다음 두 가지 방법으로 ASR1000 ED(Edge Device)에서 암호화를 달성할 수 있습니다. (i) IPSec (ii) GETVPN

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ED(Edge Device)용 ASR1000 라우터
- 코어(ISP 클라우드)
- Catalyst 2960 스위치를 각 사이트의 액세스 스위치로 사용

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

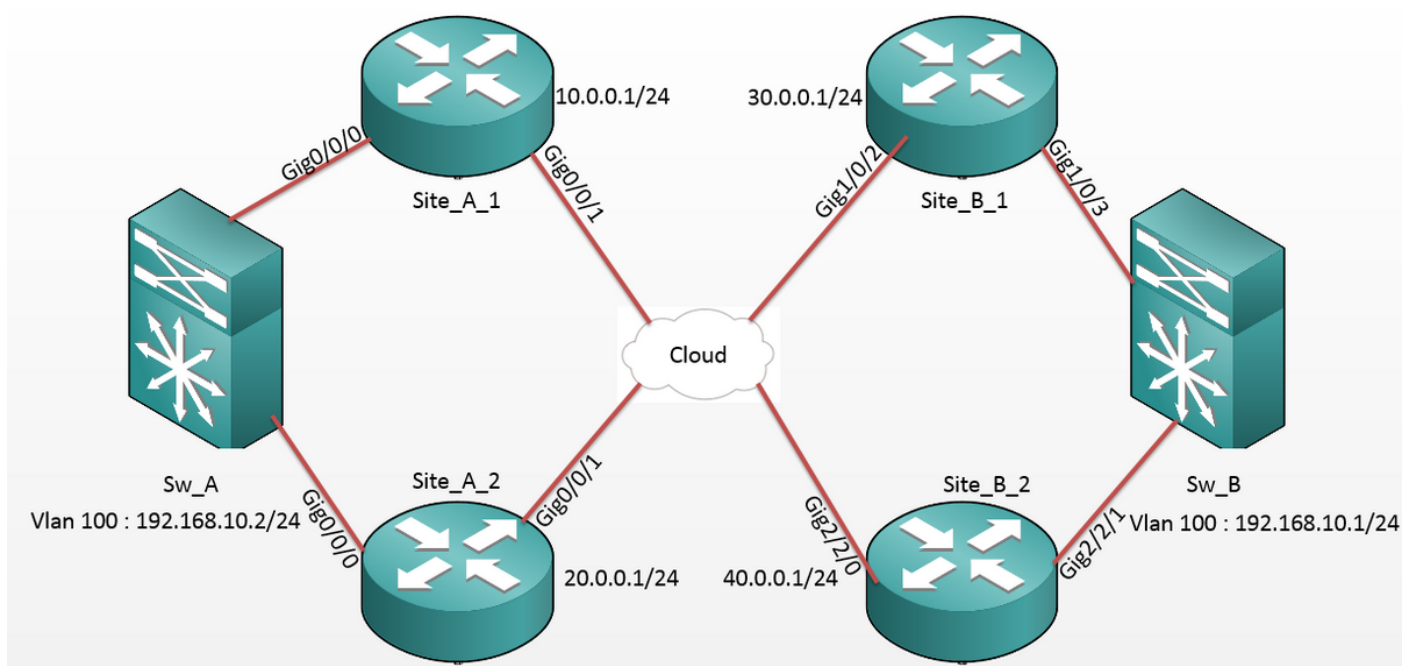
OTV의 기본 기능 및 구성은 이 문서의 사용자가 알고 있는 것으로 간주됩니다.

또한 다음 문서를 따라 이동할 수도 있습니다.

- [OTV 유니캐스트 컨피그레이션](#)
- [OTV 멀티캐스트 컨피그레이션](#)

구성

네트워크 다이어그램



설정

사이트 A: ED 구성:

```
Site_A_1#show run
Building configuration...

otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
crypto isakmp policy 10
  hash md5
```

```
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 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

```

```

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 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

```

```

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 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

```

사이트 B: ED 구성:

```

Site_B_1#sh run
Building configuration...
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
crypto isakmp policy 10
    hash md5

```

```

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
```

```
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 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
```

```

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 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 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 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

```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. 내부 VLAN 호스트(이 경우 2960 catalyst 스위치의 SVI)의 MAC 주소가 OTV 경로 테이블에서 학습되었는지 확인합니다.
2. 오버레이(OTV 트래픽) 트래픽에 대해 암호화 캡슐화 및 디캡이 수행되었는지 확인합니다.

조인 인터페이스에서 암호화 맵을 구성한 후 OTV가 시작되면 활성 전달자에서 로컬 VLAN(이 예에

서는 VLAN 100 및 101)을 확인합니다. 이는 사이트 A의 VLAN 100에서 사이트 B의 VLAN 100으로 시작된 ping에 대한 트래픽 암호화를 테스트하므로 Site_A_1 및 Site_B_2가 짝수 VLAN에 대한 활성 전달자임을 보여줍니다.

<#root>

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					

<#root>

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					

패킷이 실제로 ED에서 캡슐화되고 역캡슐화되는지 확인하려면 IPSec 세션이 활성 상태인지, 그리고 암호화 세션의 카운터 값을 확인하여 패킷이 실제로 암호화 및 암호 해독되고 있는지 확인해야 합니다. IPSec 세션이 활성 상태인지 확인하려면 트래픽이 통과하는 경우에만 활성화되므로 show crypto isakmp sa의 출력을 확인합니다. 여기서는 활성 전달자에 대한 출력만 확인되지만, OTV over encryption이 작동하려면 모든 ED의 활성 상태가 표시됩니다.

```
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

이제 패킷이 암호화 및 암호 해독되는지 확인하려면 먼저 show crypto session detail의 출력에서 예상되는 내용을 알아야 합니다. 따라서 Sw_A 스위치에서 Sw_B로 ICMP 에코 패킷을 시작하면 다음과 같이 됩니다.

- ICMP 에코가 VLAN 100의 활성 전달자인 Site_A_1 ED에서 나가는 동안에는 OTV 페이로드 (ICMP 에코 + MPLS + GRE)를 캡슐화해야 합니다
- 그런 다음 ICMP 에코가 VLAN 100의 활성 전달자인 Site_B_2 ED에 도달하면 OTV 페이로드 (ICMP 에코 + MPLS + GRE)를 역캡슐화해야 합니다
- 이제 Site_B_2 ED가 Sw_B에서 ICMP 에코 응답을 수신하면 OTV 페이로드(ICMP 에코 + MPLS + GRE)를 다시 캡슐화해야 합니다
- 그리고 ICMP 에코 응답이 Site_A_1 ED에 도달하면 다시 OTV 페이로드(ICMP 에코 + MPLS + GRE)를 역캡슐화해야 합니다

Sw_A에서 Sw_B로의 ping이 성공하면 활성 전달자 ED의 show crypto session detail 출력의 "enc" 및 "dec" 섹션 아래에 5개의 카운터가 증가합니다.

이제 ED에서도 동일한 내용을 확인하십시오.

<#root>

```
Site_A_1(config-if)#do show crypto session detail | section enc
```

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

Outbound: #pkts enc'd 0 drop 0 life (KB/Sec) 4608000/3345

Outbound: #pkts enc'd 10 drop 0 life (KB/Sec) 4607998/3291

<<<< 10 counter before ping

<#root>

Site_A_1(config-if)#do show crypto session detail | section dec

Inbound: #pkts dec'd 0 drop 0 life (KB/Sec) 4608000/3343

Inbound: #pkts dec'd 18 drop 0 life (KB/Sec) 4607997/3289

<<<< 18 counter before ping

<#root>

Site_B_2(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

Outbound: #pkts enc'd 18 drop 0 life (KB/Sec) 4607997/3295

<<<< 18 counter before ping

Outbound: #pkts enc'd 9 drop 0 life (KB/Sec) 4607999/3295

<#root>

Site_B_2(config-if)#do show crypto session detail | section dec

Inbound: #pkts dec'd 10 drop 0 life (KB/Sec) 4607998/3293

<<<< 10 counter before ping

Inbound: #pkts dec'd 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)#

<#root>

Site_A_1(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

Outbound: #pkts enc'd 0 drop 0 life (KB/Sec) 4608000/3339

Outbound: #pkts enc'd 15 drop 0 life (KB/Sec) 4607997/3284

<<<< 15 counter after ping (After ICMP Echo)

<#root>

Site_A_1(config-if)#do show crypto session detail | section dec

Inbound: #pkts dec'd 0 drop 0 life (KB/Sec) 4608000/3338

Inbound: #pkts dec'd 23 drop 0 life (KB/Sec) 4607997/3283

<<<< 23 counter after ping (After ICMP Echo Reply)

<#root>

Site_B_2(config-if)#do show crypto session detail | section enc

K - Keepalives, N - NAT-traversal, T - cTCP encapsulation

Outbound: #pkts enc'd 23 drop 0 life (KB/Sec) 4607997/3282

<<<< 23 counter after ping (After ICMP Echo Reply)

Outbound: #pkts enc'd 9 drop 0 life (KB/Sec) 4607999/3282

<#root>

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

이 컨피그레이션 가이드에서는 유니캐스트 코어 듀얼 홉 설정에 IPSec을 사용하는 데 필요한 컨피그레이션 세부사항을 전달할 수 있습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.