

# vManageポリシーを使用してcEdge上のトラフィックをブロック/照合するためのACLの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、ローカライズされたポリシーとアクセスコントロールリスト(ACL)を使用して、cEdgeでブロック/照合するプロセス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 Software-Defined Wide Area Network(SD-WAN)
- Cisco vManage
- cEdgeコマンドラインインターフェイス(CLI)

### 使用するコンポーネント

このドキュメントは、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。

- c8000vバージョン17.3.3
- vManageバージョン20.6.3

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

トラフィックをブロック、許可、または照合するためにローカル方式を必要とするさまざまなシナリオがあります。各方法は、ルータへのアクセスを制御するか、パケットがデバイスに到着して処理されることを保証します。

cEdgeルータでは、CLIまたはvManageのいずれかを使用してローカライズされたポリシーを設定し、トラフィック条件に一致させ、アクションを定義できます。

ローカライズされたポリシー特性の例を次に示します。

## 一致条件 :

- DiffServコードポイント(DSCP)
- パケット長
- プロトコル
- ソースデータプレフィックス
- 送信元ポート
- 宛先データプレフィックス
- 宛先ポート

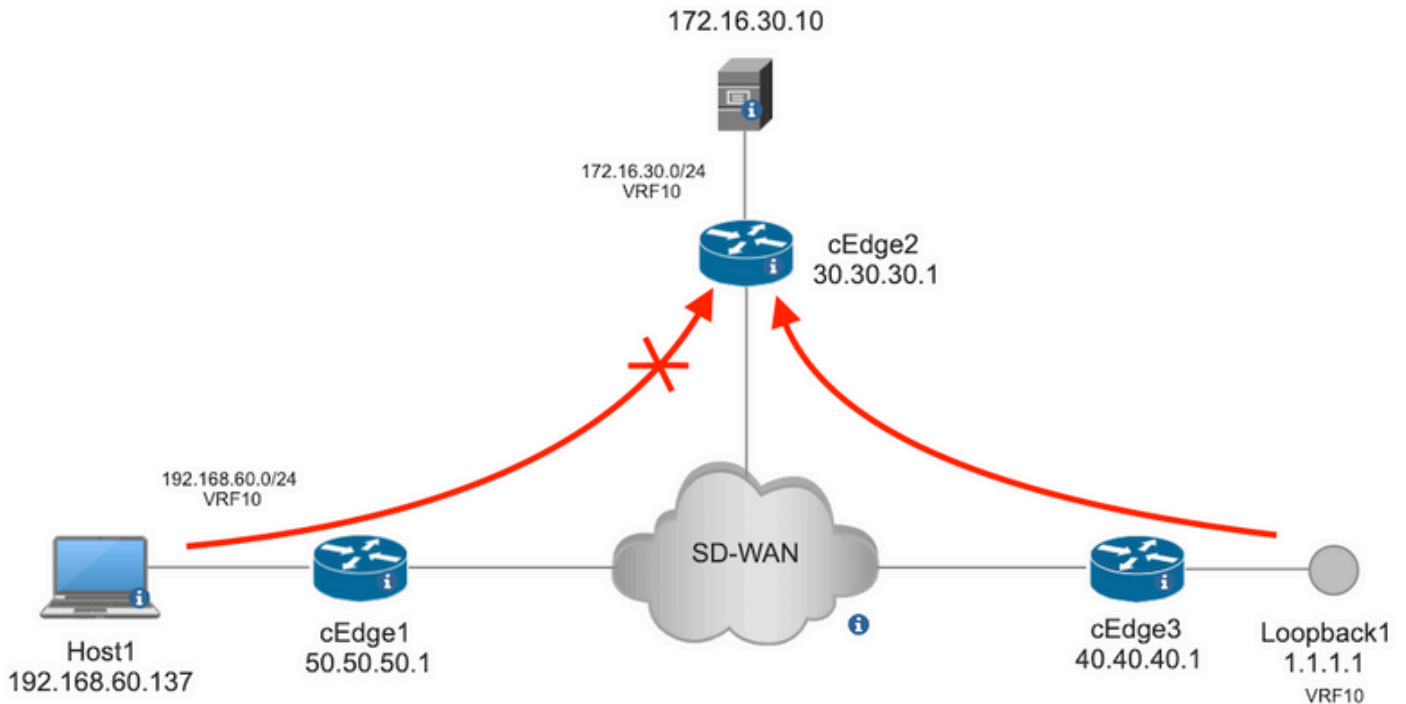
## Actions :

- Accept 追加 : カウンタ、DSCP、ログ、ネクストホップ、ミラーリスト、クラス、ポリサー
- [Drop] 追加 : カウンタ、ログ

# 設定

## ネットワーク図

この例では、cEdge2のネットワーク192.168.20.0/24からのトラフィックを出カベースでブロックし、cEdge3ループバックインターフェイスからのICMPを許可します。



ホスト1からcEdge2のサーバにping検証を実行します。

```
[Host2 ~]$ ping -I eth1 -c 5 172.16.30.10
PING 172.16.30.10 (172.16.30.10) from 192.168.60.137 eth1: 56(84) bytes of data.
64 bytes from 172.16.30.10: icmp_seq=1 ttl=253 time=20.6 ms
64 bytes from 172.16.30.10: icmp_seq=2 ttl=253 time=20.5 ms
64 bytes from 172.16.30.10: icmp_seq=3 ttl=253 time=20.5 ms
64 bytes from 172.16.30.10: icmp_seq=4 ttl=253 time=20.5 ms
64 bytes from 172.16.30.10: icmp_seq=5 ttl=253 time=20.5 ms
```

```
--- 172.16.30.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 20.527/20.582/20.669/0.137 ms
```

cEdge3からcEdge2のサーバへのping検証。

```
cEdge3# ping vrf 10 172.16.30.10 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.10, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/73/76 ms
```

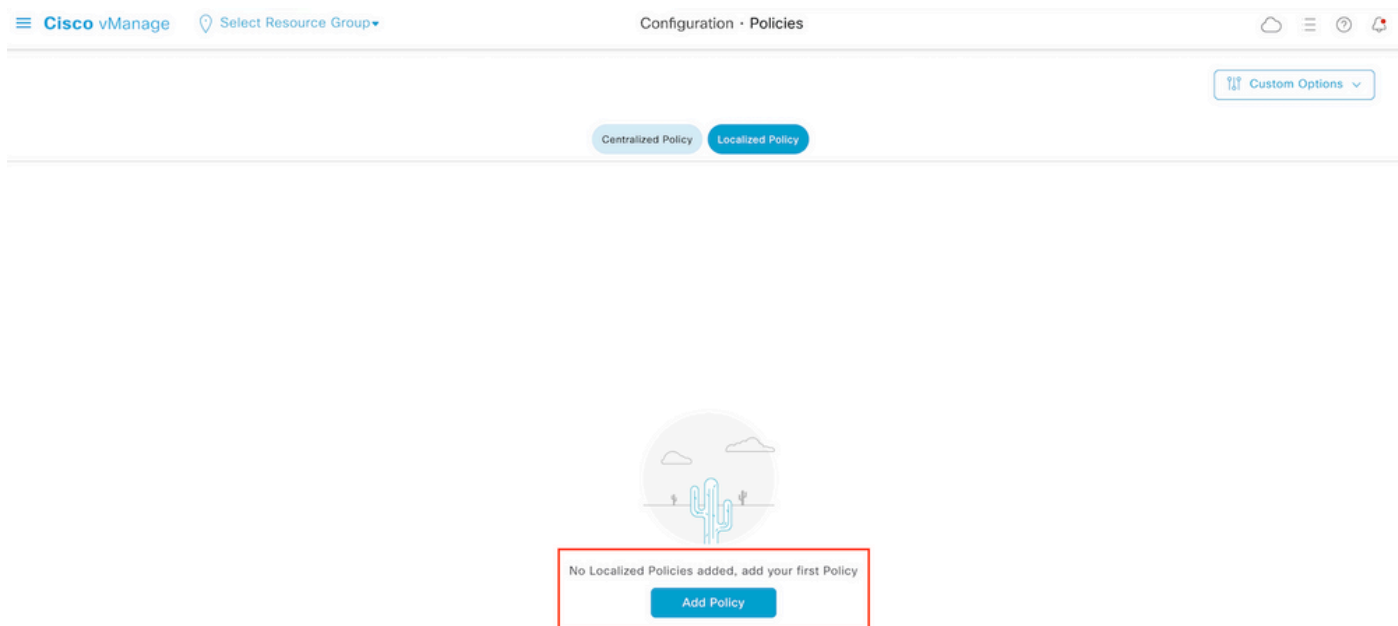
前提条件：

- cEdge2にはデバイステンプレートが添付されている必要があります。
- すべてのcEdgeでコントロール接続がアクティブになっている必要があります。
- すべてのcEdgeで、双方向フォワーディング検出(BFD)セッションがアクティブになっている必要があります。
- サービスVPN10側のネットワークに到達するには、すべてのエッジにOverlay Management Protocol(OMP)ルートが必要です。

## 設定

ステップ1:ローカライズされたポリシーを追加する。

## Cisco vManageで、 Configuration > Policies > Localized Policy. クリック Add Policy

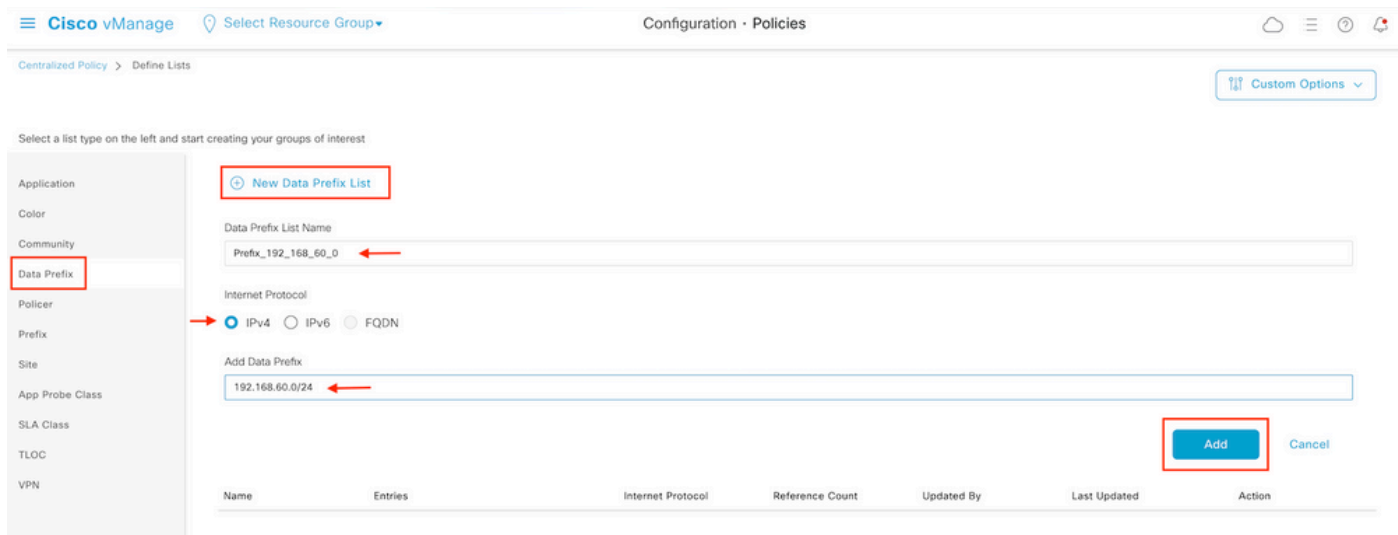


ステップ2：目的の一致に対する対象グループを作成します。

クリック Data Prefix 左側のメニューで、 New Data Prefix List.

一致条件に名前を付け、インターネットプロトコルを定義し、データプレフィックスを追加します。

クリック Add それから Next まで Configure Access Control List が表示されます。



ステップ3：一致条件を適用するアクセスリストを作成します。

選択 Add IPv4 ACL Policy Add Access Control List Policy ドロップダウンメニュー

Localized Policy &gt; Add Policy

✔ Create Groups of Interest    ✔ Configure Forwarding Classes/QoS    ● Configure Access Control Lists

Search

Add Access Control List Policy

Add Device Access Policy

(Add an Access List and configure Match and Actions)

Add IPv4 ACL Policy

Add IPv6 ACL Policy

Import Existing

Description

Mode

Reference Count

No data available

注：このドキュメントは、アクセスコントロールリスト(ACL)ポリシーに基づいており、デバイスアクセスポリシーと混同しないでください。デバイスアクセスポリシーは、Simple Network Management Protocol (SNMP；簡易ネットワーク管理プロトコル)やSecure Socket Shell (SSH；セキュアソケットシェル)などのローカルサービスの制御計画でのみ機能しますが、アクセスコントロールリストポリシーは、さまざまなサービスや一致条件に対して柔軟です。

#### ステップ4:ACLシーケンスを定義する

ACL設定画面で、ACLに名前を付け、説明を入力します。クリック **Add ACL Sequence** それから **Sequence Rule**.

[match conditions]メニューで、 **Source Data Prefix** データプレフィックスリストを **Source Data Prefix List** ドロップダウン メニューから選択します。

Access Control List

Match    Actions

DSCP    Packet Length    PLP    Protocol    **Source Data Prefix**    Source Port    Destination Data Prefix    Destination Port    TCP    Class

Source Data Prefix List

Prefix\_192\_168\_60\_0

Source: IP Prefix    Example: 10.0.0.0/12

Variables: Disabled

Actions

Accept    Enabled

#### ステップ5:シーケンスのアクションを定義し、名前を付けます

移動先 **Action** 選択 **Drop**, をクリックし、 **Save Match** と **Actions**.

Add IPv4 ACL Policy

Name: ICMP\_Block  
Description: ICMP block from cEdge 1

Access Control List

Sequence Rule Drag and drop to re-arrange rules

Match Actions

Accept Drop Counter Log

Match Conditions

Source Data Prefix List: Prefix\_192\_168\_60\_0

Source: IP Prefix Example: 10.0.0.0/12

Variables: Disabled

Actions

Drop Enabled

Counter Name: ICMP\_block\_counter

Cancel Save Match And Actions

注：このアクションは、完全にローカライズされたポリシーではなく、シーケンス自体に排他的に関連付けられます。

Access Control List

Sequence Rule Drag and drop to re-arrange rules

Match Conditions

Source Data Prefix List: Prefix\_192\_168\_60\_0

Source: IP

Actions

Drop Enabled

Counter: ICMP\_block\_counter

ステップ6:左側のメニューで、Default Action ,クリック Edit, を選択し、Accept.

Cisco vManage Select Resource Group Configuration · Policies

Add IPv4 ACL Policy

Name: ICMP\_Block  
Description: ICMP block from cEdge 1

Default Action

Accept Enabled

注：このデフォルトのアクションは、ローカライズされたポリシーの最後にあります。dropを使用しないでください。使用すると、すべてのトラフィックが影響を受け、ネットワークが停止する可能性があります。

クリック Save Access Control List Policy.

Add Access Control List Policy Add Device Access Policy (Add an Access List and configure Match and Actions)

Total Rows: 1

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
ICMP_Block	Access Control List (IPv4)	ICMP block from cEdge 1	created	0	ericgar	21 Aug 2022 5:55:54 PM CDT

ステップ7:ポリシーに名前を付ける

クリック Next まで Policy Overview 名前を付けます他の値は空白のままにします。クリック Save Policy

Enter name and description for your localized master policy

Policy Name	Policy_ICMP
Policy Description	Policy_ICMP

## Policy Settings

 Netflow  Netflow IPv6  Application  Application IPv6  Cloud QoS  Cloud QoS Service side  Implicit ACL LoggingLog Frequency  ⓘFNF IPv4 Max Cache Entries  ⓘFNF IPv6 Max Cache Entries  ⓘ[Back](#)[Preview](#)[Save Policy](#)[Cancel](#)

ポリシーが正しいことを確認するには、 **Preview**.

Name	Description	Devices Attached	Device Templates	Updated By	Last Updated	
Policy_ICMP	Policy_ICMP	0	0	ericgar	21 Aug 2022 6:05:06 PM CDT	...

[View](#)  
[Preview](#)  
[Copy](#)  
[Edit](#)  
[Delete](#)

ポリシーでシーケンスと要素が正しいことを確認します。

# Policy Configuration Preview

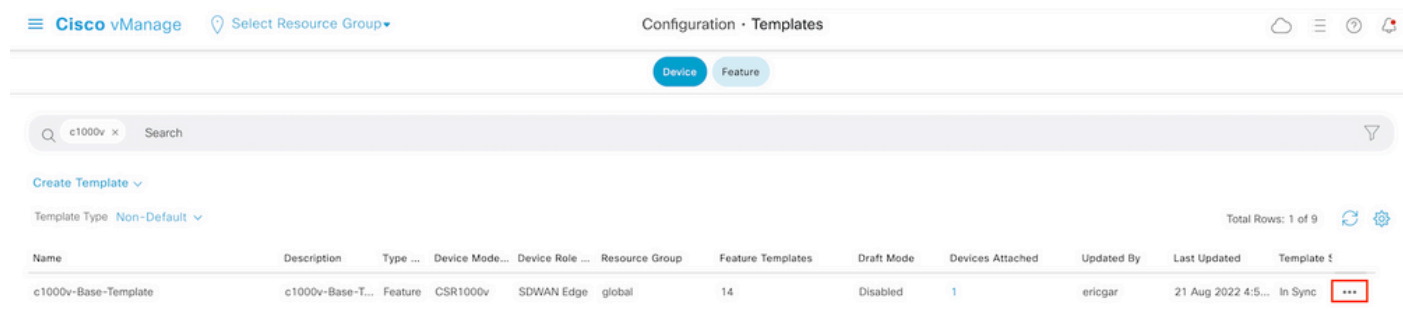
```
policy
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 ←
!
action drop ←
count ICMP_block_counter ←
!
!
default-action accept ←
!
lists
data-prefix-list Prefix_192_168_60_0
ip-prefix 192.168.60.0/24 ←
!
!
!
```

OK

ACL名をコピーします。これは、次のステップで必要になります。

ステップ8:ローカライズされたポリシーをデバイステンプレートに関連付けます。

ルータに接続されているデバイステンプレートを見つけて、3つのドットをクリックし、**Edit**.



選択 **Additional Templates** ローカライズされたポリシーを[policy]フィールドに追加し、 **Update > Next > Configure Devices** 設定をcEdgeにプッシュします。



# Additional Templates

AppQoE

Choose...

Global Template \*

Factory\_Default\_Global\_CISCO\_Templ...



Cisco Banner

Choose...

Cisco SNMP

Choose...

TrustSec

Choose...

CLI Add-On Template

Choose...

Policy

Policy\_ICMP

Probes

Choose...

Security Policy

Choose...

Push Feature Template Configuration ● Validation Success

Initiated By: ericgar From: 72.163.2.247

Total Task: 1 | Success : 1

Search

Total Rows: 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Success	Done - Push Feature Templat...	CSR-E4716CEE-A536-A79C...	CSR1000v	cEdge2	30.30.30.1	30	1.1.1.5

```
[21-Aug-2022 23:31:47 UTC] Configuring device with feature template: c1000v-Base-Template
[21-Aug-2022 23:31:47 UTC] Checking and creating device in vManage
[21-Aug-2022 23:31:48 UTC] Generating configuration from template
[21-Aug-2022 23:31:49 UTC] Device is online
[21-Aug-2022 23:31:49 UTC] Updating device configuration in vManage
[21-Aug-2022 23:31:50 UTC] Sending configuration to device
[21-Aug-2022 23:31:50 UTC] Completed template push to device.
```

注：この時点で、vManageは作成されたポリシーに基づいてACLを構築し、どのインターフェイスにも関連付けられていませんが、変更をcEdgeにプッシュします。したがって、トラフィックフローには影響しません。

ステップ9: デバイステンプレート内のトラフィックにアクションを適用するインターフェイスの機能テンプレートを特定します。

トラフィックをブロックする必要がある機能テンプレートを見つけることが重要です。

この例では、GigabitEthernet3インターフェイスはVirtual Private Network 3(Virtual Forwarding Network 3)に属しています。

[service VPN]セクションに移動し、Edit VPNテンプレートにアクセスします。

この例では、GigabitEthernet3インターフェイスにc1000v-Base-VP10-IntGi3機能テンプレートが接続されています。

Edit VPN - c1000v-Base-VP10

Cisco VPN Interface Ethernet: c1000v-Base-VP10-Lo1

Cisco VPN Interface Ethernet: c1000v-Base-VP10-IntGi3

Additional Cisco VPN Templates

- Cisco IGMP
- Cisco Multicast
- Cisco PIM
- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco VPN Interface Ethernet
- Cisco VPN Interface IPsec
- EIGRP

ステップ10:ACL名をインターフェイスに関連付けます。

移動先 Configuration > Templates > Feature. テンプレートをフィルタリングし、Edit

Cisco vManage Configuration · Templates

Device Feature

1000v × Search

Add Template

Template Type Non-Default

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
c1000v-Base-VP0-IntGi1	c1000v-Base-VP0-IntGi1	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	29 Jul 2022 12:26:31 A. ...
c1000v-Base-VP0-IntGi2	c1000v-Base-VP0-IntGi2	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	19 Aug 2022 5:40:54 P. ...
c1000v-Base-VP10-IntGi3	c1000v-Base-VP0-IntGi3	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	21 Aug 2022 4:51:08 P. ...
c1000v-Base-VP10	c1000v-Base-VP10	Cisco VPN	CSR1000v	1	global	1	ericgar	26 Jul 2022 12:34:41 P. ...
c1000v-Base-VP10-Lo1	c1000v-Base-VP10-Lo1	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	26 Jul 2022 12:06:35 A. ...
c1000v-Base-VPN0	c1000v-Base-VPN0	Cisco VPN	CSR1000v	1	global	1	ericgar	26 Jul 2022 12:48:52 A. ...

クリック ACL/QoS トラフィックがブロックする方向を有効にします。手順7でコピーしたACL名を書き込みます。Update 変更をプッシュします

Device

Feature

Feature Template &gt; Cisco VPN Interface Ethernet &gt; c1000v-Base-VP10-IntGi3

Basic Configuration

Tunnel

NAT

VRRP

ACL/QoS

ARP

TrustSec

Advanced

## ACL/QoS

Adaptive QoS	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Shaping Rate (Kbps)	<input checked="" type="checkbox"/> [ ]
QoS Map	<input checked="" type="checkbox"/> [ ]
VPN QoS Map	<input checked="" type="checkbox"/> [ ]
Rewrite Rule	<input checked="" type="checkbox"/> [ ]
Ingress ACL - IPv4	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Egress ACL - IPv4	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
IPv4 Egress Access List	<input checked="" type="checkbox"/> ICMP_Block
Ingress ACL - IPv6	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Egress ACL - IPv6	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off

Cancel

Update

注:vManageポリシー構造は両方のアーキテクチャで同じであるため、このローカライズされたポリシー作成プロセスはvEdgeでも機能します。異なる部分は、cEdgeまたはvEdgeと互換性のあるコンフィギュレーション構造を構築するデバイステンプレートによって提供されます。

## 確認

### ステップ1: ルータの設定を正しく確認する

```
cEdge2# show sdwan running-config policy
policy
lists
  data-prefix-list Prefix_192_168_60_0 <<<<<<<<<
```

```

ip-prefix 192.168.60.0/24 <<<<<<<<<
!
!
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 <<<<<<<<<
!
action drop <<<<<<<<<
count ICMP_block_counter <<<<<<<<<
!
!
default-action accept <<<<<<<<<
!
!

```

```

cEdge2# show sdwan running-config sdwan | section interface GigabitEthernet3
interface GigabitEthernet3
access-list ICMP_Block out

```

**ステップ2:**cEdge1のサービスネットワーク内にあるHost1から、cEdge2のサーバに5つのpingメッセージを送信します

```

[Host1 ~]$ ping -I eth1 -c 5 172.16.30.10
PING 172.16.30.10 (172.16.30.10) from 192.168.60.137 eth1: 56(84) bytes of data.
--- 172.16.30.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4088ms

```

**注:** この例では、host1はLinuxマシンです。「-I」はpingがルータから発信されるインターフェイスを表し、「-c」はpingメッセージの数を表します。

**ステップ3:**cEdge2から、ACLカウンタを確認します

```

cEdge2# show sdwan policy access-list-counters
NAME COUNTER NAME PACKETS BYTES
-----
ICMP_Block ICMP_block_counter 5      610
default_action_count 0 0

```

このカウンタは、ポリシーで定義されているように、ネットワーク192.168.60.0/24から送信された5つのパケットに一致しました。

**手順4:**cEdge3から、4つのpingメッセージをサーバ172.16.30.10に送信します

```

cEdge3# ping vrf 10 172.16.30.10 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.10, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/76/88 ms

```

ネットワークが異なり(この場合は1.1.1.1/32)、ポリシー内に一致する条件がないため、ルータを通過したパケットはサーバに渡されません。

**手順5:**cEdge2のACLカウンタを再度確認します。

```

cEdge2# show sdwan policy access-list-counters

```

```
NAME COUNTER NAME PACKETS BYTES
```

```
-----  
ICMP_Block ICMP_block_counter 5      610  
default_action_count 5      690
```

default\_action\_countのカウンタは、cEdge3によって送信された5個のパケットで増加しました。

カウンタをクリアするには、`clear sdwan policy access-list` コマンドが表示されない場合もあります。

vEdgeで確認するためのコマンド

```
show running-config policy  
show running-config  
show policy access-list-counters  
clear policy access-list
```

## トラブルシューティング

エラー:インターフェイス内のACL名への不正な参照

ACLを含むポリシーは、最初にデバイステンプレートに関連付ける必要があります。その後、ACL名をインターフェイスの機能デバイステンプレートで指定できます。

Push Feature Template Configuration | Validation Success Initiated By: ericgar From: 72.163.2.247

Total Task: 1 | Failure: 1

Search ▼

Total Rows: 1 ↺ ⚙️

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Failure	Failed to update configuration...	CSR-E4716CEE-A536-A79C...	CSR1000v	cEdge2	30.30.30.1	30	1.1.1.5

```
51:32 UTC] Configuring device with feature template: c1000v-Base-Template  
51:32 UTC] Checking and creating device in vManage  
51:33 UTC] Generating configuration from template  
51:33 UTC] Failed to update configuration - illegal reference /vmanage-cfs:templates/template(vedge-CSR-E4716CEE-A536-A79C-BD61-ASFFEDC7B1FB)/vpn/vpn-instance(10)/interface(gigabitEthernet3)/access-list(out)/acl-name
```

## 関連情報

- [Cisco SD-WANポリシー設定ガイド、Cisco IOS XEリリース17.x](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。