

# ACL configureren om verkeer op randen te blokkeren/matchen met vManager-beleid

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrond](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft het proces om in een cEdge te blokkeren/matchen met een gelokaliseerd beleid en een toegangscontrolelijst (ACL).

## Voorwaarden

### Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)
- Cisco vManager
- cEdge Command Line Interface (CLI)

### Gebruikte componenten

Dit document is gebaseerd op deze software- en hardwareversies:

- c800v versie 17.3.3
- vManager versie 20.6.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrond

Er zijn verschillende scenario's die een lokale methode vereisen om verkeer te blokkeren, toe te laten of aan te passen. Elke methode controleert toegang tot de router of zorgt ervoor dat de pakketten aan het apparaat aankomen en verwerkt worden.

cEdge-routers bieden de mogelijkheid om een gelokaliseerd beleid via CLI of vManager te configureren om aan de verkeersomstandigheden te voldoen en een actie te definiëren.

Dit zijn enkele voorbeelden van plaatselijke beleidskenmerken:

## Overeenkomstige voorwaarden:

- Gedifferentieerde services codepunt (DSCP)
- PacketLengte
- Protocol
- Prefix van brongegevens
- Bronpoort
- Prefix van doelgegevens
- Doelpoort

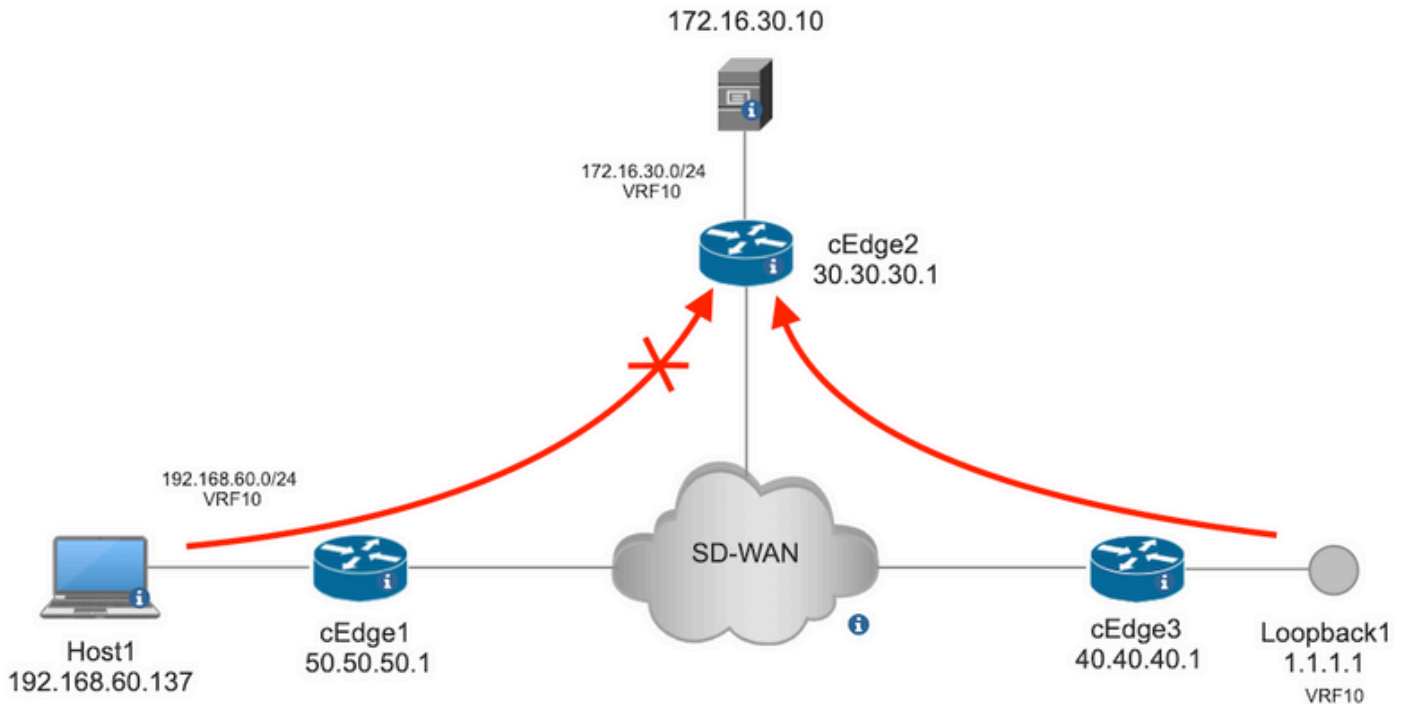
## Acties:

- accepteren Extra: teller, DSCP, logboeken, nexthop, spiegellijst, klasse, policer
- Afwijzing Extra: teller, logboek

# Configureren

## Netwerkdigram

Bij dit voorbeeld is het de bedoeling om verkeer van netwerk 192.168.20.0/24 in cEdge2 op uitgaande basis te blokkeren en ICMP toe te staan vanuit cEdge3 loopback-interface.



Ping-verificatie van host1 naar server in cEdge2.

```
[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
```

Pingel verificatie van cEdge3 naar server in cEdge2.

```
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
```

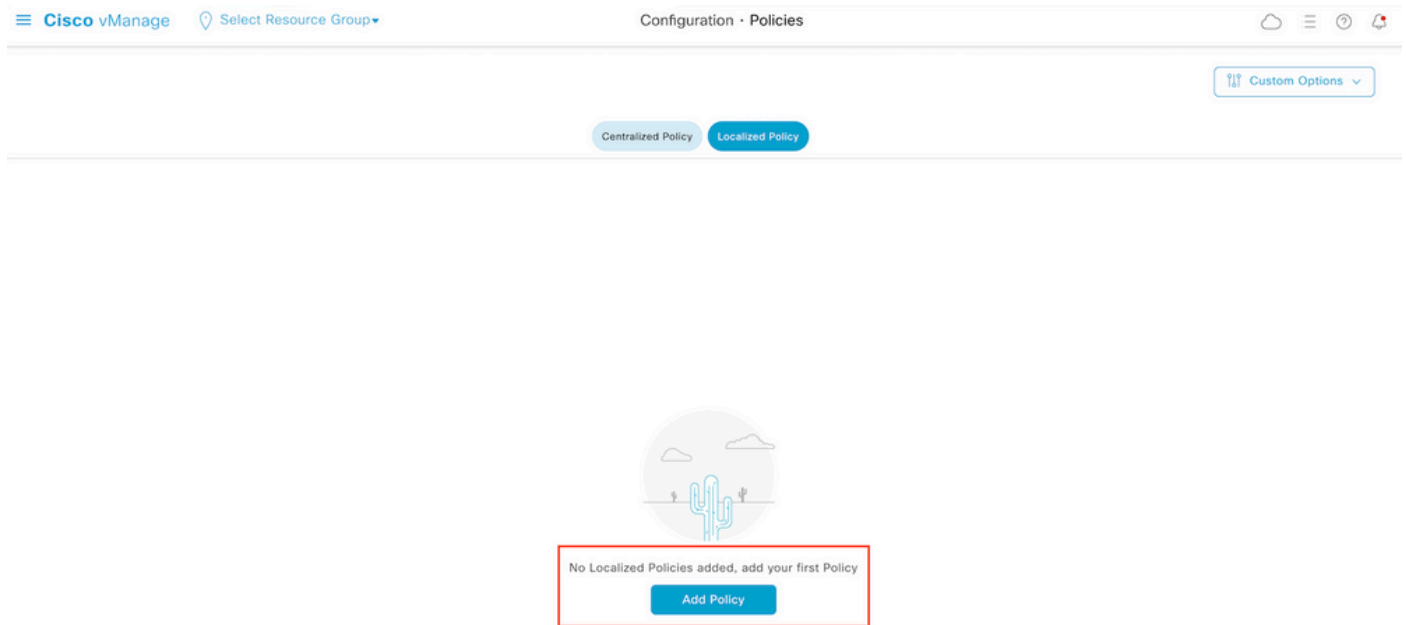
**Voorwaarden:**

- cEdge2 moet een apparaatsjabloon hebben aangesloten.
- Alle cEdges moeten besturingverbindingen actief hebben.
- Alle cEdges moeten Bidirectionele Forwarding Detection (BFD)-sessies actief hebben.
- Alle interfaces moeten over Overlay Management Protocol (OMP)-routes beschikken om de VPN10-zijnetwerken te bereiken.

## Configuraties

**Stap 1.** Voeg het lokale beleid toe.

Navigeer in Cisco vManager naar **Configuration > Policies > Localized Policy**. Klik **Add Policy**

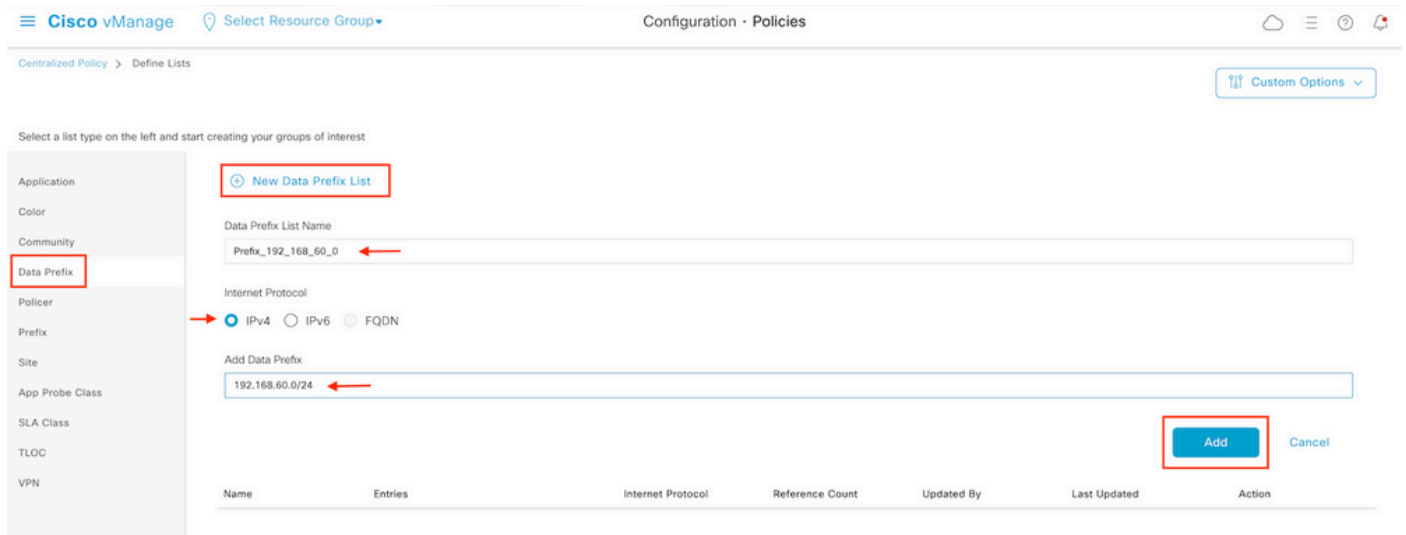


**Stap 2.** Maak belangengroepen voor de beoogde match.

Klik **Data Prefix** in het linkermenu en selecteer **New Data Prefix List**.

Geef een naam aan de overeenkomende voorwaarde, definieer het Internet-protocol en voeg een gegevensprefix toe.

Klik **Add** en vervolgens **Next** tot **Configure Access Control List** wordt weergegeven.



**Stap 3.** Maak de toegangslijst om de matchvoorwaarde toe te passen.

Kiezen **Add IPv4 ACL Policy** van de **Add Access Control List Policy** vervolgkeuzemenu.

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

**Opmerking:** Dit document is gebaseerd op het beleid van de toegangscontrolelijst en moet niet met een beleid van de apparatentoegang worden verward. Het beleid voor apparaattoegang werkt alleen in het controleplan voor lokale services zoals Simple Network Management Protocol (SNMP) en Secure Socket Shell (SSH), terwijl het beleid voor de toegangscontrolelijst flexibel is voor verschillende services en overeenkomende voorwaarden.

#### Stap 4. Definieer de ACL-reeks

Geef in het configuratiescherm van de ACL de naam van de ACL en geef een beschrijving op. Klik **Add ACL Sequence** en vervolgens **Sequence Rule**.

Selecteer in het menu Overeenkomstige voorwaarden de optie **Source Data Prefix** en kies vervolgens de prefixlijst met gegevens uit de **Source Data Prefix List** vervolgkeuzelijst.

The screenshot shows the configuration page for an IPv4 ACL Policy. The 'Name' field is filled with 'ICMP\_Block' and the 'Description' is 'ICMP block from cEdge 1'. On the left, there are buttons for 'Add ACL Sequence' and 'Sequence Rule'. The main area is divided into 'Match' and 'Actions' tabs. Under the 'Match' tab, several match conditions are listed: DSCP, Packet Length, PLP, Protocol, Source Data Prefix (highlighted), Source Port, Destination Data Prefix, Destination Port, TCP, and Class. The 'Source Data Prefix' condition is expanded to show a dropdown menu with 'Source Data Prefix List' and a selected item 'Prefix\_192\_168\_60\_0'. Below this, there is a 'Source' field set to 'IP Prefix' with an example '10.0.0.0/12' and a 'Variables: Disabled' checkbox. The 'Actions' tab shows 'Accept' and 'Enabled'.

#### Stap 5. Bepaal de actie voor de opeenvolging en noem het

Navigeer naar **Action selecteren Drop**, en klik op **Save Match** en **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

**Opmerking:** Deze actie is uitsluitend gekoppeld aan de sequentie zelf, niet aan het volledige lokale beleid.

**Access Control List**

Sequence Rule: Drag and drop to re-arrange rules

1 Match Conditions

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

Source: IP

Actions

Drop Enabled

Counter ICMP\_block\_counter

**Stap 6.** Selecteer in het linkermenu **Default Action**, klikken **Edit**, en kiezen **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

**Opmerking:** Deze standaardactie is aan het eind van het gelocaliseerde beleid. Gebruik de **drop** niet, anders kan al het verkeer worden beïnvloed en een netwerkstroomonderbreking veroorzaken.

Klik **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

**Stap 7.** Geef het beleid een naam

Klik **Next** tot **Policy Overview** en noem het. Laat de andere waarden leeg. Klik **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](#)

Om er zeker van te zijn dat het beleid correct is, klikt u op **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](#)

Controleer of de volgorde en elementen in het beleid juist zijn.

# Policy Configuration Preview

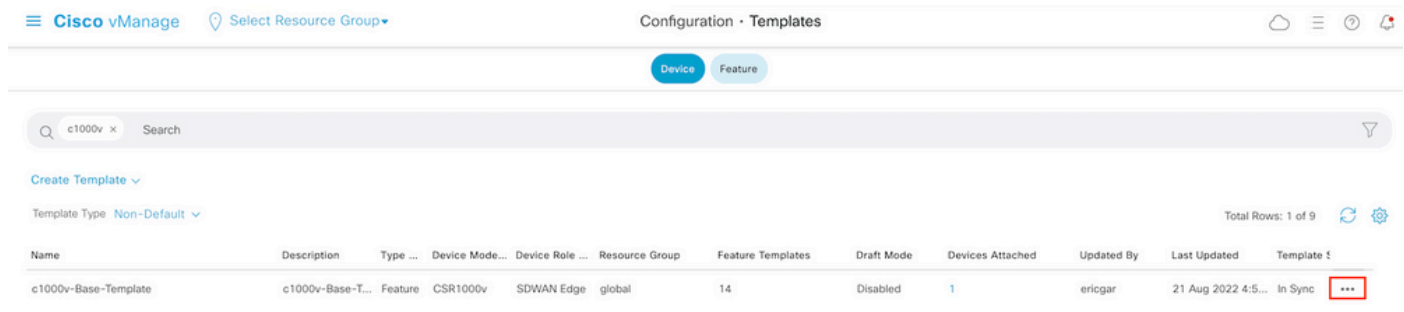
```
policy
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 ←
!
action drop ←
count ICMP_block_counter ←
!
!
default-action accept ←
!
lists
data-prefix-list Prefix_192_168_60_0
ip-prefix 192.168.60.0/24 ←
!
!
!
```

OK

Kopieert de ACL-naam. Dit is een verdere stap.

**Stap 8.** Associeer het gelokaliseerde beleid met het apparatenmalplaatje.

Bepaal de plaats van het apparatenmalplaatje in bijlage aan de router, klik de drie punten, en klik **Edit**.



Kiezen **Additional Templates** en voeg het gelokaliseerde beleid toe aan het beleidsveld en klik op **Update > Next > Configure Devices** om de configuratie naar de cEdge te duwen.



# 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.
```

**Opmerking:** Op dit punt bouwt vManager de ACL op basis van het gemaakte beleid en drukt de wijzigingen in de cEdge, hoewel deze niet aan enige interface is gekoppeld. Daarom heeft het geen effect op de verkeersstroom.

**Stap 9.** Identificeer het eigenschapsplaatje van de interface waar het bedoeld is om de actie op het verkeer in het apparatenplaatje toe te passen.


Het is belangrijk om van het eigenschapsmaalplaatje de plaats te bepalen waar het verkeer moet worden geblokkeerd.


In dit voorbeeld behoort de Gigabit Ethernet3-interface tot Virtual Private Network 3 (Virtual Forwarding Network 3).

Navigeer naar VPN-sectie voor service en klik op **Edit** om toegang te krijgen tot de VPN-sjablonen.

In dit voorbeeld is de Gigabit Ethernet3-interface voorzien van c1000v-Base-VP10-IntGi3 functiesjabloon in bijlage.

Edit VPN - c1000v-Base-VP10

Cisco VPN Interface Ethernet   [+ Sub-Templates](#) ▾





Cisco VPN Interface Ethernet   [+ Sub-Templates](#) ▾

**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



**Stap 10.** Associeer de ACL-naam met de interface.

Navigeer naar **Configuration > Templates > Feature**. Filter de sjablonen en klik **Edit**

Cisco vManage [Select Resource Group](#) Configuration · Templates    

[Device](#) [Feature](#)

[Add Template](#)

Template Type [Non-Default](#) ▾ Total Rows: 7 of 32  

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-VP10-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. ...

Klik **ACL/00s** en de richting van het verkeer instellen om te blokkeren. Schrijf de ACL-naam die in stap 7 is gekopieerd. Klik op **Update** en druk op de veranderingen.

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"/> <input type="text"/>
QoS Map	<input checked="" type="checkbox"/> <input type="text"/>
VPN QoS Map	<input checked="" type="checkbox"/> <input type="text"/>
Rewrite Rule	<input checked="" type="checkbox"/> <input type="text"/>
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

**Opmerking:** dit proces voor het maken van gelokaliseerd beleid werkt ook voor vEdge-servers omdat de beleidsstructuur van vManager voor beide architecturen hetzelfde is. Het verschillende deel wordt gegeven door het apparaatsjabloon dat een configuratiestructuur maakt die compatibel is met cEdge of vEdge.

## Verifiëren

**Stap 1.** Controleer de configuraties correct in de router

```
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

```

**Stap 2.** Verzend 5 ping-berichten naar de server in cEdge2 vanaf Host1 dat in een servicenetwerk van cEdge1 is

```

[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

```

**Opmerking:** In dit voorbeeld is host1 een Linux machine. "-I" staat voor de interfaces waar de ping de router verlaat en "-c" staat voor het aantal ping-berichten.

**Stap 3.** Controleer vanuit cEdge2 de ACL-tellers

```

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

```

De teller kwam overeen met vijf (5) pakketten die van netwerk 192.168.60.0/24 kwamen, zoals bepaald in het beleid.

**Stap 4.** Verzend vanuit cEdge3 4 ping-berichten naar server 172.16.30.10

```

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

```

De pakketten gingen door de router aan de server over omdat het netwerk verschillend is (in dit geval is 1.1.1.1/32) en er is geen passende voorwaarde voor het in het beleid.

**Stap 5.** Controleer de ACL-tellers in cEdge2 opnieuw.

```

cEdge2# show sdwan policy access-list-counters

```

```
NAME COUNTER NAME PACKETS BYTES
```

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

De teller van default\_action\_count nam toe met de 5 pakketten die door cEdge3 verzonden werden.

Om tellers te wissen, voert u `clear sdwan policy access-list` uit.

Opdrachten voor verificatie in vEdge

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

## Problemen oplossen

**Fout:** Ongeldige verwijzing naar de ACL-naam in de interface

Het beleid dat ACL bevat moet eerst aan het apparatenmalplaatje worden vastgemaakt. Daarna, kan de ACL naam in het malplaatje van het eigenschapapparaat van de interface worden gespecificeerd.

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
```

## Gerelateerde informatie

- [Cisco SD-WAN Policy Configuration Guide, Cisco IOS XE release 17.x](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.