配置SD-WAN基於區域的防火牆(ZBFW)和路由洩漏

目錄

簡介

本文說明如何配置、驗證基於區域的防火牆(ZBFW)，並對虛擬專用網路(VPN)之間的路由洩漏進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco SD-WAN重疊會啟動初始配置
- 從vManage使用者介面(UI)配置ZBFW
- 從vManage UI進行路由洩漏控制策略配置

採用元件

為了演示目的，使用了以下軟體：

- 採用20.6.2軟體版本的Cisco SD-WAN vSmart控制器
- 採用20.6.2軟體版本的Cisco SD-WAN vManage控制器

- 兩台運行17.6.2軟體版本的Cisco IOS®-XE Catalyst 8000V虛擬邊緣平台路由器，在控制器模式下運行
- 三台運行17.6.2軟體版本的Cisco IOS-XE Catalyst 8000V虛擬邊緣平台路由器，在自主模式下運行

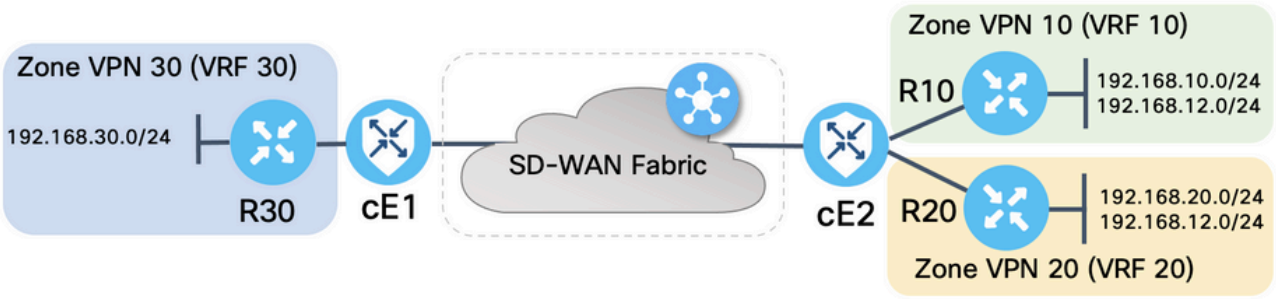
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔介紹路由器如何在SD-WAN重疊中確定目標VPN對映，以及如何驗證和排除VPN之間的路由洩漏。還介紹了在從不同的VPN通告同一子網時路徑選擇的特性，以及由此可能引起的問題型別。

設定

網路圖表



這兩台SD-WAN路由器均配置了基本引數，以建立與SD-WAN控制器的控制連線以及它們之間的資料平面連線。此組態的詳細資訊超出本檔案的範圍。下表彙總了VPN、站點ID和區域分配。

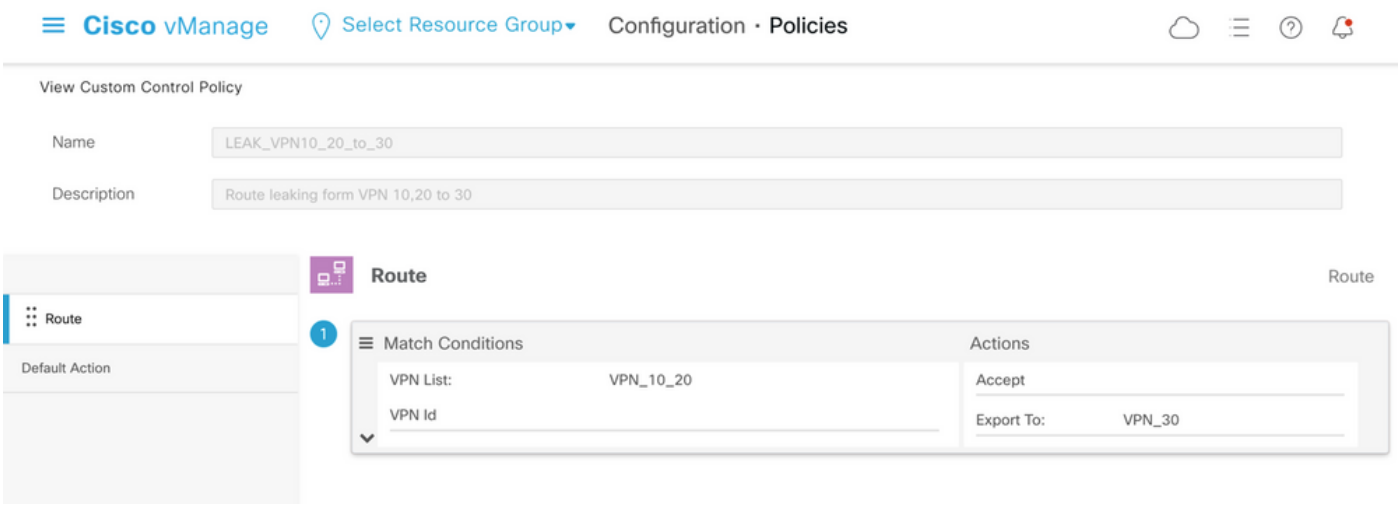
	cE1	cE2
Site-ID	11	12
VPN	30	10,20
System-IP	169.254.206.11	169.254.206.12

服務端的路由器在每個虛擬路由和轉發(VRF)中配置了靜態預設路由，這些路由指向對應的SD-WAN路由器。同樣，SD-WAN邊緣路由器也配置了指向相應子網的靜態路由。請注意，為了演示路由洩漏和ZBFW的潛在問題，cE2服務端後面的路由器具有相同的子網192.168.12.0/24。在cE2後面的兩台路由器上，都配置了一個環回介面，用於模擬具有相同IP地址192.168.12.12的主機。

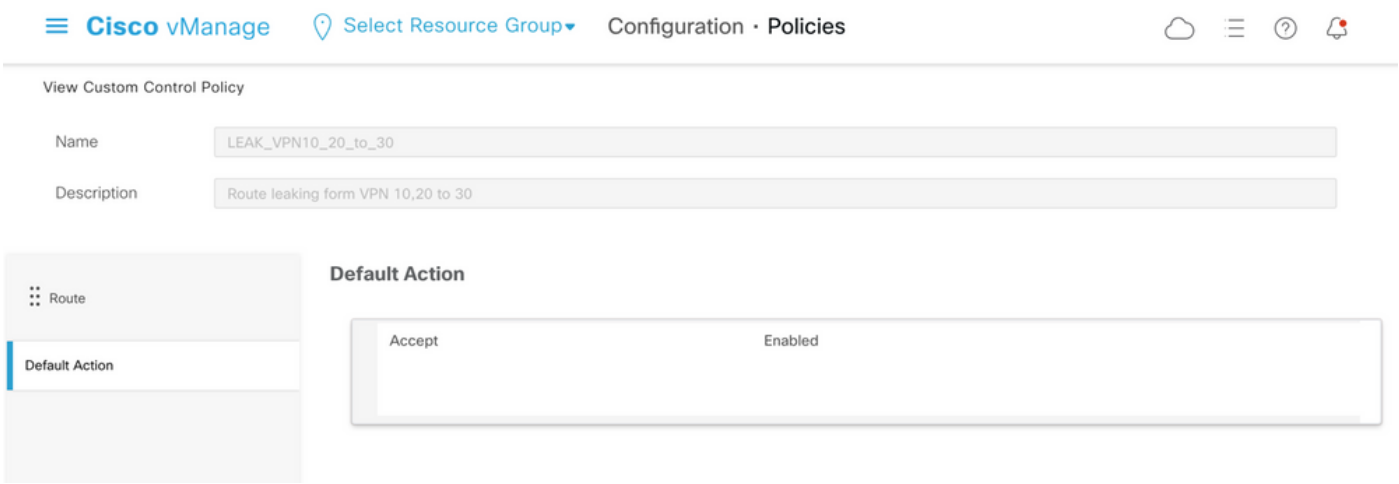
必須注意的是，在本演示中，Cisco IOS-XE路由器R10、R20和R30在SD-WAN邊緣路由的服務端以自主模式運行，這些路由主要用於模擬終端主機。SD-WAN邊緣路由上的環回介面不能用於此目的，而不是服務端路由器等實際主機，因為源自SD-WAN邊緣路由器VRF中的介面的流量不被視為源自ZBFW區域中相應的資料流，而是屬於邊緣路由器的特殊自身區域。因此，不能將ZBFW區域視為VRF相同。詳細討論自帶區不屬於本文範圍。

路由洩漏配置

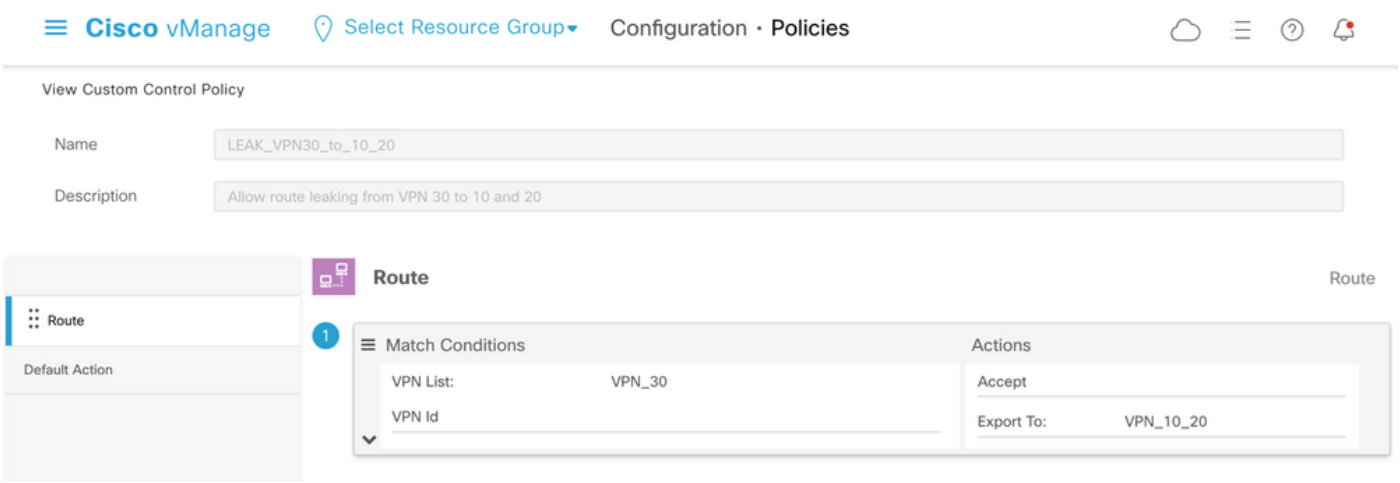
主要控制策略的配置目標是允許從VPN 10和20到VPN 30的所有路由的路由洩漏。VRF 30僅存在於路由器cE1上，而VRF 10和20僅配置在路由器cE2上。為此，配置了兩個拓撲（自定義控制）策略。下面是從VPN 10和20將所有路由匯出到VPN 30的拓撲。

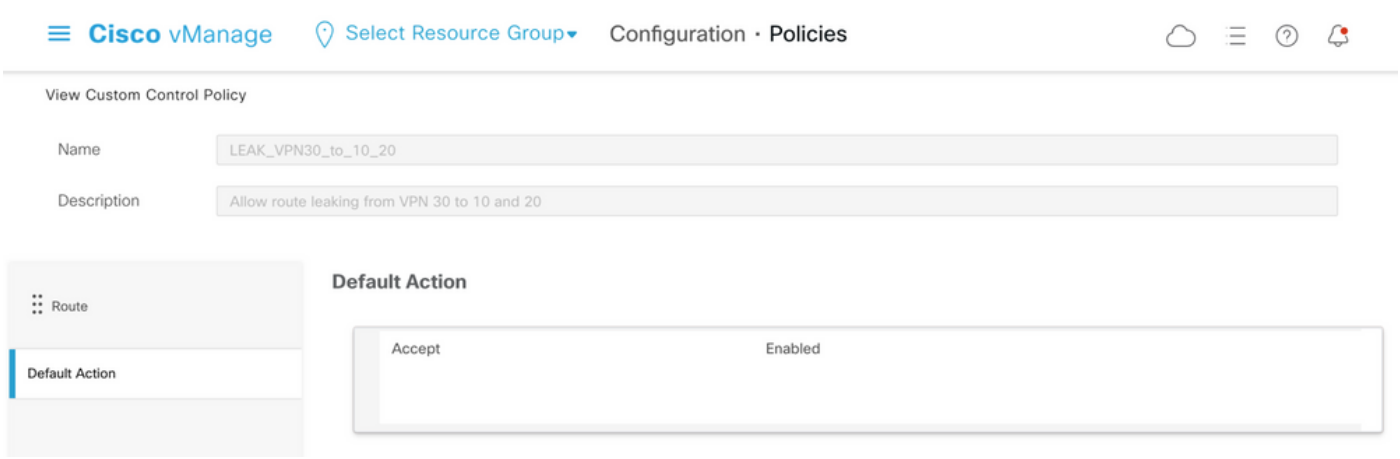


請注意，Default Action設定為Allow，以避免意外阻止TLOC通告或正常的VPN內路由通告。

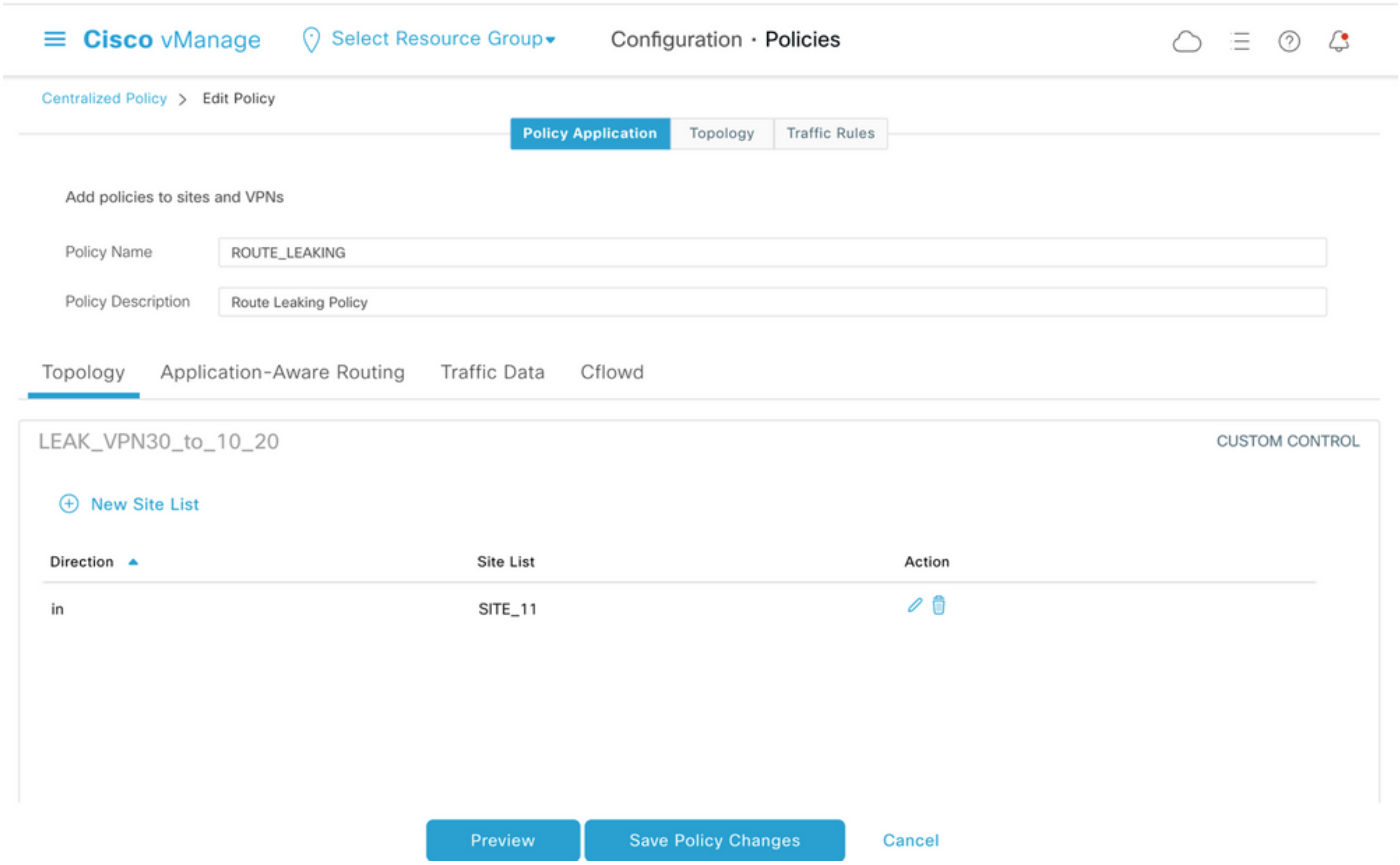


同樣，拓撲策略配置為允許從VPN 30到VPN 10和20反向通告路由資訊。

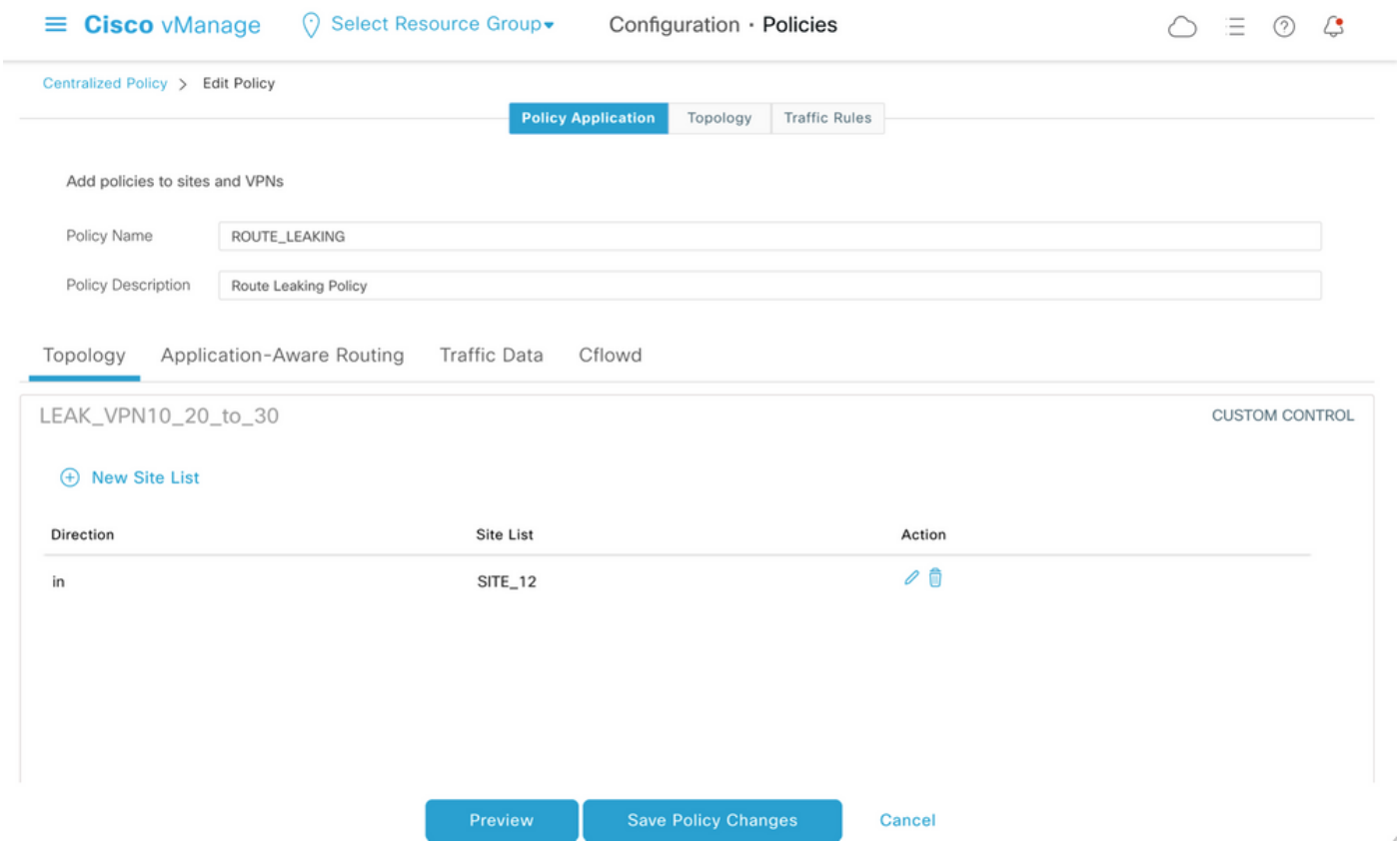




然後，兩個拓撲策略都分配到入口（傳入）方向對應的站點清單。從cE1(site-id 11)接收來自VPN 30的路由時，vSmart控制器會將其匯出到VPN 10和20的重疊管理協定(OMP)表中。



同樣，從cE2（站點ID 12）接收VPN 10和20路由時，vSmart會將來自VPN 10和20的路由匯出到VPN 30路由表中。



這裡還有一個完整的控制策略配置預覽以供參考。

```
viptela-policy:policy
 control-policy LEAK_VPN10_20_to_30
    sequence 1
     match route
      vpn-list VPN_10_20
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      export-to vpn-list VPN_30
     !
    !
  default-action accept
 !
 control-policy LEAK_VPN30_to_10_20
    sequence 1
     match route
      vpn-list VPN_30
      prefix-list _AnyIpv4PrefixList
     !
     action accept
      export-to vpn-list VPN_10_20
     !
    !
  default-action accept
 !
 lists
```

```
  site-list SITE_11
   site-id 11
  !
  site-list SITE_12
   site-id 12
  !
  vpn-list VPN_10_20
   vpn 10
   vpn 20
  !
  vpn-list VPN_30
   vpn 30
  !
  prefix-list _AnyIpv4PrefixList
   ip-prefix 0.0.0.0/0 le 32
  !
 !
!
apply-policy
 site-list SITE_12
  control-policy LEAK_VPN10_20_to_30 in
 !
 site-list SITE_11
  control-policy LEAK_VPN30_to_10_20 in
 !
!
```

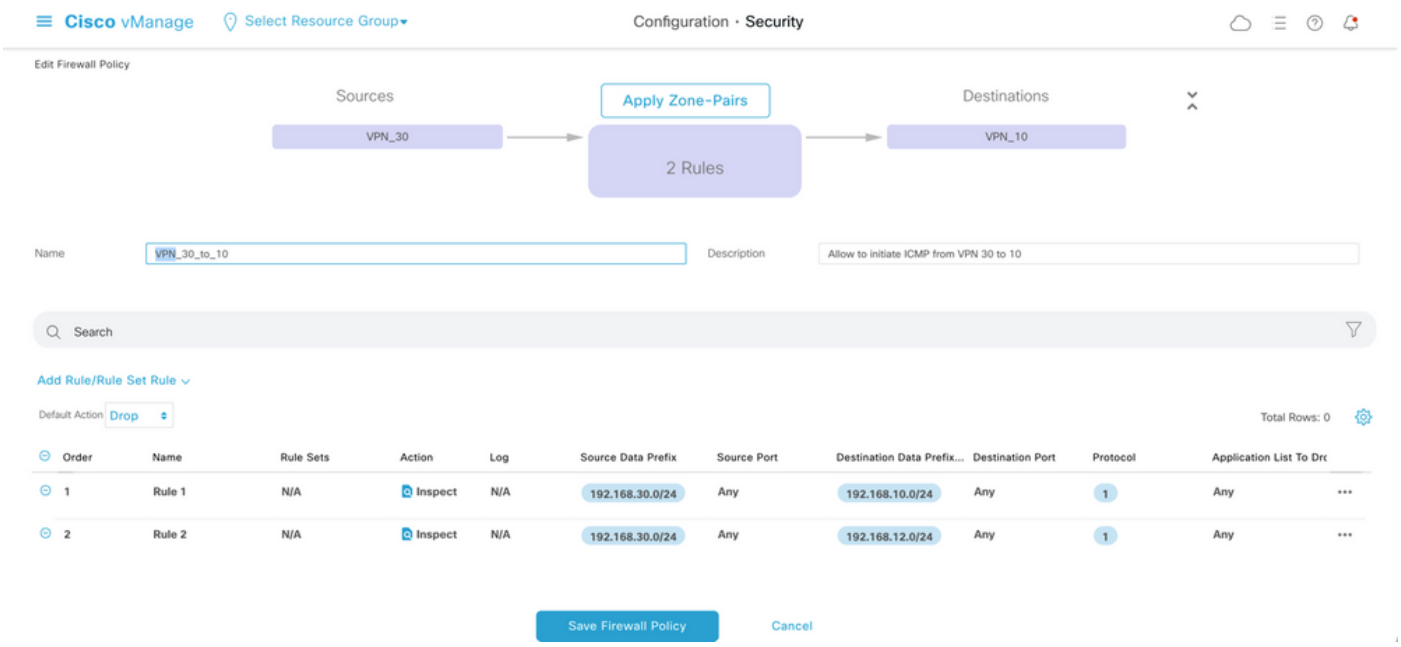
必須從vManage controller Configuration > Policies部分啟用該策略，才能在vSmart控制器上生效。

ZBFW配置

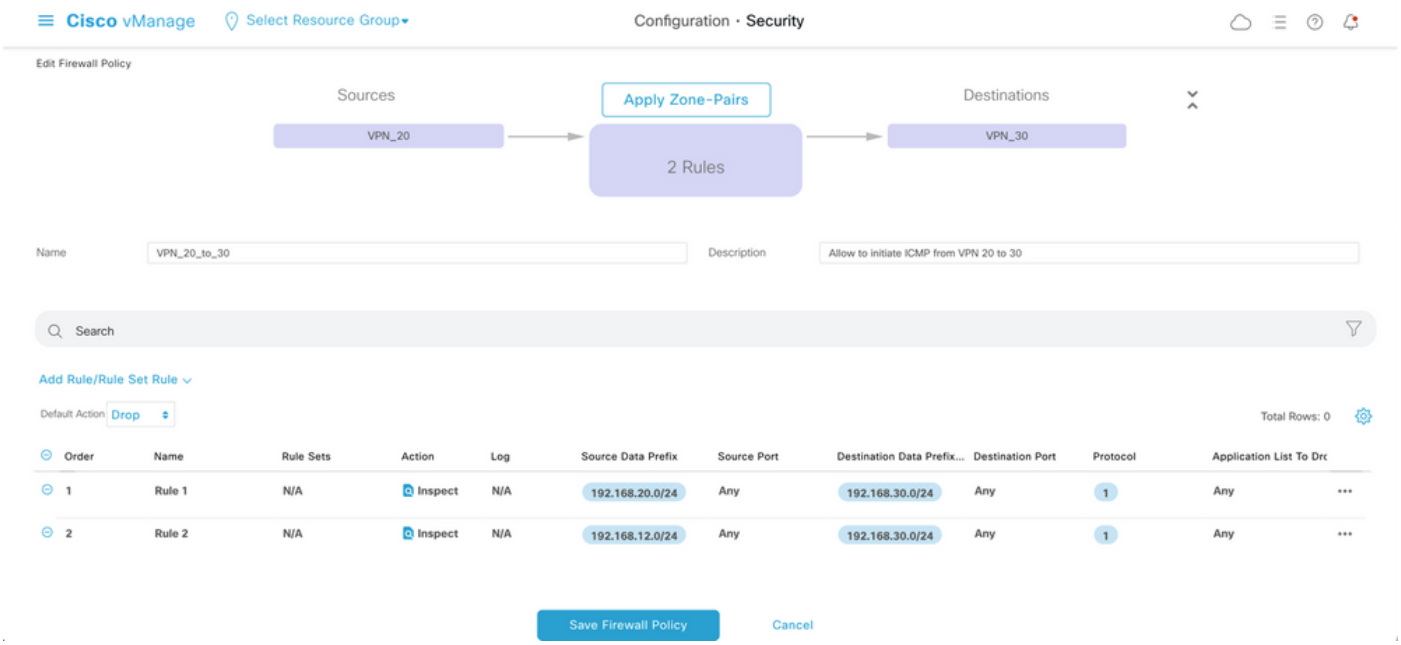
下表彙總了ZBFW以過濾要求，達到本文的演示目的。

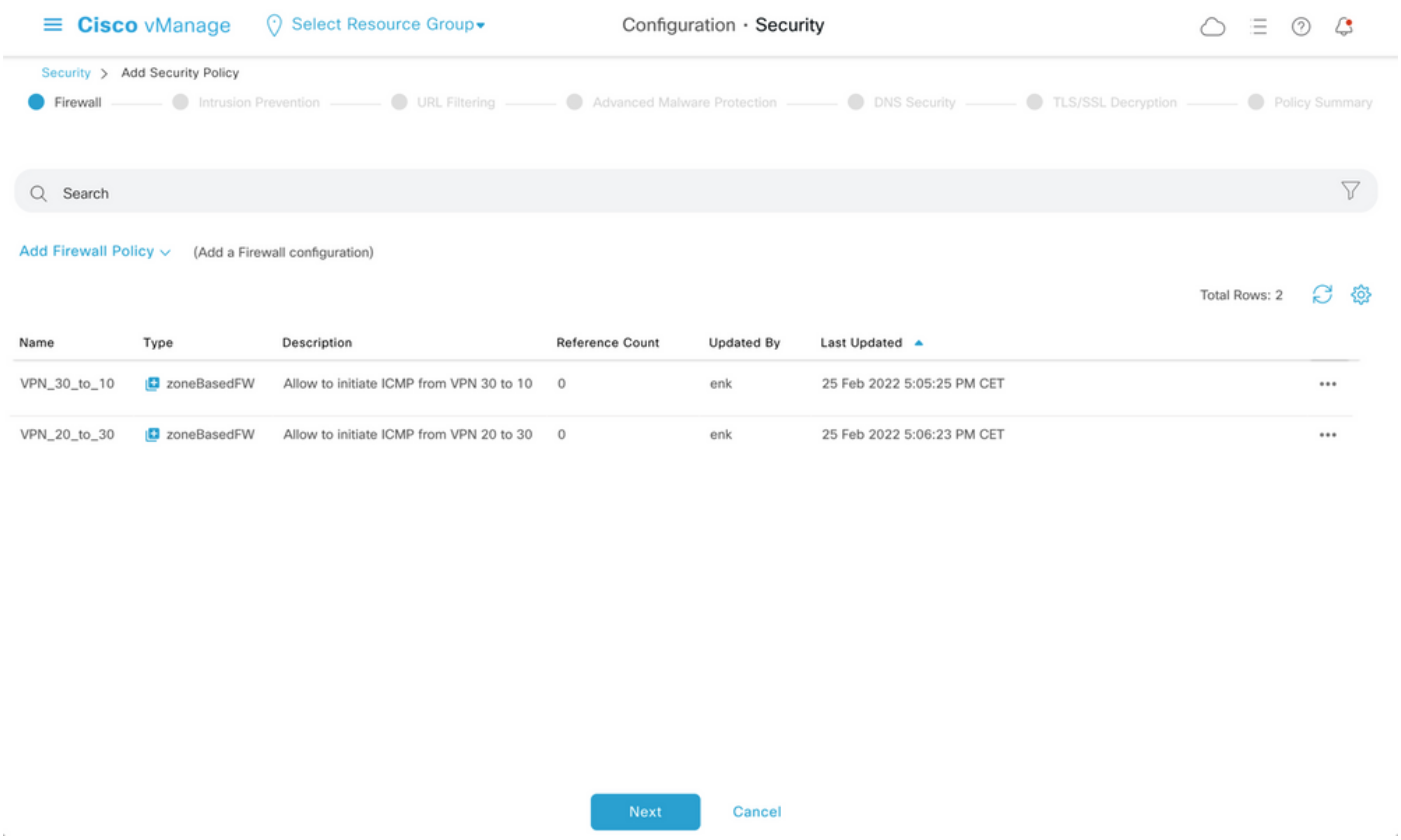
目標區域 源區域	VPN_10	VPN_2	VPN_30
VPN_10	區域內allow	拒絕	拒絕
VPN_2	拒絕	區域內allow	允許
VPN_30	允許	拒絕	區域內allow

主要目標是允許任何源自路由器cE1 VPN 30服務端且目的地為VPN 10但不目的地為VPN 20的網際網路控制消息協定(ICMP)流量。必須自動允許返回流量。



此外，必須允許來自路由器cE2服務端VPN 20的任何ICMP流量傳輸到cE1的VPN 30服務端，但不能從VPN 10傳輸。必須自動允許從VPN 30返回到VPN 20的流量。



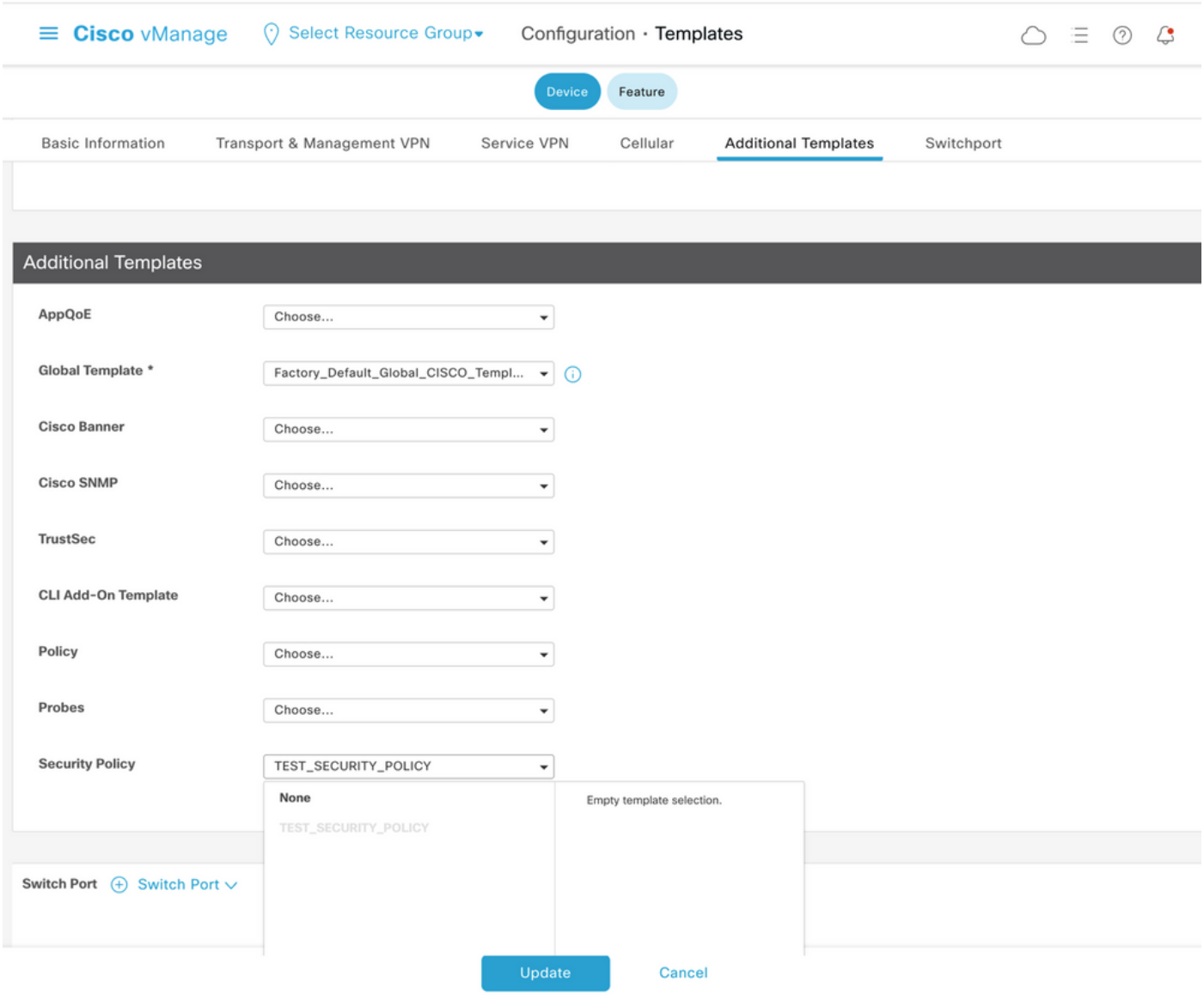


在這裡，您可以找到可供參考的ZBFW策略預覽。

```
policy
 zone-based-policy VPN_20_to_30
    sequence 1
     seq-name Rule_1
     match
      source-ip 192.168.20.0/24
      destination-ip 192.168.30.0/24
      protocol 1
     !
     action inspect
     !
    !
    sequence 11
     seq-name Rule_2
     match
      source-ip 192.168.12.0/24
      destination-ip 192.168.30.0/24
      protocol 1
     !
     action inspect
     !
    !
  default-action drop
 !
 zone-based-policy VPN_30_to_10
    sequence 1
     seq-name Rule_1
     match
      source-ip 192.168.30.0/24
      destination-ip 192.168.10.0/24
```

```
      protocol 1
     !
     action inspect
     !
    !
    sequence 11
     seq-name Rule_2
     match
      protocol 1
      source-ip 192.168.30.0/24
      destination-ip 192.168.12.0/24
     !
     action inspect
     !
    !
  default-action drop
 !
  zone VPN_10
   vpn 10
  !
  zone VPN_20
   vpn 20
  !
  zone VPN_30
   vpn 30
  !
  zone-pair ZP_VPN_20_VPN_30_VPN_20_to_30
   source-zone VPN_20
   destination-zone VPN_30
   zone-policy VPN_20_to_30
  !
  zone-pair ZP_VPN_30_VPN_10_VPN_30_to_10
   source-zone VPN_30
   destination-zone VPN_10
   zone-policy VPN_30_to_10
  !
 zone-to-nozone-internet deny
!
```

要應用安全策略，必須在裝置模板Additional Templates部分的Security Policy下拉選單部分下分配它。



更新裝置模板後，安全策略在應用安全策略的裝置上變為活動狀態。為便於本文檔中的演示，僅在cE1路由器上啟用安全策略就足夠了。

驗證

現在，您需要驗證是否已達到所需的安全策略(ZBFW)目標。

使用ping進行測試可確認從區域VPN 10到VPN 30的流量被按預期拒絕，因為沒有為從VPN 10到VPN 30的流量配置區域對。

```
R10#ping 192.168.30.30 source 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.10
.....
Success rate is 0 percent (0/5)
R10#ping 192.168.30.30 source 192.168.12.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.12.12
.....
Success rate is 0 percent (0/5)
```

類似地，根據安全策略配置的預期，允許來自VPN 20的流量到達VPN 30。

```
R20#ping 192.168.30.30 source 192.168.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.20
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R20#ping 192.168.30.30 source 192.168.12.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.12.12
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

根據策略配置的預期，允許從區域VPN 10中的VPN 30到子網192.168.10.0/24的流量。

```
R30#ping 192.168.10.10 source 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.30
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

從區域VPN 20中的VPN 30到子網192.168.20.0/24的流量被拒絕，因為沒有為此流量配置區域對（這是預期的）。

```
R30#ping 192.168.20.20 source 192.168.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.30
.....
Success rate is 0 percent (0/5)
```

當您嘗試ping IP地址192.168.12.12時，可以觀察到您感興趣的其他結果，因為該地址可能位於區域VPN 10或VPN 20中，而且從位於SD-WAN邊緣路由器cE1服務端的路由器R30的角度無法確定目標VPN。

```
R30#ping 192.168.12.12 source 192.168.30.30
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.30
.....
Success rate is 0 percent (0/5)
```

對於VRF 30中的所有源，結果都相同。這確認它不依賴於等價多路徑(ECMP)雜湊函式結果：

```
R30#ping 192.168.12.12 source 192.168.30.31
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.31
.....
Success rate is 0 percent (0/5)
R30#ping 192.168.12.12 source 192.168.30.32
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.12, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.32
.....
Success rate is 0 percent (0/5)
```

根據目標IP 192.168.12.12的測試結果，您只能猜測它位於VPN 20中，因為它不響應ICMP回應請求，並且最有可能被阻止，因為沒有將區域對配置為允許從VPN 30到VPN 20的流量（根據需要）。如果具有相同IP位址192.168.12.12的目的地位於VPN 10中並假設回應ICMP回應請求，則根據VPN 30到VPN 20之間ICMP流量的ZBFW安全策略，必須允許流量。您必須確認目標VPN。

疑難排解

方法1.從OMP表中查詢目標VPN

對cE1上的路由表進行簡單檢查無助於瞭解實際目的VPN。您可以從輸出中獲得的最有用資訊是目的地(169.254.206.12)的系統IP，而且不會發生ECMP。

```
cE1# show ip route vrf 30 192.168.12.0 255.255.255.0

Routing Table: 30
Routing entry for 192.168.12.0/24
  Known via "omp", distance 251, metric 0, type omp
  Last update from 169.254.206.12 on Sdwan-system-intf, 01:34:24 ago
  Routing Descriptor Blocks:
  * 169.254.206.12 (default), from 169.254.206.12, 01:34:24 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
```

要查詢目標VPN，首先需要從cE1上的OMP表中查詢服務標籤以獲取感興趣的字首。

```
cE1#show sdwan omp routes vpn 30 192.168.12.0/24
Generating output, this might take time, please wait ...
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
                  PATH                        ATTRIBUTE
FROM PEER         ID     LABEL    STATUS      TYPE       TLOC IP          COLOR            ENCAP  PREFEREN
-----------------------------------------------------------------------------------------------------------
169.254.206.4     12     1007     C,I,R       installed  169.254.206.12   private2         ipsec  -
```

可以看到標籤值為1007。最後，如果在vSmart控制器上檢查了來自具有系統IP 169.254.206.12的路由器的所有服務，就可以找到目標VPN。

```
vsmart1# show omp services family ipv4 service VPN originator 169.254.206.12
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                PATH
VPN    SERVICE  ORIGINATOR      FROM PEER        ID     LABEL    STATUS
-------------------------------------------------------------------------
1      VPN      169.254.206.12  169.254.206.12   82     1003     C,I,R
2      VPN      169.254.206.12  169.254.206.12   82     1004     C,I,R
10     VPN      169.254.206.12  169.254.206.12   82     1006     C,I,R
17     VPN      169.254.206.12  169.254.206.12   82     1005     C,I,R
20     VPN      169.254.206.12  169.254.206.12   82     1007     C,I,R
```

根據VPN標籤1007，可以確認目的VPN為20。

方法2.藉助平台命令查詢目標VPN

要藉助平台命令查詢目標VPN，首先需要藉助show ip vrf detail 30或show platform software ip f0 cef table *摘要命令，獲取cE1路由器上VPN 30的內部VRF ID 。

```
cE1#show ip vrf detail 30 | i Id
VRF 30 (VRF Id = 1); default RD 1:30; default VPNID
```

```
cE1#show platform software ip f0 cef table * summary | i VRF|^30
Name              VRF id  Table id    Protocol         Prefixes    State
30                1       1           IPv4             21          hw: 0x561b60f07a50 (created)
```

在本例中，VRF ID 1被分配給名為30的VRF。平台命令顯示SD-WAN軟體中的輸出鏈元素(OCE)對象鏈，該對象表示確定Cisco IOS-XE軟體中資料包路徑的內部轉發邏輯：

```
cE1#show platform software ip F0 cef table index 1 prefix 192.168.12.0/24 oce
=== Prefix OCE ===
Prefix/Len: 192.168.12.0/24
  Next Obj Type: OBJ_SDWAN_NH_SLA_CLASS
  Next Obj Handle: 0xf800045f, urpf: 0
  Prefix Flags: unknown
  aom id: 1717, HW handle: 0x561b60eeba20 (created)
```

感興趣的字首指向可以進一步驗證的ID為0xf800045f的Service Level Agreement(SLA)類型別(OBJ_SDWAN_NH_SLA_CLASS)的下一跳對象，如下所示：

```
cE1#show platform software sdwan F0 next-hop sla id 0xf800045f
SDWAN Nexthop OCE

SLA: num_class 16, client_handle 0x561b610c3f10, ppe addr 0xdbce6c10
  SLA_0: num_nhops 1, Fallback_sla_flag TDL_FALSE, nhobj_type SDWAN_NH_INDIRECT
  ECMP: 0xf800044f 0xf800044f 0xf800044f 0xf800044f
        0xf800044f 0xf800044f 0xf800044f 0xf800044f
        0xf800044f 0xf800044f 0xf800044f 0xf800044f
        0xf800044f 0xf800044f 0xf800044f 0xf800044f
  SLA_1: num_nhops 0, Fallback_sla_flag TDL_FALSE, nhobj_type ADJ_DROP
  ECMP: 0xf800000f 0xf800000f 0xf800000f 0xf800000f
        0xf800000f 0xf800000f 0xf800000f 0xf800000f
        0xf800000f 0xf800000f 0xf800000f 0xf800000f
        0xf800000f 0xf800000f 0xf800000f 0xf800000f
```

這是一個較長的輸出，因此跳過從2到15的SLA類，因為未配置回退SLA類，並且所有類都指向與

SLA 1相同的特殊DROP鄰接關係。主要興趣是SLA 0的間接型別(SDWAN_NH_INDIRECT)的下一跳對象。我們還可以注意到，沒有ECMP，所有ID都相同(0xf800044f)。 可進一步驗證以找到最終目標VPN和服務標籤。

```
cE1#show platform software sdwan F0 next-hop indirect id 0xf800044f
SDWAN Nexthop OCE

Indirect: client_handle 0x561b610f8140, ppe addr 0xd86b4cf0
  nhobj_type: SDWAN_NH_LOCAL_SLA_CLASS, nhobj_handle: 0xf808037f
  label: 1007, vpn: 20, sys-ip: 169.254.206.12, vrf_id: 1, sla_class: 1
```

方法3.使用資料包跟蹤工具查詢目標VPN

查詢目標VPN的另一種方法是packet-trace工具，它可以即時分析通過路由器運行的真實資料包。調試條件設定為僅與IP地址192.168.12.12之間的流量匹配。

```
cE1#debug platform condition ipv4 192.168.12.12/32 both
cE1#debug platform packet-trace packet 10
 Please remember to turn on 'debug platform condition start' for packet-trace to work
cE1#debug platform condition start
```

接下來，如果流量是通過ping的幫助從R30發起的，則可以在cE1上看到匹配的資料包並檢查每個資料包的詳細資訊。在本例中，它是第一個資料包編號0，例如。最重要的線條突出顯示為<<<<<符號。

```
cE1#show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
1     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
2     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
3     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
4     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)
5     Gi6                       Tu3                       DROP   52  (FirewallL4Insp)


cE1#show platform packet-trace packet 0
Packet: 0           CBUG ID: 0
Summary
  Input     : GigabitEthernet6
  Output    : Tunnel3
  State     : DROP 52  (FirewallL4Insp) <<<<<<<<<<<<<<<<<<<<<<<<<
  Timestamp
    Start   : 161062920614751 ns (03/24/2022 16:19:31.754050 UTC)
    Stop    : 161062920679374 ns (03/24/2022 16:19:31.754114 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet6
    Output      :
```

```
    Source      : 192.168.30.30
    Destination : 192.168.12.12
    Protocol    : 1 (ICMP)
  Feature: SDWAN Forwarding
    SDWAN adj OCE:
    Output       : GigabitEthernet3
    Hash Value   : 0xda
    Encap        : ipsec
    SLA          : 0
    SDWAN VPN    : 20
    SDWAN Proto  : IPV4
    Out Label    : 1007 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Local Color  : private2
    Remote Color : private2
    FTM Tun ID   : 218
    SDWAN Session Info
      SRC IP       : 192.168.10.11
      SRC Port     : 12366
      DST IP       : 192.168.10.12
      DST Port     : 12346
      Remote System IP : 169.254.206.12
      Lookup Type : TUN_DEMUX
      Service Type : NONE
  Feature: ZBFW
    Action  : Drop
    Reason  : No Zone-pair found <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Zone-pair name         : N/A <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Class-map name         : N/A
    Policy    name         : N/A
    Input interface        : GigabitEthernet6
    Egress interface       : Tunnel3
    Input  VPN ID          : 30
    Output VPN ID          : 20 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Input  VRF ID:Name     : 1:30
    Output VRF ID:Name     : 1:30
    AVC Classification ID  : 0
    AVC Classification name: N/A
    UTD Context ID         : 0
```

packet-trace告知通過ping傳送的所有5個ICMP回應封包都已捨棄，而且捨棄程式碼為52(FirewallL4Insp)。 節功能：SDWAN轉發指示目標VPN為20，並且隧道資料包內部報頭中的服務標籤1007用於轉發，以便在cE2上指定目標VPN。部分功能：ZBFW進一步確認資料包被丟棄，因為沒有為來自輸入VPN 20且目的地為VPN 30區域的流量配置區域對。

故障轉移導致的潛在問題

如果路由192.168.12.0/24被R20撤銷或無法從VRF 20中的cE2繼續訪問，會發生什麼情況？雖然從VRF 30的角度來看，子網是相同的，因為ZBFW安全策略對從區域VPN 30到區域VPN 20和10的流量處理的方式不同，所以可能會導致不希望的結果（例如允許的流量），但一定不能是相反的。

例如，如果您模擬cE2和R20路由器之間的鏈路故障。這會導致從vSmart控制器上的VPN 20路由表中退出192.168.12.0/24路由，相反，VPN 10路由會洩漏到VPN 30路由表中。根據在cE1上應用的安全策略，允許從VPN 30到VPN 10的連線（從安全策略的角度來看這是預期的，但對於兩個VPN中呈現的特定子網來說不是理想的）。

```
cE1#show platform packet-trace packet 0
Packet: 0           CBUG ID: 644
Summary
  Input     : GigabitEthernet6
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 160658983624344 ns (03/24/2022 16:12:47.817059 UTC)
    Stop    : 160658983677282 ns (03/24/2022 16:12:47.817112 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet6
    Output      :




    Source      : 192.168.30.30
    Destination : 192.168.12.12
    Protocol    : 1 (ICMP)
  Feature: SDWAN Forwarding
    SDWAN adj OCE:
    Output       : GigabitEthernet3
    Hash Value   : 0xda
    Encap        : ipsec
    SLA          : 0
    SDWAN VPN    : 10
    SDWAN Proto  : IPV4
    Out Label    : 1006
    Local Color  : private2
    Remote Color : private2
    FTM Tun ID   : 188
    SDWAN Session Info
      SRC IP       : 192.168.10.11
      SRC Port     : 12366
      DST IP       : 192.168.10.12
      DST Port     : 12346
      Remote System IP : 169.254.206.12
      Lookup Type : TUN_DEMUX
      Service Type : NONE
  Feature: ZBFW
    Action  : Fwd
    Zone-pair name         : ZP_VPN_30_VPN_10_VPN_30_to_10
    Class-map name         : VPN_30_to_10-seq-11-cm_
    Policy    name         : VPN_30_to_10
    Input interface        : GigabitEthernet6
    Egress interface       : Tunnel3
    Input  VPN ID          : 30
    Output VPN ID          : 10
    Input  VRF ID:Name     : 1:30
    Output VRF ID:Name     : 1:30
    AVC Classification ID  : 0
    AVC Classification name: N/A
    UTD Context ID         : 0
```

```
Feature: IPSec
  Result    : IPSEC_RESULT_SA
  Action    : ENCRYPT
  SA Handle : 74
  Peer Addr : 192.168.10.12
  Local Addr: 192.168.10.11
```

請注意，標籤1006而不是1007，輸出VPN ID現在是10而不是20。此外，根據ZBFW安全策略允許該資料包，並提供了相應的區域對、類對映和策略名稱。

由於VPN 30的路由表中儲存了最早的路由，因此會出現一個更大的問題，在這種情況下，VPN 10路由是在初始控制策略應用VPN 20路由洩漏到vSmart上的VPN 30 OMP表中之後出現的。想象一下，當原始概念與本文所述的ZBFW安全策略邏輯完全相反時，會出現什麼情況。例如，目標是允許從VPN 30到VPN 20而不是到VPN 10的流量。如果在初始策略配置後允許該流量，則在故障或192.168.12.0/24路由從VPN 20撤銷後，即使恢復後，流量仍然被阻止到192.168.12.0/24子網，因為192.168.12.0/24路由仍然從VPN 10洩漏。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。