SD-WANゾーンベースファイアウォール(ZBFW)とルート漏出の設定

内容

概要

このドキュメントでは、Virtual Private Network（VPN；バーチャルプライベートネットワーク）間のルート漏出を使用したゾーンベースファイアウォール(ZBFW)の設定、確認、トラブルシューティングの方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco SD-WANオーバーレイは、初期設定を開始します
- vManage User Interface(UI)からのZBFW設定
- vManage UIからのルートリーク制御ポリシー設定

使用するコンポーネント

デモンストレーションの目的で、次のソフトウェアを使用しました。

- Cisco SD-WAN vSmartコントローラ(20.6.2ソフトウェアリリース)
- Cisco SD-WAN vManageコントローラ(20.6.2ソフトウェアリリース)
- コントローラモードで稼働する17.6.2ソフトウェアリリースのCisco IOS®-XE Catalyst

8000V仮想エッジプラットフォームルータ2台
- 自律モードで動作する17.6.2ソフトウェアリリースのCisco IOS-XE Catalyst 8000V仮想エッジプラットフォームルータ3台

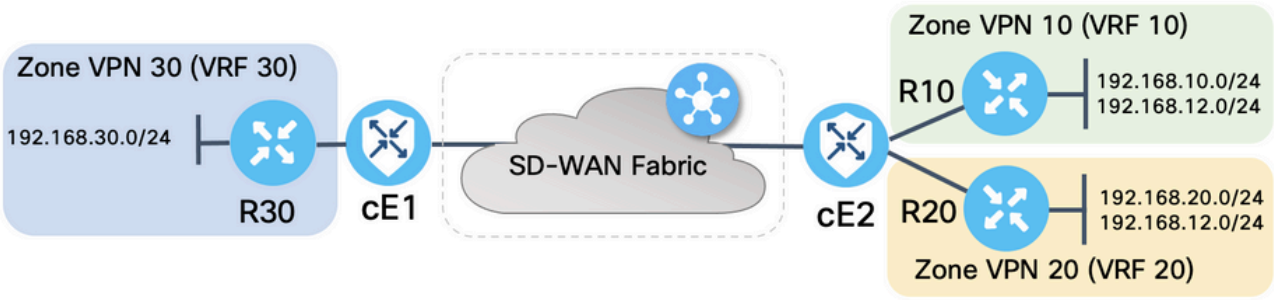
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、ルータがSD-WANオーバーレイで宛先VPNマッピングを決定する方法、およびVPN間のルート漏洩の検証とトラブルシューティングの方法について説明します。また、同じサブネットが異なるVPNからアドバタイズされる場合のパス選択の特性と、この問題によって発生する可能性のある問題についても説明します。

設定

ネットワーク図



両方のSD-WANルータは、SD-WANコントローラとの制御接続およびこれらの間のデータプレーン接続を確立するための基本パラメータで設定されました。この設定の詳細は、このドキュメントの目的では範囲外です。次の表は、VPN、サイトID、およびゾーンの割り当てをまとめたものです。

	cE1	cE2
site-id	11	12
VPN	30	10,20
system-ip	169.254.206.11	169.254.206.12

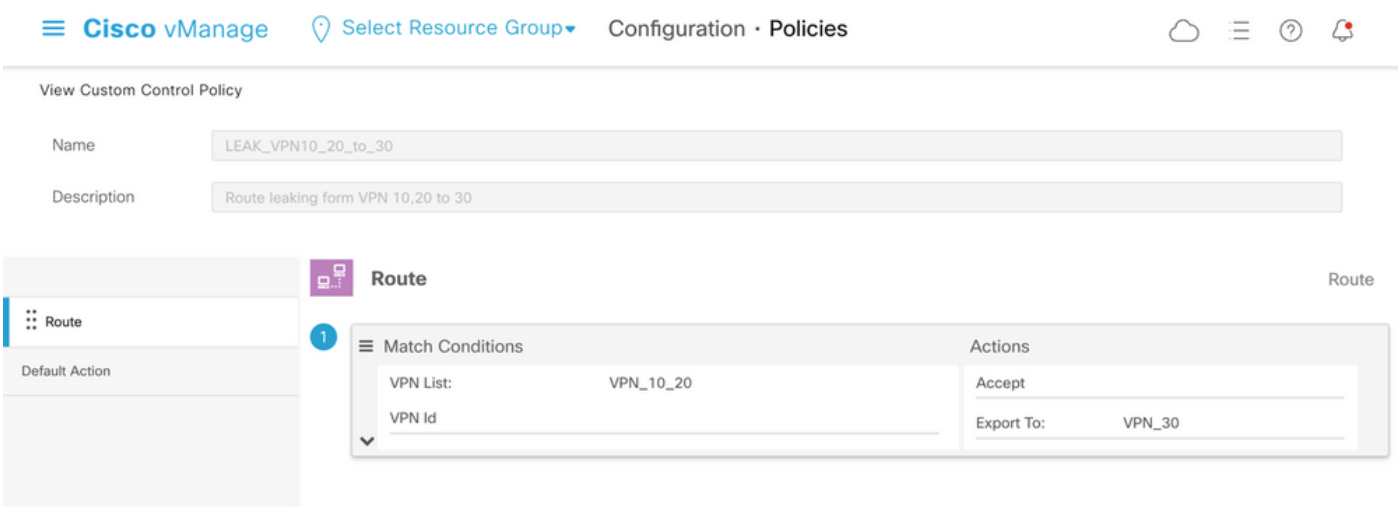
サービス側のルータは、対応するSD-WANルータをポイントする各Virtual Routing and Forwarding(VRF)でスタティックデフォルトルートを使用して設定されました。同様に、SD-WANエッジルータは、対応するサブネットをポイントするスタティックルートで設定されています。ルート漏出とZBFWに関する潜在的な問題を実証するため、cE2のサービス側のルータのサブネットは同じ192.168.12.0/24です。cE2の背後にある両方のルータには、同じIPアドレス192.168.12.12のホストをエミュレートするように設定が設定されています。

Cisco IOS-XEルータR10、R20、およびR30は、このデモンストレーションで主にエンドホストをエミュレートするSD-WANエッジルートのサービス側で自律モードで動作することに注意してください。SD-WANエッジルータのVRFのインターフェイスから発信されたトラフィックは、対

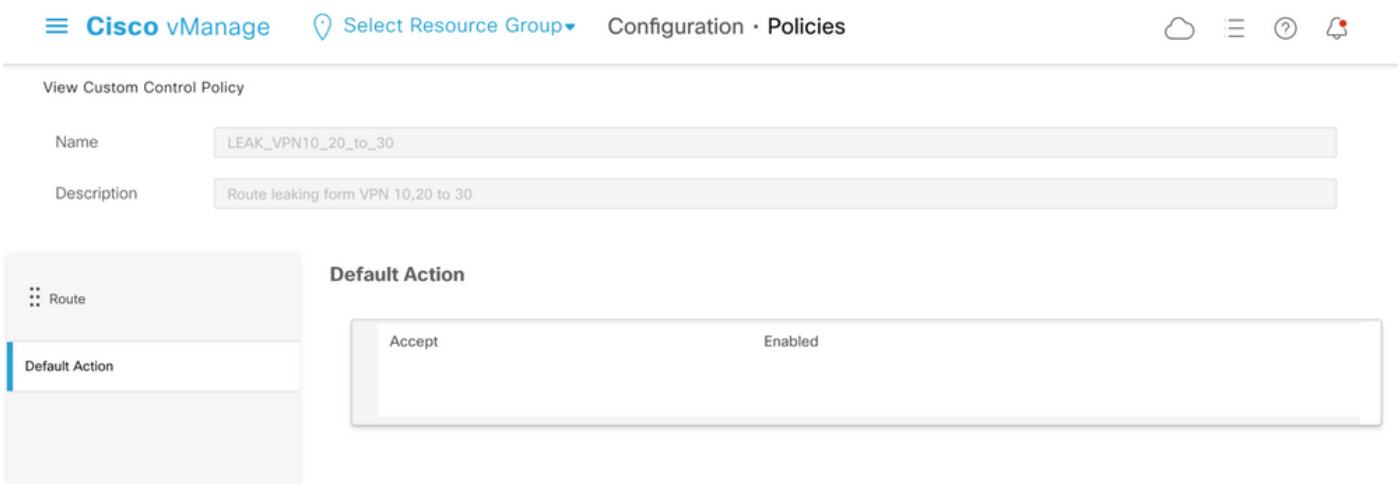
応するZBFWゾーンで発信されたトラフィックではなく、エッジルータの特別なセルフゾーンに属するトラフィックと見なされるため、サービスサイドルータなどの実ホストの代わりにループバックインターフェイスをは使用できません。そのため、ZBFWゾーンをVRFと同じとみなすことはできません。セルフゾーンの詳細な説明は、この記事の範囲外です。

ルートリークの設定

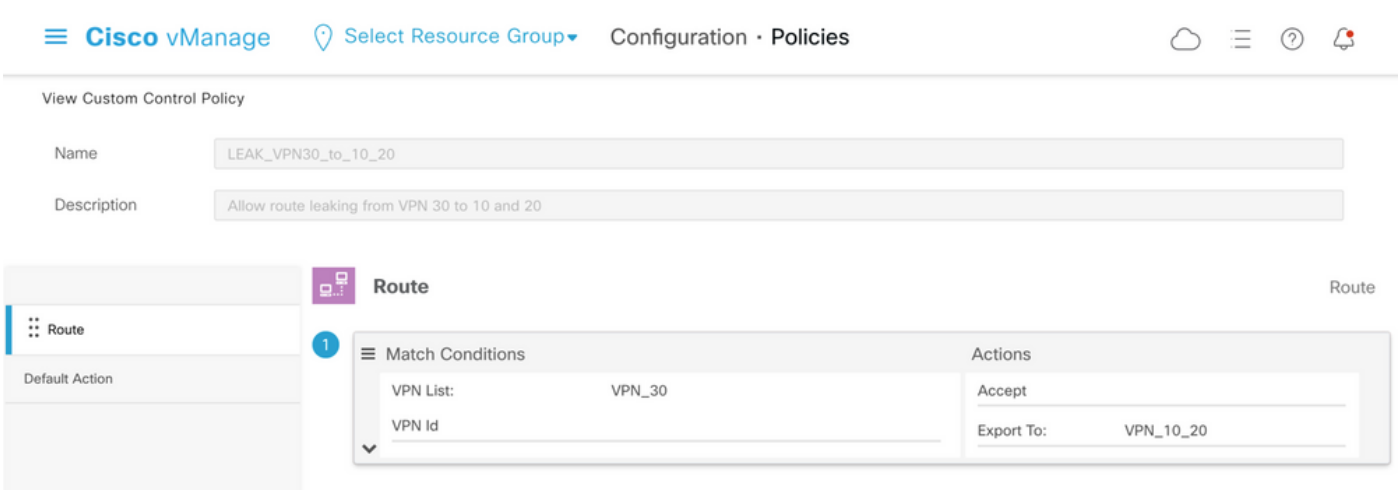
主な制御ポリシー設定の目的は、VPN 10および20からVPN 30へのすべてのルートのリークを許可することです。VRF 30はルータcE1にのみ存在し、VRF 10および20はルータcE2にのみ設定されます。そのためには、2つのトポロジ（カスタムコントロール）ポリシーを設定しました。VPN 10および20からすべてのルートをVPN 30にエクスポートするトポロジを次に示します。

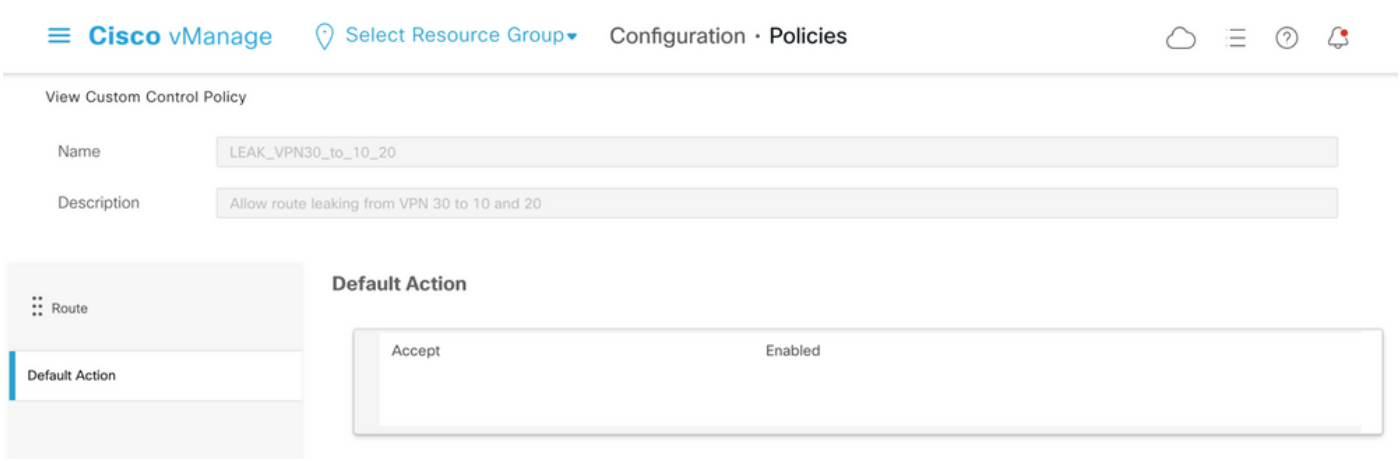


[Default Action]が[**Allow**]に設定されている場合は、TLOCアドバタイズメントまたは通常のVPN内ルートのアドバタイズメントが誤ってブロックされるのを回避できます。

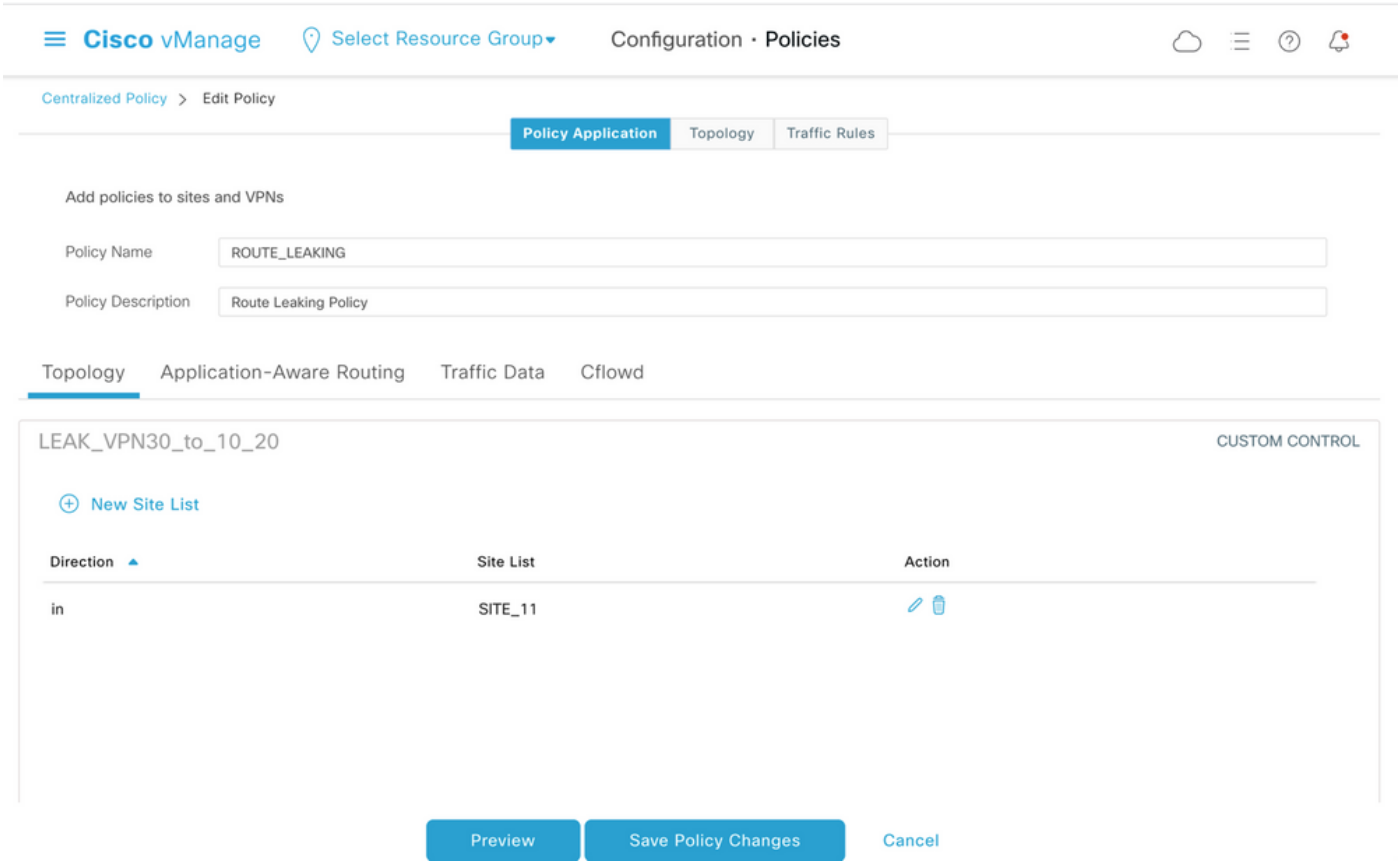


同様に、トポロジポリシーは、VPN 30からVPN 10および20へのルーティング情報の逆アドバタイズメントを許可するように設定されました。

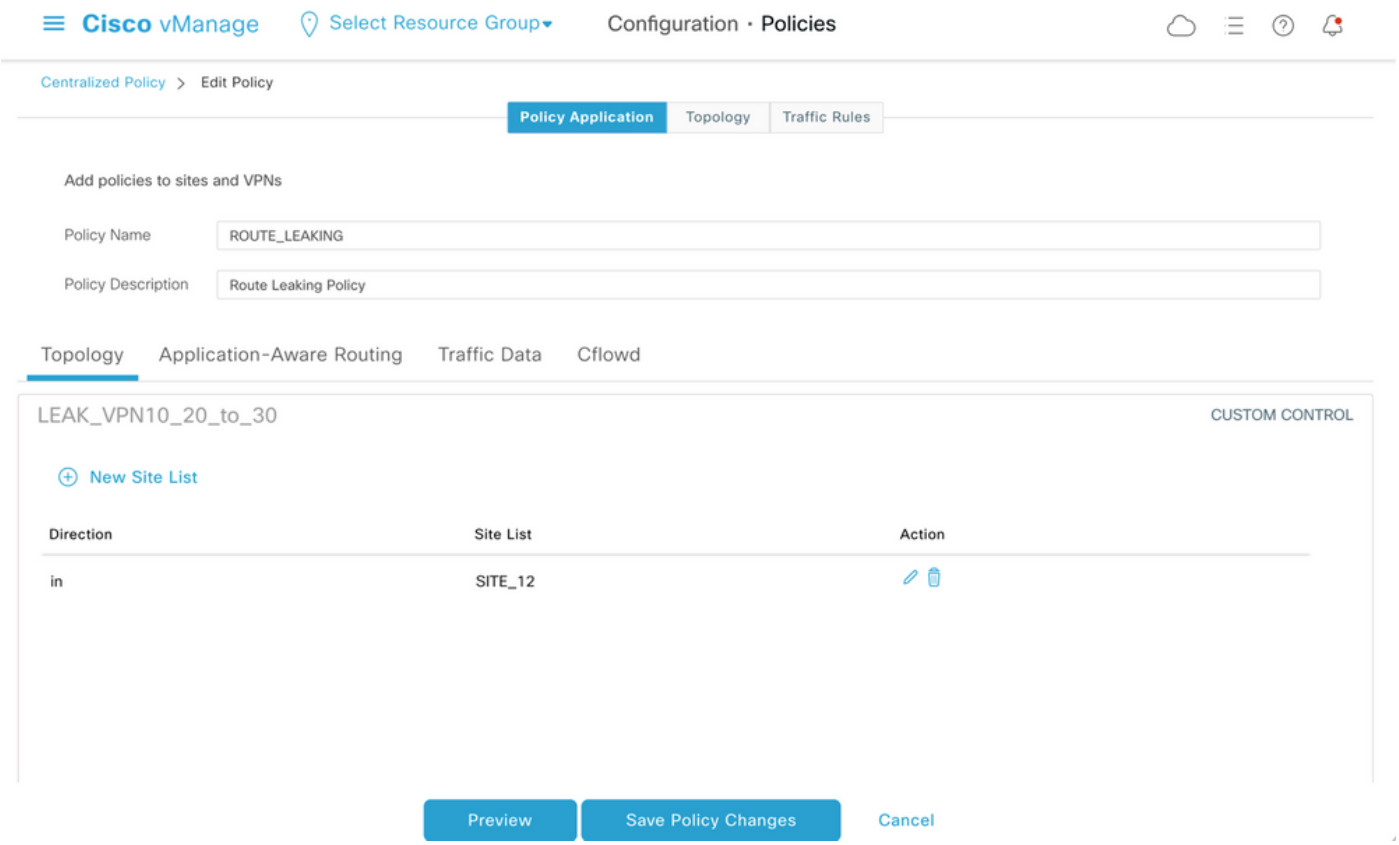




次に、両方のトポロジポリシーが、入力（着信）方向に対応するサイトリストに割り当てられます。VPN 30からのルートは、cE1(site-id 11)から受信されると、vSmartコントローラによってVPN 10および20のオーバーレイ管理プロトコル(OMP)テーブルにエクスポートされます。



同様に、VPN 10および20からのルートは、vSmartによってVPN 30ルーティングテーブルにエクスポートされ、cE2(site-id 12)からのVPN 10および20ルートを受信します。



また、参照用の完全な制御ポリシー設定のプレビューも示します。

```
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 ! !
```

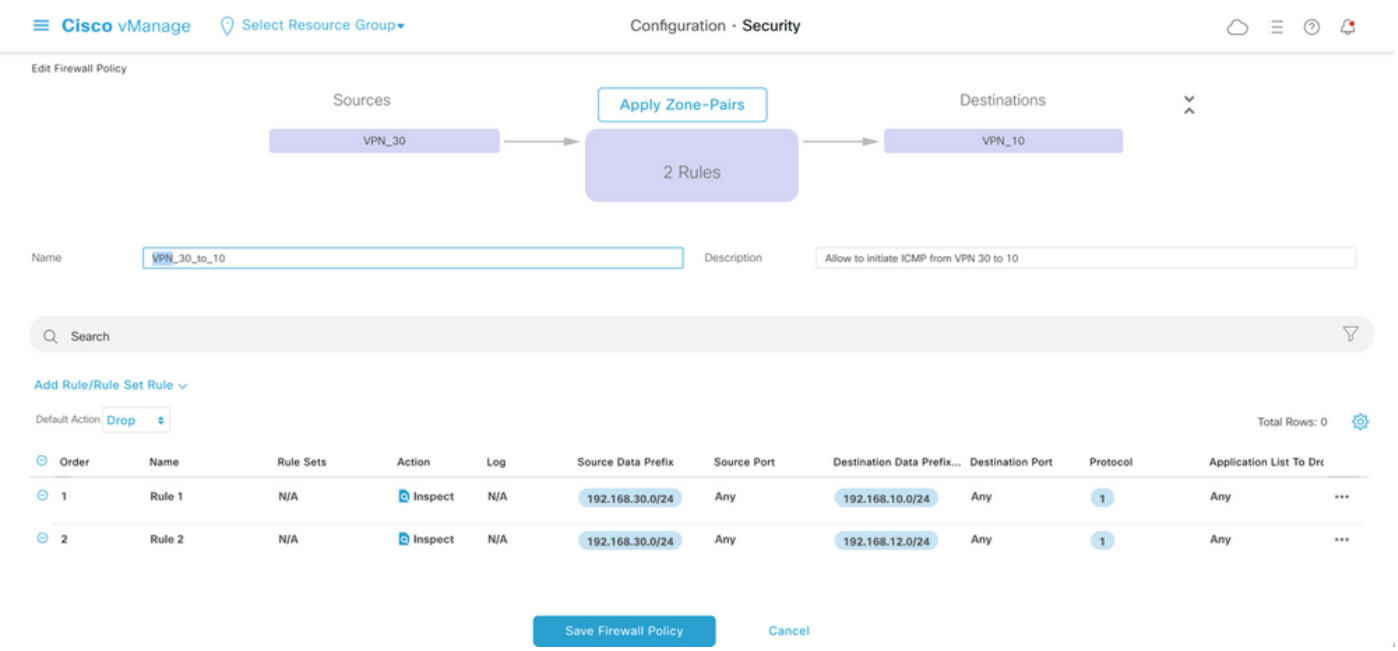
vSmartコントローラで有効にするには、[vManage controller **Configuration] > [Policies]セクション**からポリシーをアクティブにする必要があります。

ZBFWの設定

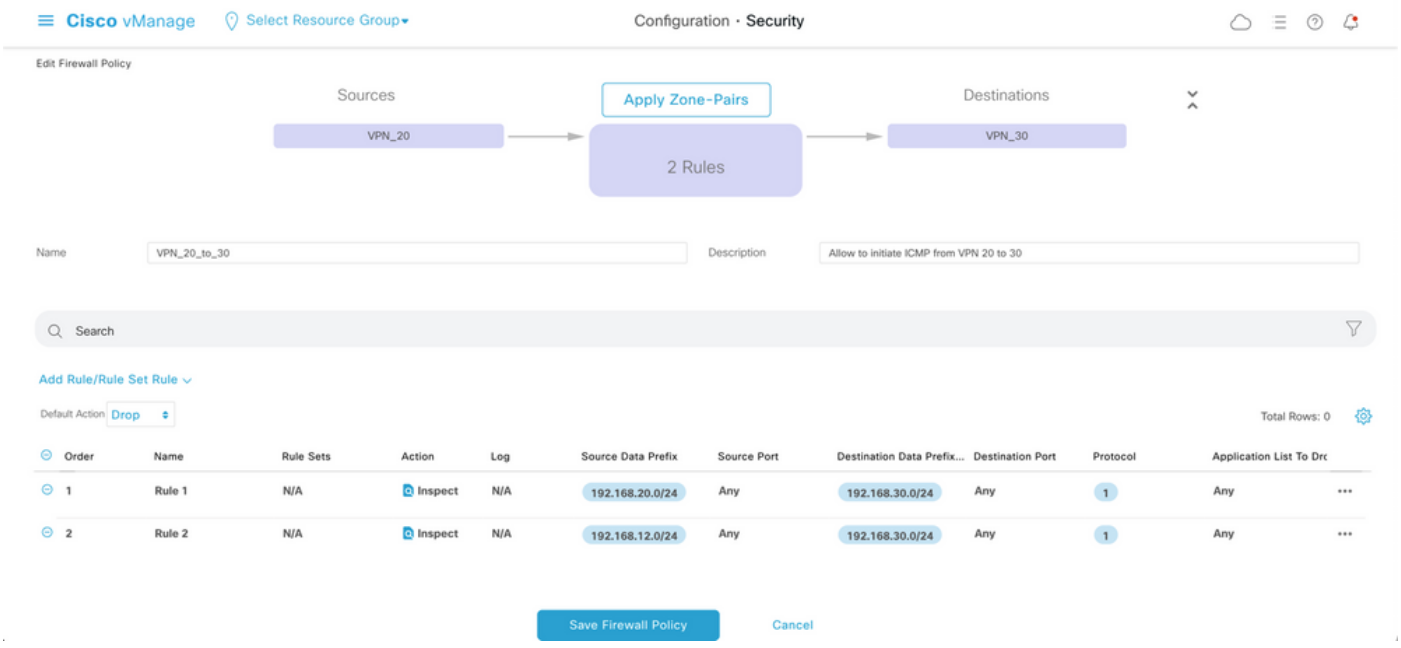
この記事のデモンストレーションの目的で要件をフィルタリングするためのZBFWを要約した表を次に示します。

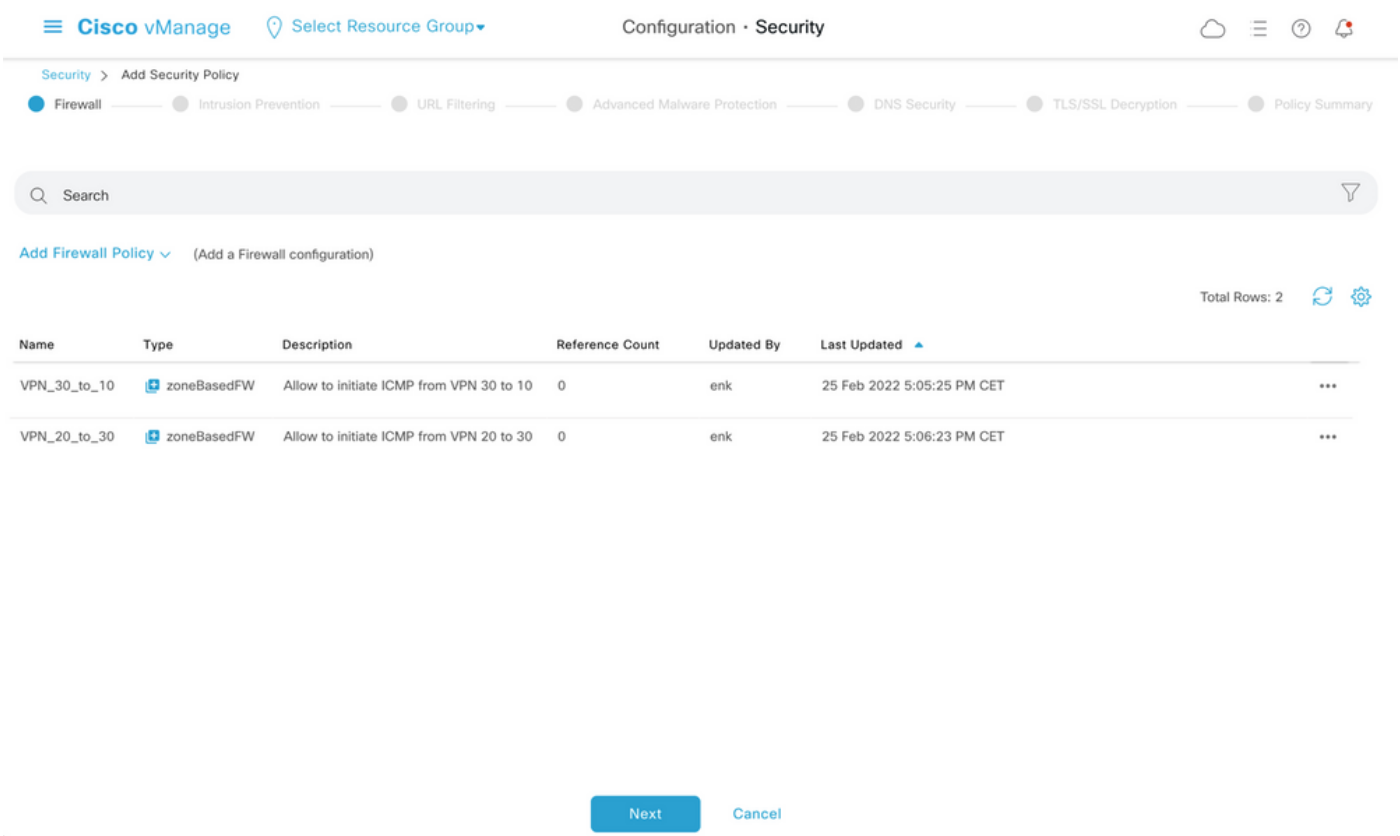
宛先ゾーン ソースゾーン	VPN_10	VPN_20	VPN_30
VPN_10	intra-zone allow	拒否	拒否
VPN_20	拒否	intra-zone allow	プライベート ネットワーク間で
VPN_30	プライベート ネットワーク間で	拒否	intra-zone allow

主な目的は、ルータcE1 VPN 30のサービス側から発信され、VPN 10宛ではなくVPN 20宛てのInternet Control Message Protocol(ICMP)トラフィックを許可することです。リターントラフィックは自動的に許可される必要があります。



また、ルータcE2サービス側VPN 20からのICMPトラフィックは、VPN 30サービス側cE1への通過を許可する必要がありますが、VPN 10からの通過は許可しません。VPN 30からVPN 20へのリターントラフィックは自動的許可されます。

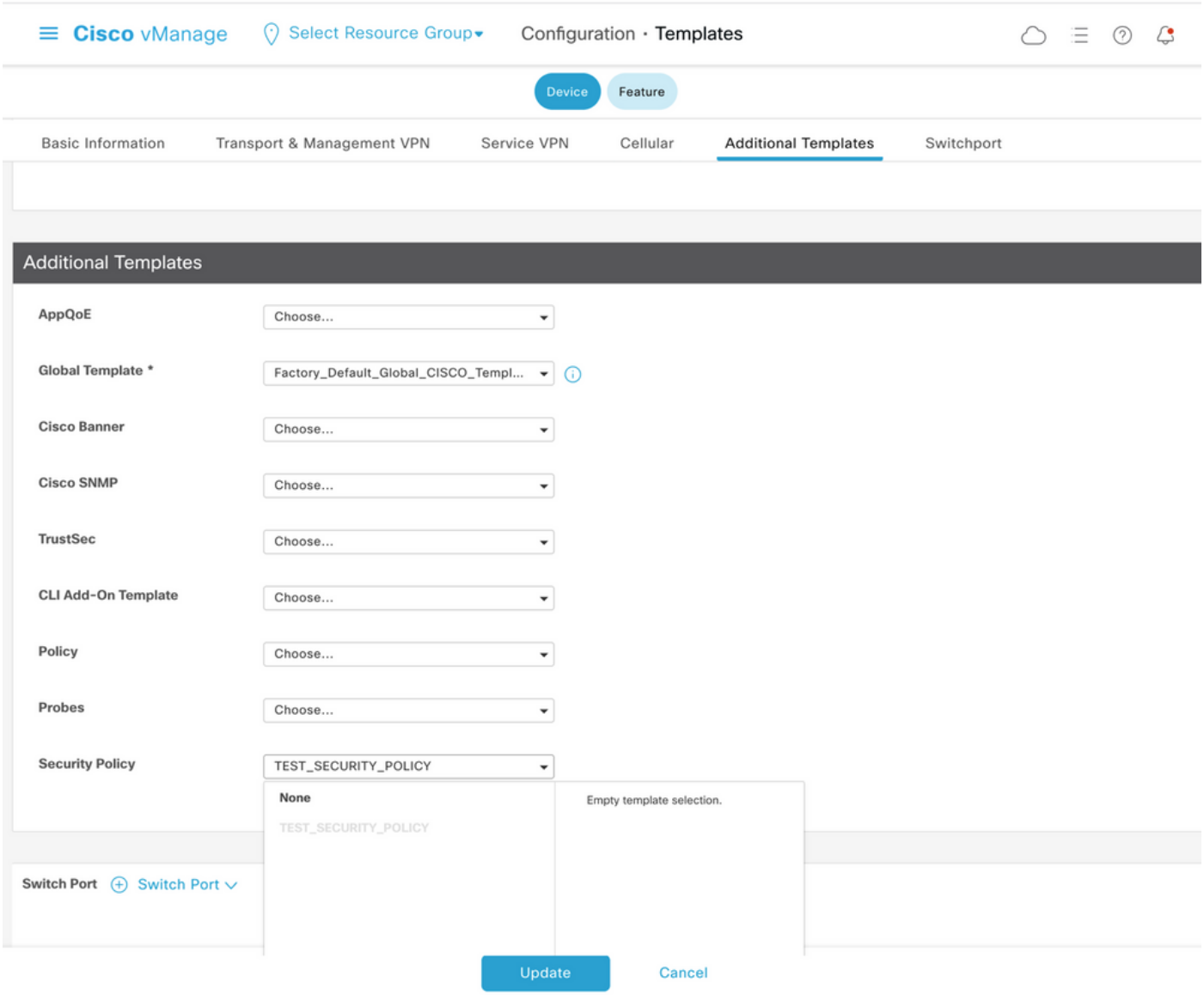




ここでは、参照用にZBFWポリシーのプレビューを確認できます。

```
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 !
```

セキュリティポリシーを適用するには、デバイステンプレートの[追加テンプレート]セクションの[セキュリティポリシー]ドロップダウンメニューの下に割り当てる必要があります。



デバイステンプレートが更新されると、セキュリティポリシーが適用されたデバイスでセキュリティポリシーがアクティブになります。このドキュメントのデモンストレーションを行うために、cE1ルータでのみセキュリティポリシーを有効にするのに十分でした。

確認

次に、必要なセキュリティポリシー(ZBFW)の目標が達成されたことを確認する必要があります。

pingを使用してテストすると、VPN 10からVPN 30へのトラフィックにゾーンペアが設定されていないため、ゾーンVPN 10からVPN 30へのトラフィックが期待どおりに拒否されることを確認できます。

```
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)
```

同様に、VPN 20からのトラフィックは、セキュリティポリシーの設定で想定どおりにVPN 30に許可されます。

```
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
```

ゾーンVPN 10のVPN 30からサブネット192.168.10.0/24へのトラフィックは、ポリシー設定によって期待どおりに許可されます。

```
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
```

このトラフィックに対してゾーンペアが設定されていないため、VPN 30からサブネット192.168.20.0/24へのトラフィックはゾーンVPN 20で拒否されます。これは予期されています。

```
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)
```

IPアドレス192.168.12.12はゾーンVPN 10またはVPN 20に存在し、SD-WANエッジルータcE1のサービス側に位置するルータR30の観点から宛先VPNを判別できないため、pingを試みた場合に発生する可能性のある追加のの結果です。

```
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)
```

結果は、VRF 30のすべてのソースで同じです。これにより、Equal-Cost Multi-Path(ECMP)ハッシュ関数の結果に依存しないことが確認されます。

```
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)
```

宛先IP 192.168.12.12のテスト結果から、VPN 20がICMPエコー要求に応答せず、VPN 30からVPN 20（必要に応じて）へのトラフィックを許可するようにゾーンペアが設定されていないため、ブロックされる可能性が高いため、VPN 20内に0が存在のみを推測します。 同じIPアドレス192.168.12.12の宛先がVPN 10にあり、ICMPエコー要求に応答すると想定される場合は、VPN 30からVPN 20へのICMPトラフィックに対するZBFWセキュリティポリシーに従って、トラフィックを許可する必要があります。宛先VPNを確認する必要があります。

トラブルシュート

方法1. OMPテーブルから宛先VPNを検索する

cE1のルーティングテーブルを簡単にチェックしても、実際の宛先VPNを理解するのに役立ちません。出力から得られる最も有用な情報は、宛先(169.254.206.12)のシステムIPであり、ECMPは発生しません。

```
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
```

宛先VPNを見つけるには、まず、対象のプレフィクスのcE1のOMPテーブルからサービスラベルを見つける必要があります。

```
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 PREFERENCE ---
-------------------------------------------------------------------------------------------
-------- 169.254.206.4 12 1007 C,I,R installed 169.254.206.12 private2 ipsec -
```

ラベル値が1007であることがわかります。最後に、vSmartコントローラで、system-IP 169.254.206.12を持つルータから発信されるすべてのサービスがチェックされると、宛先VPNが検出されます。

```
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
```

VPNラベル1007に基づいて、宛先VPNが20であることを確認できます。

方法2.プラットフォームコマンドを使用して宛先VPNを検索する

プラットフォームコマンドを使用して宛先VPNを調べるには、まず、**show ip vrf detail 30またはshow platform software ip f0 cef table * summaryコマンドを使用して、cE1ルータのVPN 30の内部VRF IDを取得する必要があります。**

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

この場合、30という名前のVRFにVRF ID 1が割り当てられています。プラットフォームコマンドは、Cisco IOS-XEソフトウェアのパケットパスを決定する内部転送ロジックを表すSD-WANソフトウェアのオブジェクトの出力チェーンを示します。

```
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)
```

対象のプレフィクスは、さらに確認できるID 0xf800045fのサービスレベル契約(SLA)クラスタイプ(OBJ_SDWAN_NH_SLA_CLASS)のネクストホップオブジェクトを示します。

```
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
```

これは長い出力であるため、2 ~ 15のSLAクラスはスキップされました。フォールバックSLAクラスが設定されておらず、すべてのSLA 1と同じ特別なDROP隣接関係を指しています。主な目的は、SLA 0からの間接タイプ(SDWAN_NH_INDIRECT)のは同じ(0xf800044f)。 最終的な宛先VPNとサービスラベルを見つけることがさらに確認できます。

```
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.パケットトレースツールを使用して宛先VPNを検索する

宛先VPNを検出するもう1つの方法は、ルータを実際に実行するパケットをリアルタイムで分析できるパケットトレースツールです。デバッグ条件は、IPアドレス192.168.12.12との間でのみトラフィックを照合するように設定されます。

```
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
```

次に、トラフィックがR30からpingを使用して開始された場合、cE1で一致するパケットを確認し、各パケットの詳細を確認できます。この例では、これは最初のパケット番号0です。最も重要な行は、**<<<<<記号で強調表示さ**れます。

```
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 :
```

packet-traceは、pingによって送信された5つのICMPエコーパケットすべてがドロップコード52(FirewallL4Insp)でドロップされたことを示します。 セクション機能：SDWAN Forwardingは、宛先VPNが20であることを示し、トンネル化されたパケットの内部ヘッダーのサービスラベル1007を使用して、cE2上の宛先VPNを指定します。セクション機能：ZBFWは、ゾーンペアがVPN 30ゾーンを宛先とする入力VPN 20からのトラフィックに対して設定されていないため、パケットがドロップされたことを確認します。

フェールオーバーによる潜在的な問題

ルート192.168.12.0/24がR20によって取り消されるか、VRF 20のcE2から到達不能になった場合はどうなりますか。VRF 30の観点からはサブネットは同じですが、ZBFWセキュリティポリシーはゾーンVPN 30からゾーンVPN 20および10へのトラフィックを異なる方法で扱うため、トラフィックが許可されるなどの望ましくない結果を招く可能性があります。

たとえば、cE2ルータとR20ルータ間のリンク障害をシミュレートする場合です。これにより、vSmartコントローラ上のVPN 20ルーティングテーブルから192.168.12.0/24ルートが引き出され、代わりにVPN 10ルートがVPN 30ルーティングテーブルにリークされます。VPN 30からVPN 10への接続は、cE1に適用されるセキュリティポリシーに従って許可されます（これはセキュリティポリシーの観点から予想されますが、両方のVPNで提示される特定のサブネットでは望ましくありません）。

```
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 :
```

ラベル1006が1007の代わりに使用され、出力VPN IDが20ではなく10であることに注意してください。また、パケットはZBFWセキュリティポリシーに従って許可され、対応するゾーンペア、クラスマップ、およびポリシー名が与えられました。

最も古いルートがVPN 30のルーティングテーブルに保持され、この場合は、初期制御ポリシーアプリケーションVPN 20ルートがvSmart上のVPN 30 OMPテーブルにリークされた後のVPN 10ルートが原因で発生するする可能性があります。この記事で説明したZBFWセキュリティポリシーロジックと正反対の考え方を想像してみてください。たとえば、VPN 30からVPN 20へのトラフィックを許可し、VPN 10へのトラフィックを許可することが目的でした。初期ポリシー設定後、障害の後、またはVPN 20からの192.168.12.0/24ルートの取り消しが許可された場合、192.168.12.0/242.168.12.0/24サブネットへの0.