OTVユニキャストでのASR1000暗号化の設定

内容

概要

このドキュメントでは、IPSec暗号化を使用してOverlay Transport Virtualization(OTV)を起動するために使用される基本的な構成セットについて説明します。Encryption over OTVでは、OTV側からの追加設定は必要ありません。OTVとIPSECの共存について理解する必要があります。

OTVに暗号化を追加するには、OTV PDUの上にEncapsulating Security Payload(ESP)ヘッダーを追加する必要があります。ASR1000エッジデバイス(ED)では、次の2つの方法で暗号化を実現できます。(i) IPSec(ii) GETVPN

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- エッジデバイス(ED)用ASR1000ルータ
- コア（ISPクラウド）
- いずれかのサイトのアクセススイッチとしてCatalyst 2960スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

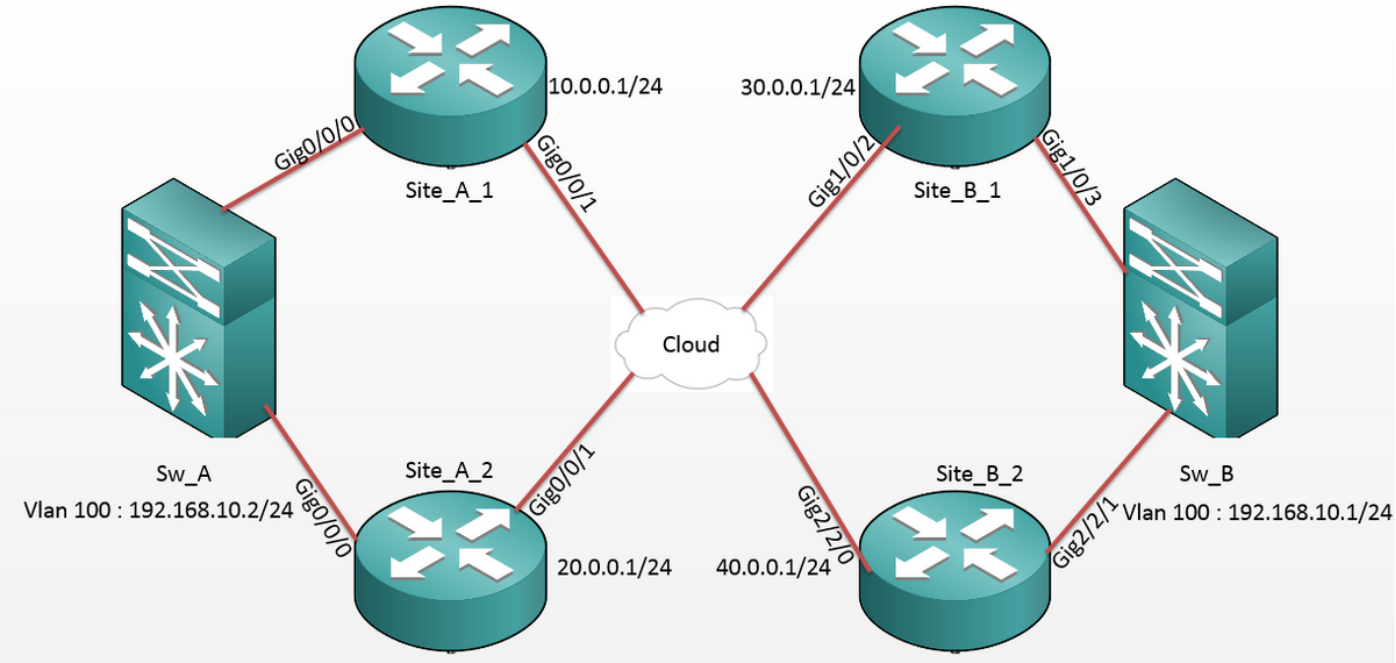
OTVの基本機能と設定は、このドキュメントのユーザが知っていると想定されています。

また、次のドキュメントに従うこともできます。

- OTVユニキャスト設定
- OTVマルチキャストの設定

設定

ネットワーク図



設定

サイトA: ED構成：

```
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
crypto isakmp key cisco address 30.0.0.1
crypto isakmp key cisco address 40.0.0.1
```

```
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
 bridge-domain 99
 !
```

```
!
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 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
```

サイトB:ED構成：

```
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
!
crypto ipsec transform-set tset esp-aes
esp-md5-hmac
```

```
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
 bridge-domain 99
 !
```

```
 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
 !
 service instance 100 ethernet
```

```
 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
```

```
 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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. 内部VLANホストのMACアドレス（この場合は2960 CatalystスイッチのSVI）がOTVルートテーブルで学習されているかどうかを確認します。
2. 暗号カプセル化とカプセル化解除がオーバーレイ（OTVトラフィック）トラフィックに対して実行されているかどうかを確認します。

参加インターフェイスで暗号マップを設定した後にOTVが起動したら、ローカルVLAN（この場合はVLAN 100および101）のアクティブフォワーダをチェックします。 これは、サイトAのVLAN 100からサイトBのVLAN 100に対して開始されたpingのトラフィック暗号化をテストするため、Site_A_1とSite_B_2が偶数のVLANのアクティブフォワーダであることを示しています。

```
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
```

パケットがどちらのEDでも実際にカプセル化および力プセル化解除されているかどうかを確認するには、IPSecセッションがアクティブかどうか、および暗号化セッションのカウンタ値を確認して、パケットが実際に暗号化および復号化されていることを確認します。IPSecセッションがアクティブかどうかを確認するには、トラフィックが通過する場合にのみアクティブになるため、**show crypto isakmp saの出力を確認します。**ここでは、アクティブなフォワーダの出力だけがチェックされますが、これは暗号化を使用するすべてのEDのアクティブ状態を示します。

```
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
```

ここで、パケットが暗号化および復号化されたかどうかを確認するには、まず**show crypto session detailの出力で何を期待するかを知る必要があります。**したがって、Sw_Aスイッチから Sw_Bに向かうICMPエコーパケットを開始すると、次のことが予想されます。

- ICMPエコーはVLAN 100のアクティブフォワーダであるSite_A_1 EDから送信されますが、

OTVペイロード（ICMPエコー+ MPLS + GRE）をカプセル化する必要があります
- 次に、ICMPエコーがVLAN 100のアクティブフォワーダであるSite_B_2 EDに到達すると、OTVペイロード（ICMPエコー+ MPLS + GRE）をカプセル化する必要があります
- ここで、Site_B_2 EDがSw_BからICMPエコー応答を受信したら、OTVペイロード（ICMPエコー+ MPLS + GRE）を再度カプセル化する必要があります
- ICMPエコー応答がSite_A_1 EDに到達したら、OTVペイロード（ICMPエコー+ MPLS + GRE）を再びデカプセル化する必要があります

Sw_AからSw_Bへのpingが成功した後、アクティブなフォワーダEDの両方で**show crypto session detail出力の「enc」および「dec」セクションに5つのカウンタが増加すると予想されます。**

次に、EDの同じ項目を確認します。

```
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
```

この設定ガイドでは、ユニキャストコアデュアルホーム設定にIPSecを使用して、必要な設定の詳細を伝えることができます。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。