

Configure a ACL para bloquear/corresponder o tráfego nas bordas com a política vManage

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o processo para bloquear/corresponder em um cEdge com uma política localizada e uma ACL (Access Control List, lista de controle de acesso) .

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)
- Cisco vManage
- Interface de linha de comando (CLI)

Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

- c8000v versão 17.3.3
- vManage versão 20.6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Há diferentes cenários que exigem um método local para bloquear, permitir ou corresponder o tráfego. Cada método controla o acesso ao roteador ou garante que os pacotes cheguem ao dispositivo e sejam processados.

Os roteadores cEdge oferecem a capacidade de configurar uma política localizada por meio de CLI ou vManage para corresponder às condições de tráfego e definir uma ação.

Estes são alguns exemplos de características localizadas da política:

Condições de correspondência:

- Ponto de código de serviços diferenciados (DSCP)
- Comprimento do pacote
- Protocolo
- Prefixo de Dados de Origem
- Porta de origem
- Prefixo de dados de destino
- Porta de Destino

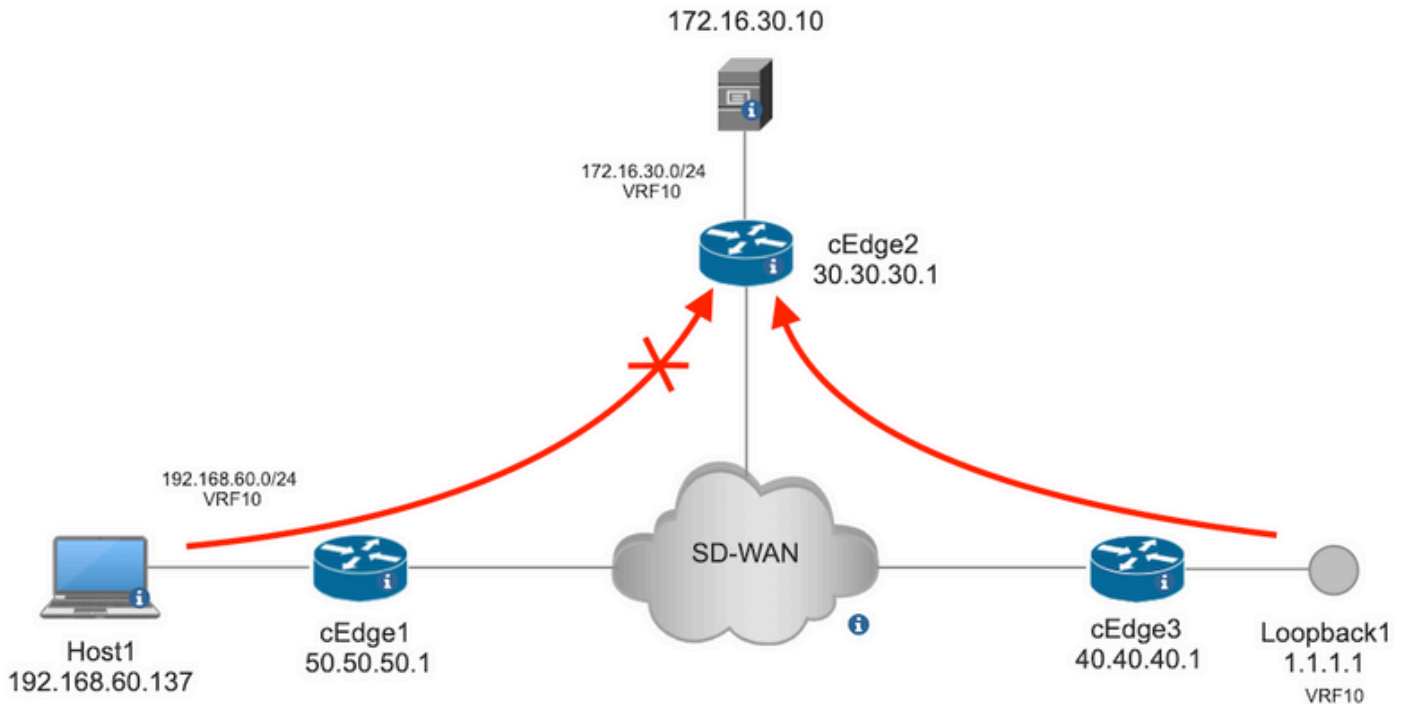
Ações:

- Aceitar Adicional: contador, DSCP, logs, nexthop, lista espelho, classe, policer
- Soltar Adicional: contador, log

Configurar

Diagrama de Rede

Para este exemplo, a intenção é bloquear o tráfego da rede 192.168.20.0/24 no cEdge2 com base na saída e permitir o ICMP da interface de loopback do cEdge3.



Verificação de ping do Host1 para o Servidor no 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
```

Verificação de ping do cEdge3 para o servidor no 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
```

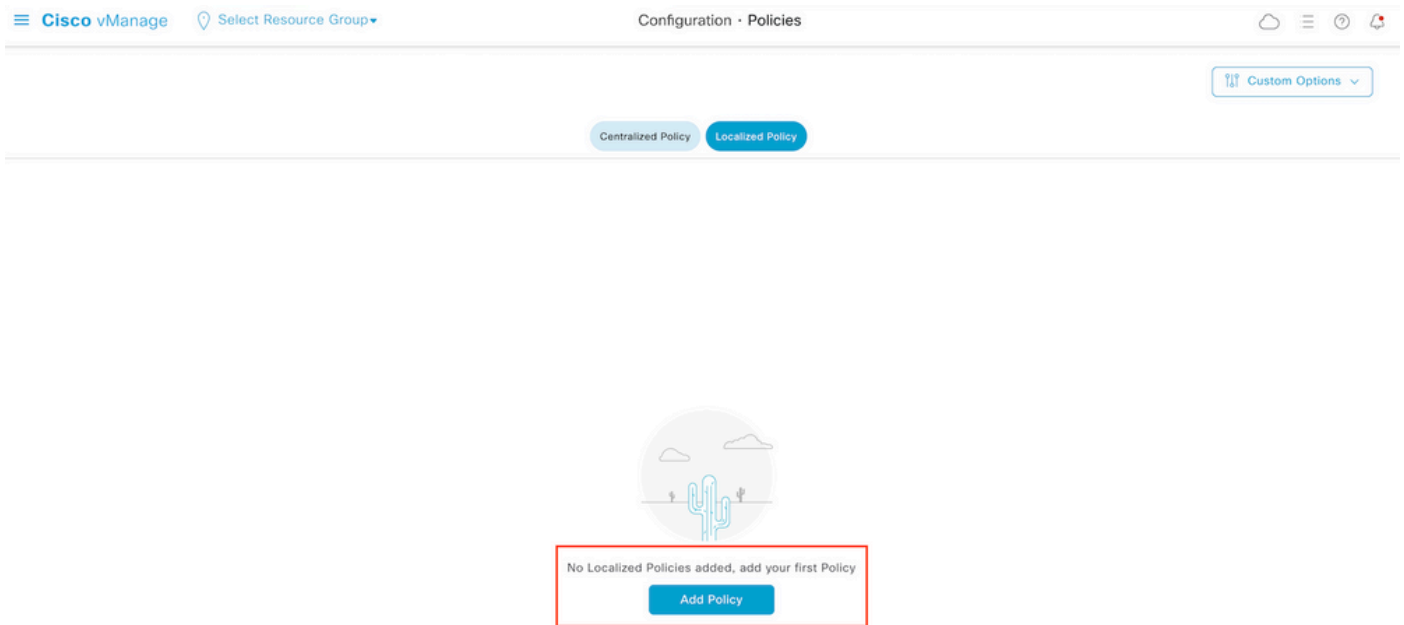
Condições prévias:

- O cEdge2 deve ter um modelo de dispositivo anexado.
- Todas as bordas devem ter conexões de controle ativas.
- Todas as Bordas devem ter sessões de Detecção de Encaminhamento Bidirecional (BFD) ativas.
- Todos os nós devem ter rotas de Protocolo de Gerenciamento de Sobreposição (OMP - Overlay Management Protocol) para acessar as redes do lado VPN10 de serviço.

Configurações

Etapa 1. Adicione a política localizada.

No Cisco vManage, navegue até **Configuration > Policies > Localized Policy**. Clique em **Add Policy**

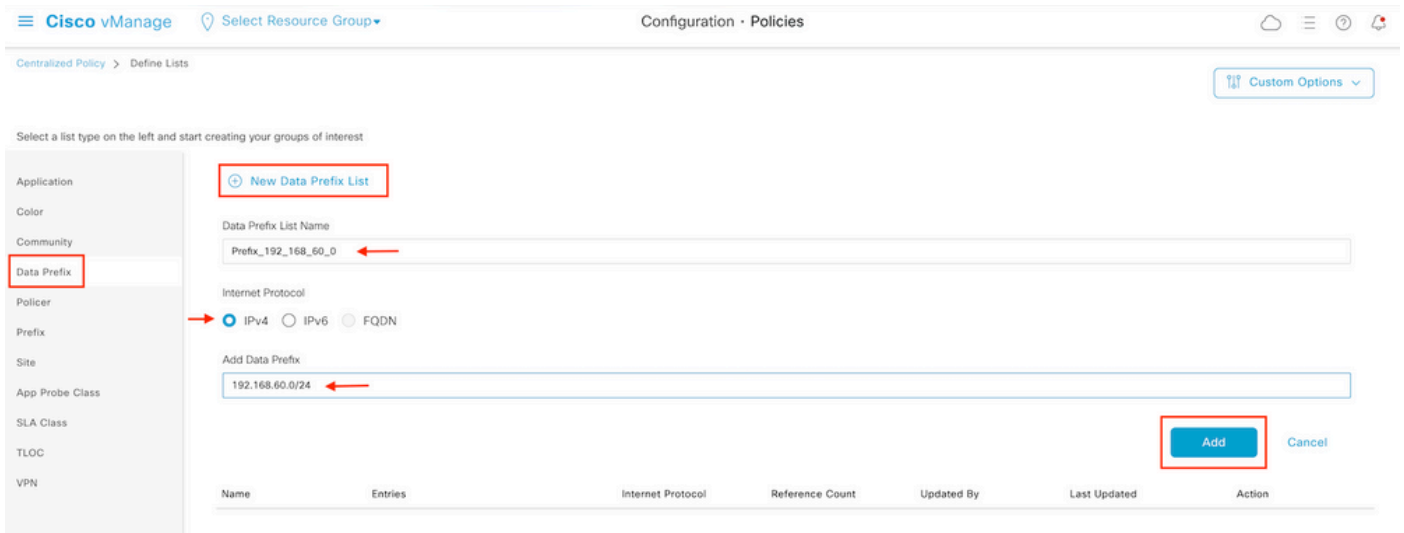


Etapa 2. Crie grupos de interesse para a correspondência desejada.

Clique em **Data Prefix** no menu à esquerda e selecione **New Data Prefix List**.

Dê um nome à condição de correspondência, defina o protocolo de Internet e adicione um prefixo de dados.

Clique em **Add** e depois **Next** até **Configure Access Control List** é exibido.



Etapa 3. Crie a lista de acesso para aplicar a condição de correspondência.

Selecionar **Add IPv4 ACL Policy NOS** **Add Access Control List Policy** menu suspenso.

Localized Policy > 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

Note: Este documento é baseado na política de lista de controle de acesso e não deve ser confundido com uma política de acesso a dispositivo. A política de acesso a dispositivos atua no plano de controle para serviços locais, como o SNMP (Simple Network Management Protocol) e o SSH (Secure Socket Shell), apenas, enquanto a política de lista de controle de acesso é flexível para diferentes serviços e condições de correspondência.

Etapa 4. Definir a sequência ACL

Na tela de configuração da ACL, nomeie a ACL e forneça uma descrição. Clique em **Add ACL Sequence** e depois **Sequence Rule**.

No menu de condições de correspondência, selecione **Source Data Prefix** e, em seguida, escolha a lista de prefixos de dados na **Source Data Prefix List** menu suspenso.

Access Control List configuration page showing the 'Add ACL Sequence' button and the 'Sequence Rule' configuration. The 'Match' tab is selected, and the 'Source Data Prefix' option is highlighted. The 'Source Data Prefix List' dropdown menu is open, showing 'Prefix_192_168_60_0' selected.

Etapa 5. Definir a ação para a sequência e nomeá-la

Navegue até **Action** selecionar **Drop**, e clique em **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

Note: Esta ação está exclusivamente associada à sequência em si, não à política localizada completa.

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

Etapa 6. No menu à esquerda, selecione **Default Action**, clicar **Edit**, e escolher **Accept**.

Cisco vManage Configuration · Policies

Add IPv4 ACL Policy

Name: ICMP_Block
Description: ICMP block from cEdge 1

Default Action

Accept Enabled

Note: Esta ação padrão está no final da política localizada. Não use **drop**, caso contrário, todo o tráfego pode ser afetado e causar uma interrupção de rede.

Clique em 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

Etapa 7. Nomear a política

Clique em **Next** até **Policy Overview** e dê um nome a ela. Deixe os outros valores em branco. Clique em **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](#)

Para garantir que a política esteja correta, clique em **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](#)

Verifique se a sequência e os elementos estão corretos na política.

Policy Configuration Preview

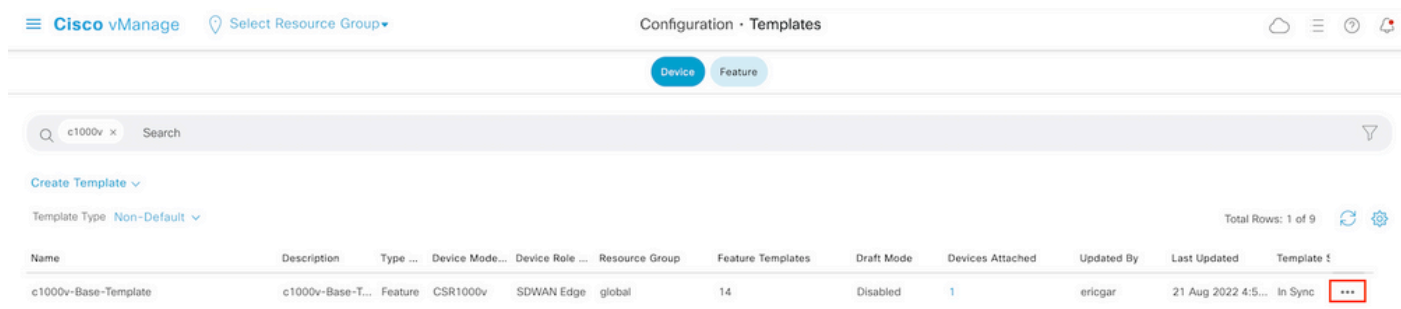
```
policy
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 ←
!
action drop ←
count ICMP_block_counter ←
!
!
default-action accept ←
!
lists
data-prefix-list Prefix_192_168_60_0
ip-prefix 192.168.60.0/24 ←
!
!
!
```

OK

Copie o nome da ACL. É necessário dar mais um passo.

Etapa 8. Associe a política localizada ao modelo do dispositivo.

Localize o modelo de dispositivo conectado ao roteador, clique nos três pontos e clique em **Edit**.



Selecionar **Additional Templates** e adicionar a política localizada ao campo de política e clique em **Update > Next > Configure Devices** para enviar a configuração para o 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.
```

Note: Neste ponto, o vManage cria a ACL com base na política criada e envia as alterações para o cEdge, embora não esteja associado a nenhuma interface. Portanto, não tem nenhum efeito no fluxo de tráfego.

Etapa 9. Identifique o modelo de recurso da interface em que pretende aplicar a ação ao tráfego no modelo do dispositivo.

É importante localizar o modelo de recurso onde o tráfego precisa ser bloqueado.

Neste exemplo, a interface GigabitEthernet3 pertence à Virtual Private Network 3 (Virtual Forwarding Network 3).

Navegue até a seção VPN de serviço e clique em **Edit** para acessar os modelos de VPN.

Neste exemplo, a interface GigabitEthernet3 tem o modelo de recurso c1000v-Base-VP10-IntGi3 anexado.

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

Etapa 10. Associe o nome da ACL à interface.

Navegue até **Configuration > Templates > Feature**. Filtre os modelos e clique em **Edit**

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. ...

Clique em **ACLs** e habilite a direção para o bloqueio do tráfego. Escreva o nome da ACL copiado na etapa 7. Clique em **Update** e enviar as alterações.

Device

Feature

Feature Template > Cisco VPN Interface Ethernet > 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

Observação: esse processo de criação de política localizada também funciona para vEdges porque a estrutura de política do vManage é a mesma para ambas as arquiteturas. A parte diferente é fornecida pelo modelo de dispositivo que cria uma estrutura de configuração compatível com cEdge ou vEdge.

Verificar

Etapa 1. Verificar as configurações corretamente no roteador

```
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

```

Etapa 2. Do Host 1 que está na rede de serviço do cEdge1, envie 5 mensagens ping ao servidor no 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

```

Note: Para este exemplo, host1 é uma máquina Linux. "-I" representa as interfaces em que o ping sai do roteador e "-c" representa o número de mensagens de ping.

Etapa 3. A partir do cEdge2, verifique os contadores da 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

```

O contador correspondeu a cinco (5) pacotes que vieram da rede 192.168.60.0/24, conforme definido na política.

Etapa 4. Do cEdge3, envie 4 mensagens ping ao servidor 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

```

Os pacotes passaram pelo roteador para o servidor porque a rede é diferente (nesse caso é 1.1.1.1/32) e não há nenhuma condição correspondente para ela na política.

Etapa 5. Verifique novamente os contadores ACL no 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
```

O contador de default_action_count incrementado com os 5 pacotes enviados pelo cEdge3.

Para limpar os contadores, execute `clear sdwan policy access-list` comando.

Comandos para verificação no vEdge

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

Troubleshoot

Erro: Referência ilegal ao nome da ACL na interface

A política que contém a ACL deve ser anexada primeiro ao modelo do dispositivo. Depois disso, o nome da ACL pode ser especificado no modelo de dispositivo de recurso da interface.

Push Feature Template Configuration | Validation Success
Initiated By: ericgar From: 72.163.2.247
Total Task: 1 | Failure: 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
```

Informações Relacionadas

- [Guia de configuração de políticas do Cisco SD-WAN, Cisco IOS XE versão 17.x](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.