

# Configurazione dell'ACL per bloccare/associare il traffico sui bordi con criteri vManage

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Sfondo](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto il processo di blocco/corrispondenza in un cEdge con un criterio localizzato e un Access Control List (ACL).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- Cisco vManage
- CLI (Command Line Interface) cEdge

### Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

- c800v versione 17.3.3
- vManage versione 20.6.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Sfondo

Esistono diversi scenari che richiedono un metodo locale per bloccare, autorizzare o associare il traffico. Ogni metodo controlla l'accesso al router o assicura che i pacchetti arrivino al dispositivo e vengano elaborati.

I router cEdge consentono di configurare un criterio localizzato tramite CLI o vManage per soddisfare le condizioni del traffico e definire un'azione.

Di seguito sono riportati alcuni esempi di caratteristiche localizzate dei criteri:

## Condizioni di corrispondenza:

- DSCP (Differentiated Services Code Point)
- Lunghezza pacchetto
- Protocollo
- Prefisso dati di origine
- Porta di origine
- Prefisso dati di destinazione
- Porta di destinazione

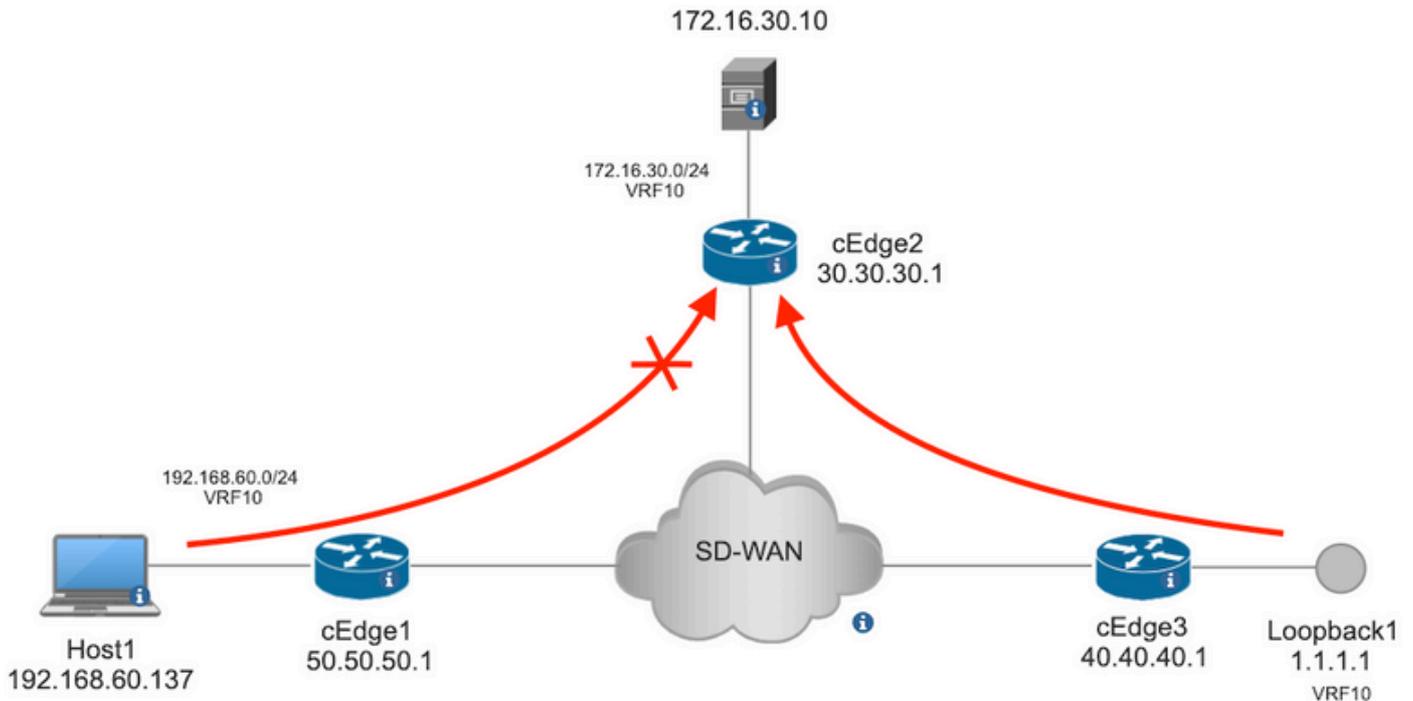
## Azioni:

- Accetta Altro: contatore, DSCP, registri, nexthop, elenco mirror, classe, policer
- Drop Altro: contatore, registro

# Configurazione

## Esempio di rete

Per questo esempio, l'intenzione è bloccare il traffico proveniente dalla rete 192.168.20.0/24 in cEdge2 in uscita e autorizzare l'ICMP dall'interfaccia di loopback cEdge3.



Eseguire il ping della verifica da Host1 a 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
```

Eseguire il ping della verifica da cEdge3 al 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
```

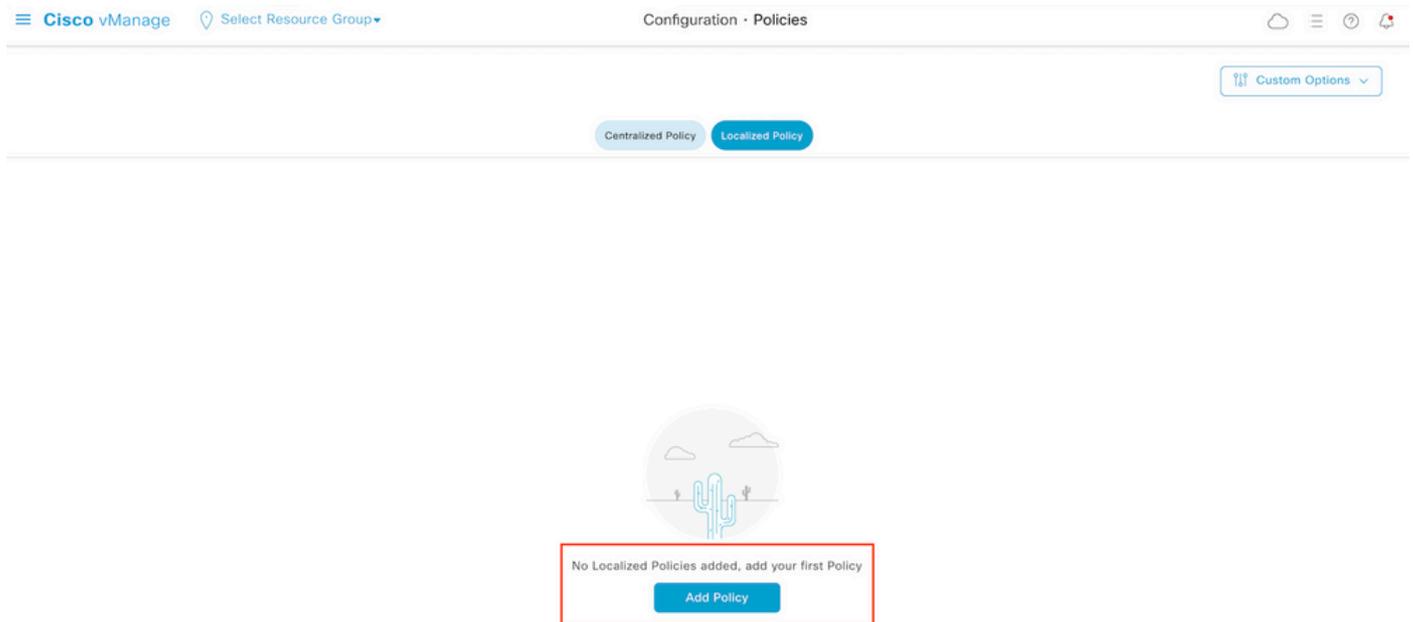
### Condizioni preliminari:

- a cEdge2 deve essere associato un modello di dispositivo.
- Tutti gli spigoli devono avere connessioni di controllo attive.
- Tutti i bordi devono avere sessioni BFD (Bidirectional Forwarding Detection) attive.
- Tutti i nodi devono avere route OMP (Overlay Management Protocol) per raggiungere le reti lato VPN10 del servizio.

## Configurazioni

**Passaggio 1.** Aggiungere il criterio localizzato.

In Cisco vManage, passare a **Configuration > Policies > Localized Policy**. Clic **Add Policy**



**Passaggio 2.** Creare i gruppi di interesse per la corrispondenza desiderata.

Clic **Data Prefix** nel menu a sinistra e selezionare **New Data Prefix List**.

Assegnare un nome alla condizione di corrispondenza, definire il protocollo Internet e aggiungere un prefisso dati.

Clic **Add** e poi **Next** fino al **Configure Access Control List** viene visualizzato.



**Passaggio 3.** Creare l'elenco degli accessi per applicare la condizione di corrispondenza.

Seleziona **Add IPv4 ACL Policy** dal **Add Access Control List Policy** menu a discesa.

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

**Nota:** Questo documento è basato sui criteri dell'elenco di controllo di accesso e non deve essere confuso con i criteri di accesso alle periferiche. I criteri di accesso ai dispositivi agiscono solo nel piano di controllo per i servizi locali, ad esempio SNMP (Simple Network Management Protocol) e SSH (Secure Socket Shell), mentre i criteri degli elenchi di controllo di accesso sono flessibili per servizi diversi e soddisfano le condizioni.

#### Passaggio 4. Definizione della sequenza ACL

Nella schermata di configurazione dell'ACL, assegnare un nome all'ACL e fornire una descrizione. Clic **Add ACL Sequence** e poi **Sequence Rule**.

Nel menu Condizioni di corrispondenza, selezionare **Source Data Prefix** e quindi scegliere l'elenco di prefissi dei dati dal **Source Data Prefix List** menu a discesa.

Add IPv4 ACL Policy

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

**Add ACL Sequence**

**Sequence Rule** Drag and drop to re-arrange rules

Match Conditions

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

Source: IP Prefix Example: 10.0.0.0/12  
Variables: Disabled

Match Actions

Accept Enabled

#### Passaggio 5. Definire l'azione per la sequenza e denominarla

Passa a **Action** selezionare **Drop**, e fare clic su **Save Match e 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

**Nota:** Questa azione è associata in modo esclusivo alla sequenza stessa, non al criterio localizzato completo.

**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

**Passaggio 6.** Nel menu a sinistra, selezionare **Default Action**, fare clic **Edit**, e scegliere **Accept**.

Cisco vManage Configuration · Policies

Add IPv4 ACL Policy

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

**Default Action**

Accept Enabled

**Nota:** Questa azione predefinita è alla fine del criterio localizzato. Non utilizzare il comando **drop**, altrimenti tutto il traffico potrebbe risentirne e causare un'interruzione della rete.

**Clic 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

**Passaggio 7.** Assegnare un nome al criterio

Clic **Next** fino al **Policy Overview** e lo chiami. Lasciare vuoti gli altri valori. Clic **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](#)

Per verificare la correttezza del criterio, fare clic su **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](#)

Verificare che la sequenza e gli elementi siano corretti nel criterio.

# Policy Configuration Preview

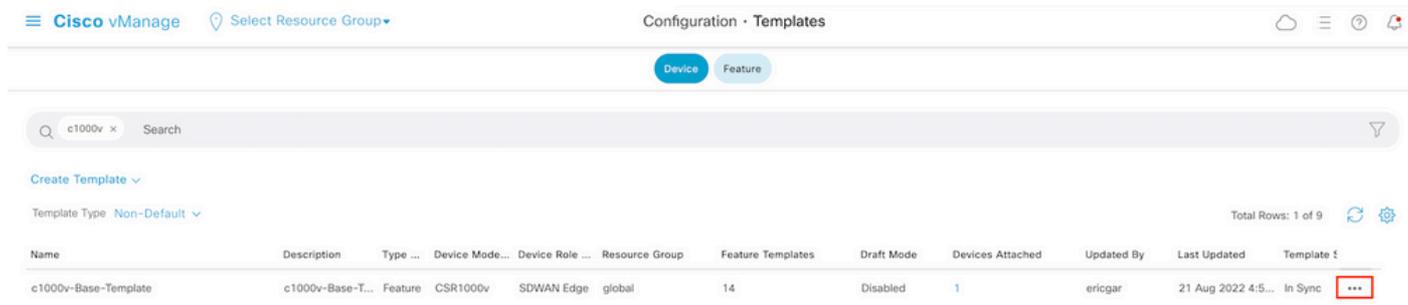
```
policy
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 ←
!
action drop ←
count ICMP_block_counter ←
!
!
default-action accept ←
!
lists
data-prefix-list Prefix_192_168_60_0
ip-prefix 192.168.60.0/24 ←
!
!
!
```

OK

Copiare il nome dell'ACL. È richiesto in una fase successiva.

## Passaggio 8. Associare il criterio localizzato al modello di dispositivo.

Individuare il modello di dispositivo collegato al router, fare clic sui tre punti, quindi fare clic su **Edit**.



Seleziona **Additional Templates** e aggiungere il criterio localizzato al campo criterio e fare clic su **Update > Next > Configure Devices** per eseguire il push della configurazione su cEdge.

## 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.
```

**Nota:** A questo punto, vManage crea l'ACL in base al criterio creato e invia le modifiche a cEdge, anche se non è associato ad alcuna interfaccia. Pertanto, non ha alcun effetto sul flusso del traffico.

**Passaggio 9.** Identificare il modello di funzionalità dell'interfaccia a cui deve essere applicata l'azione al traffico nel modello di dispositivo.

È importante individuare il modello di funzionalità in cui il traffico deve essere bloccato.

Nell'esempio, l'interfaccia Gigabit Ethernet3 appartiene a Virtual Private Network 3 (Virtual Forwarding Network 3).

Passare alla sezione Service VPN e fare clic su **Edit** per accedere ai modelli VPN.

Nell'esempio, all'interfaccia Gigabit Ethernet3 è associato un modello di funzionalità c1000v-Base-VP10-IntGi3.

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

**Passaggio 10.** Associare il nome ACL all'interfaccia.

Passa a **Configuration > Templates > Feature**. Filtrare i modelli e fare clic su **Edit**

Cisco vManage | Select Resource Group | Configuration - Templates

Device | **Feature**

1000v x Search

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-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. ...

Clic **ACL/QoS** e abilitare la direzione di blocco del traffico. Scrivere il nome ACL copiato nel passaggio 7. Fare clic su **Update** e premere i cambiamenti.

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 type="text"/>
QoS Map	<input type="text"/>
VPN QoS Map	<input type="text"/>
Rewrite Rule	<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 type="text" value="ICMP_Block"/>
Ingress ACL - IPv6	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Egress ACL - IPv6	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off

Cancel

Update

**Nota:** questo processo di creazione localizzato dei criteri funziona anche per vEdges, in quanto la struttura dei criteri di vManage è la stessa per entrambe le architetture. L'altra parte viene fornita dal modello di dispositivo che crea una struttura di configurazione compatibile con cEdge o vEdge.

## Verifica

**Passaggio 1.** Verificare la corretta configurazione nel 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

```

**Passaggio 2.** Dall'host 1 nella rete di servizio di cEdge1, inviare 5 messaggi ping al server in cEdge2

```

[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

```

**Nota:** Per questo esempio, host1 è un computer Linux. "-I" rappresenta le interfacce su cui il ping esce dal router e "-c" rappresenta il numero di messaggi ping.

**Passaggio 3.** Da cEdge2, verificare i contatori ACL

```

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

```

Il contatore corrisponde a cinque (5) pacchetti provenienti dalla rete 192.168.60.0/24, come definito nel criterio.

**Passaggio 4.** Da cEdge3, inviare 4 messaggi ping al 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

```

I pacchetti passati attraverso il router al server perché la rete è diversa (in questo caso è 1.1.1.1/32) e non esiste alcuna condizione corrispondente nel criterio.

**Passaggio 5.** Verificare di nuovo i contatori ACL in cEdge2.

```

cEdge2# show sdwan policy access-list-counters

```

```
NAME COUNTER NAME PACKETS BYTES
```

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

Il contatore di default\_action\_count è stato incrementato con i 5 pacchetti inviati da cEdge3.

Per cancellare i contatori, eseguire `clear sdwan policy access-list`

Comandi per la verifica in vEdge

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

## Risoluzione dei problemi

**Errore:** Riferimento non valido al nome ACL nell'interfaccia

Il criterio che contiene l'ACL deve essere prima associato al modello di dispositivo. Quindi, il nome ACL può essere specificato nel modello di dispositivo della funzione dell'interfaccia.

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

Total Task: 1 | Failure: 1

Q 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
```

## Informazioni correlate

- [Guida alla configurazione delle policy Cisco SD-WAN, Cisco IOS XE release 17.x](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).