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

Contents

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

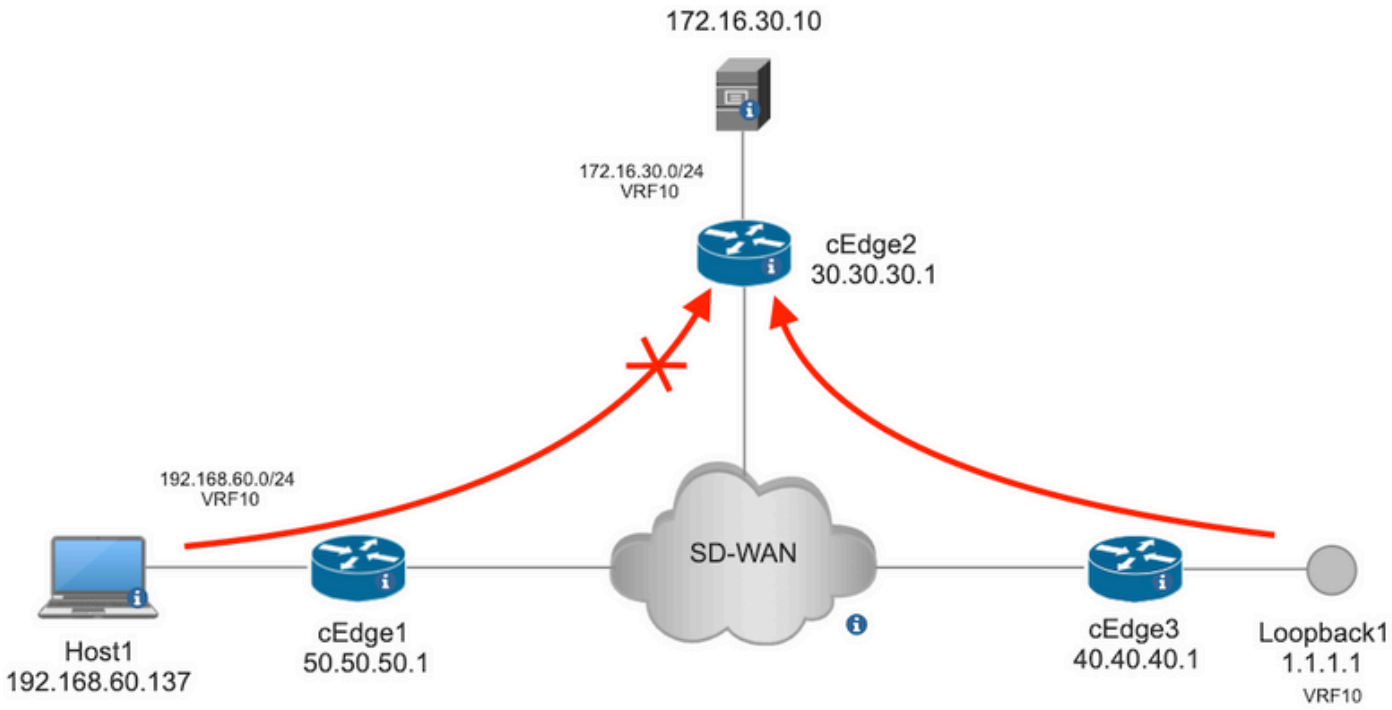
Ações:

- 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
```

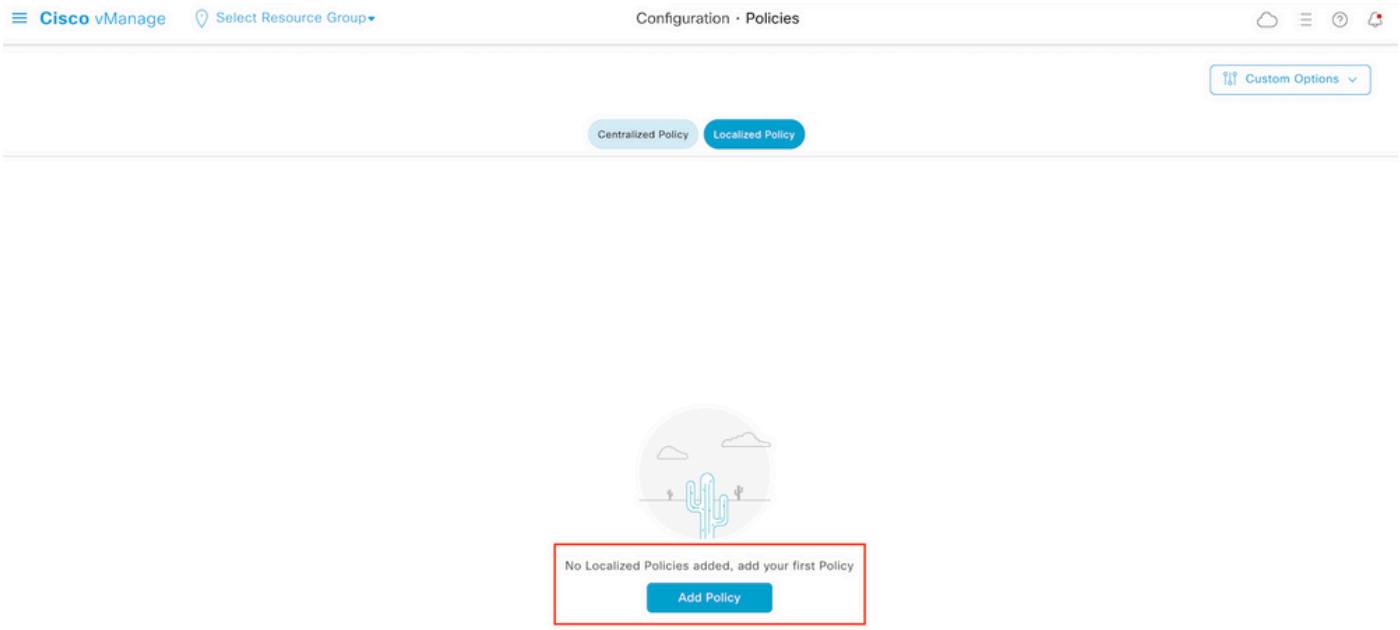
Condições prévias:

- 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**

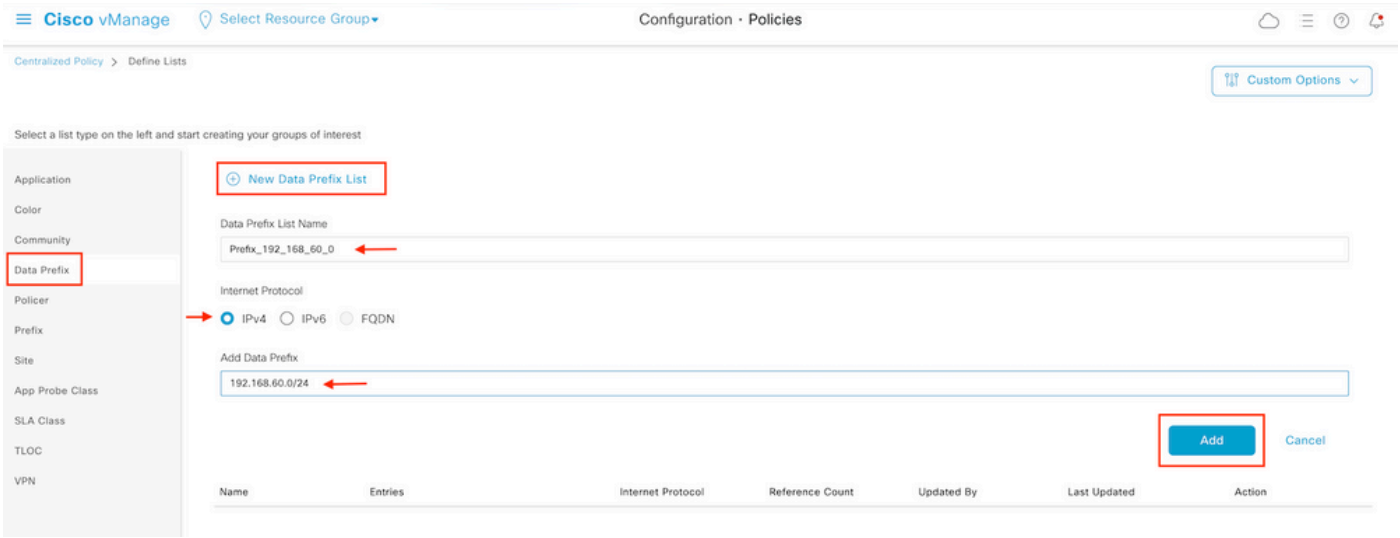


Etapa 2. Crie grupos de interesse para a correspondência desejada.

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

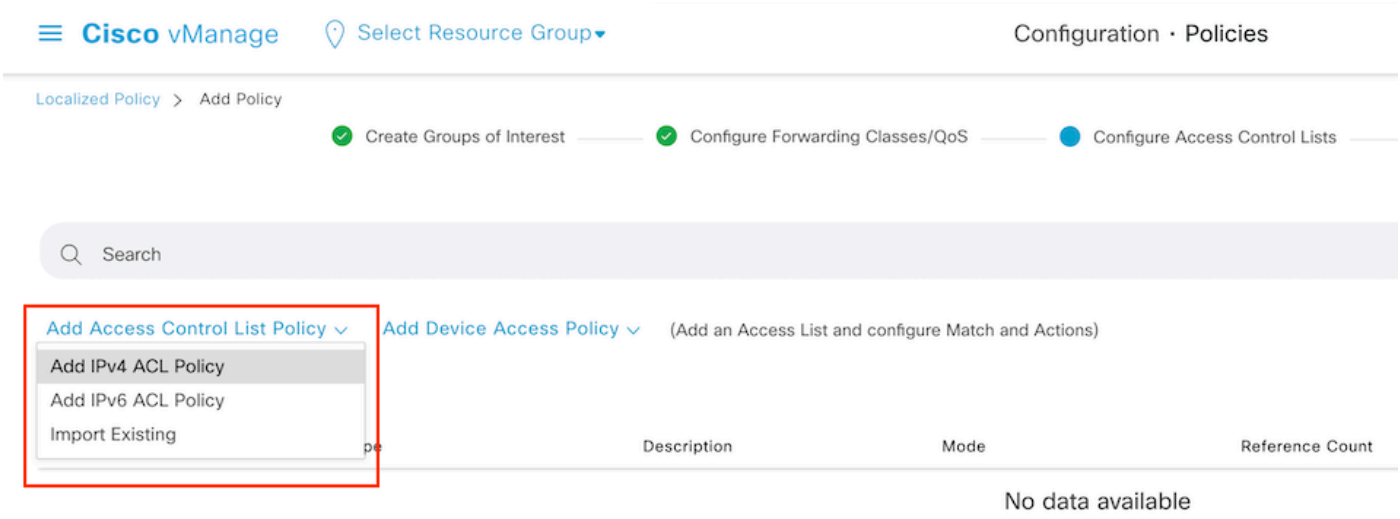
Dê um nome à condição de correspondência, defina o protocolo de Internet e adicione um prefixo de dados.

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.

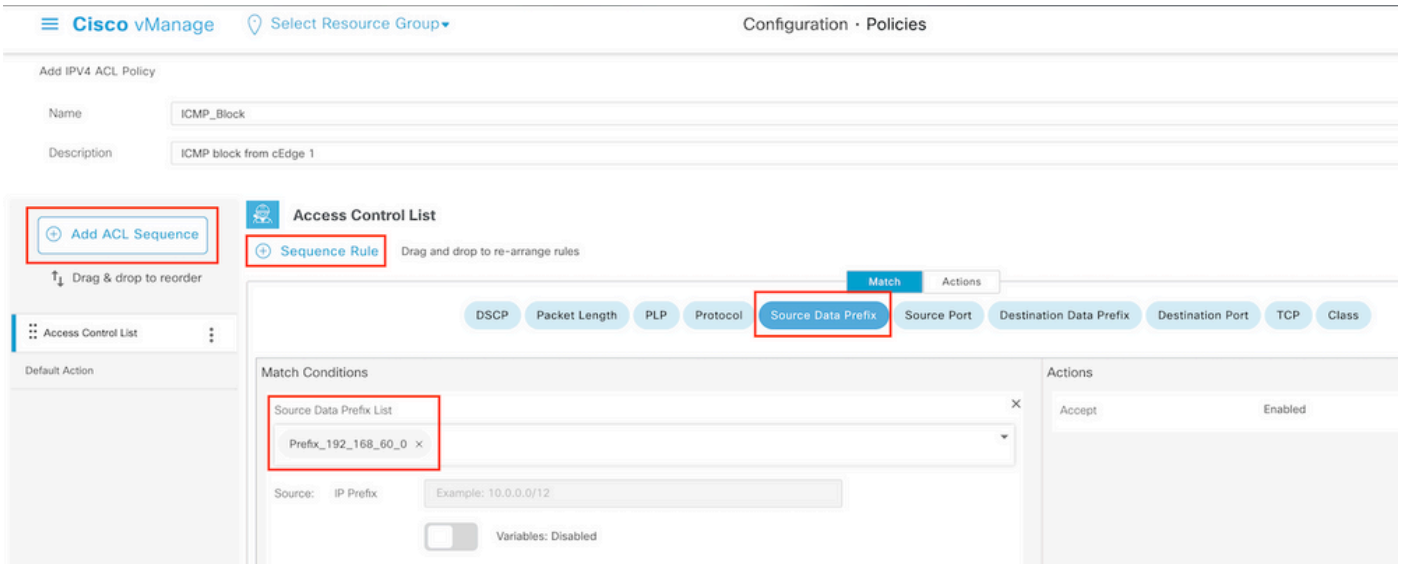


Note: Este documento é baseado na política de lista de controle de acesso e não deve ser confundido com uma política de acesso a dispositivo. A política de acesso a dispositivos atua no plano de controle para serviços locais, como o SNMP (Simple Network Management Protocol) e o SSH (Secure Socket Shell),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

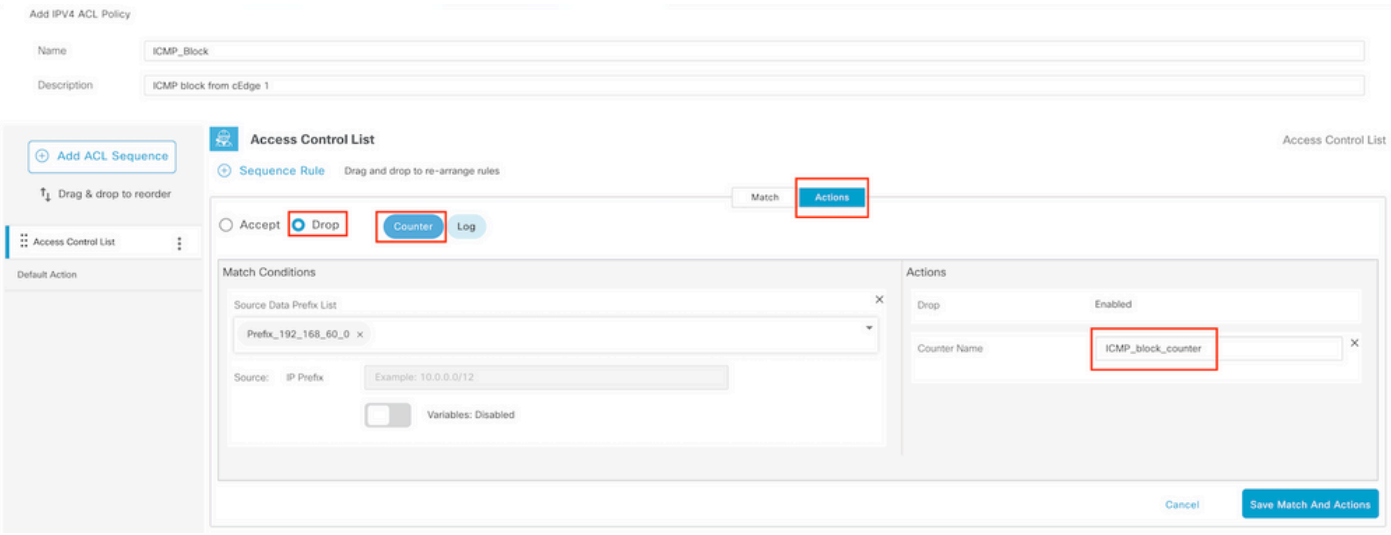
Na tela de configuração da ACL, nomeie a ACL e forneça uma descrição. Clique em **Add ACL Sequence** e depois **Sequence Rule.**

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.

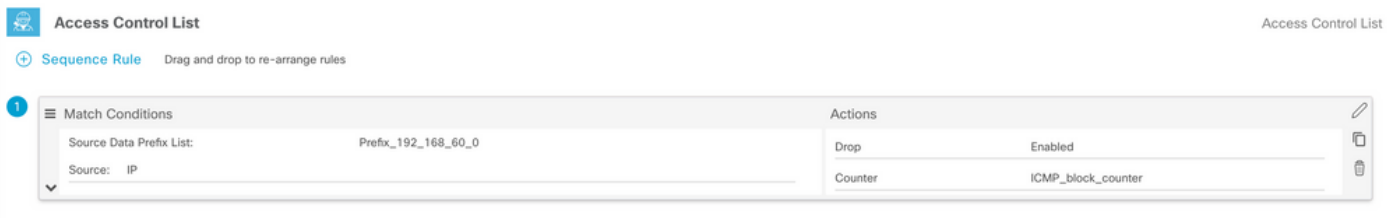


Etapa 5. Definir a ação para a sequência e nomeá-la

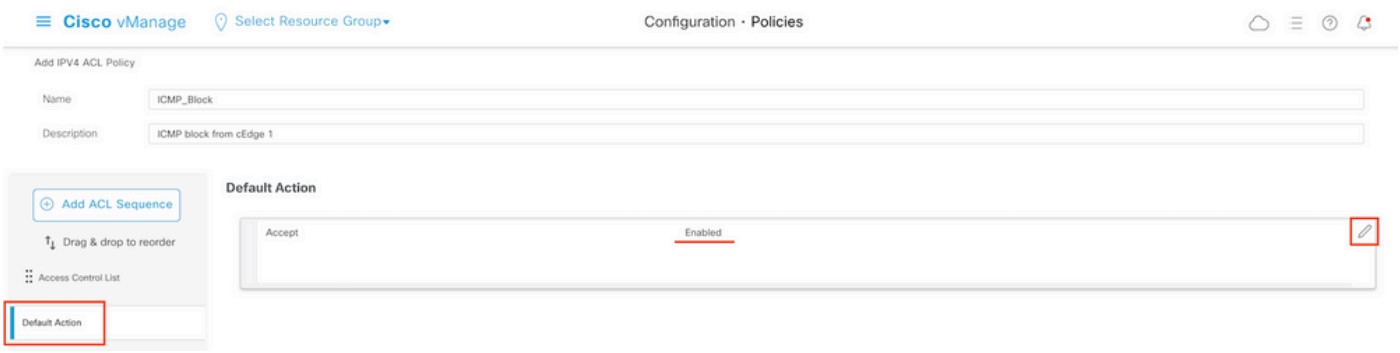
Navegue até **Action** selecionar **Drop**, e clique em **Save Match** e **Actions**.



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



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

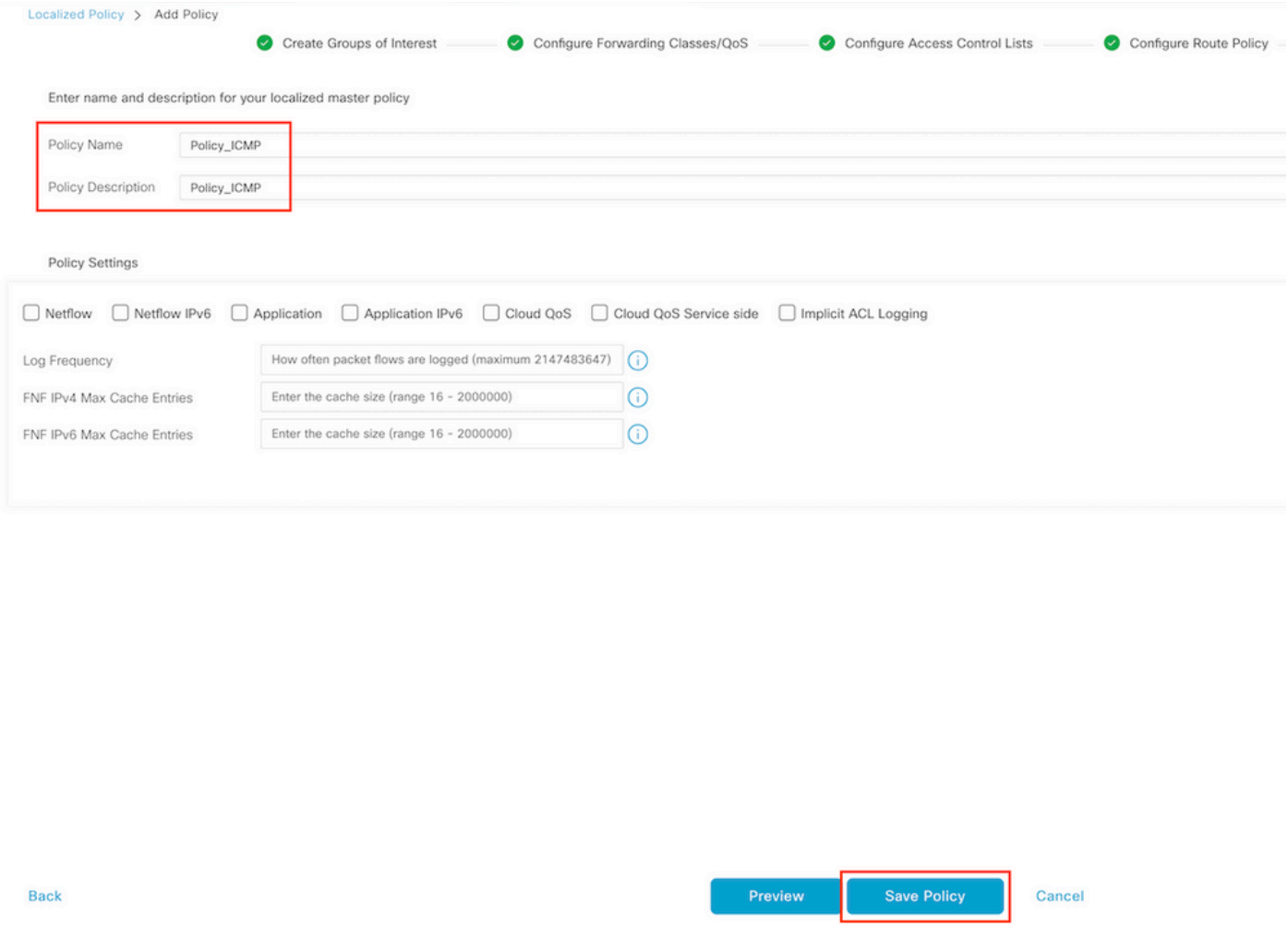


Note: Esta ação padrão está no final da política localizada. Não use **drop**, caso contrário, todo o tráfego pode ser afetado e causar uma interrupção de rede.

Clique em **Save Access Control List Policy.**

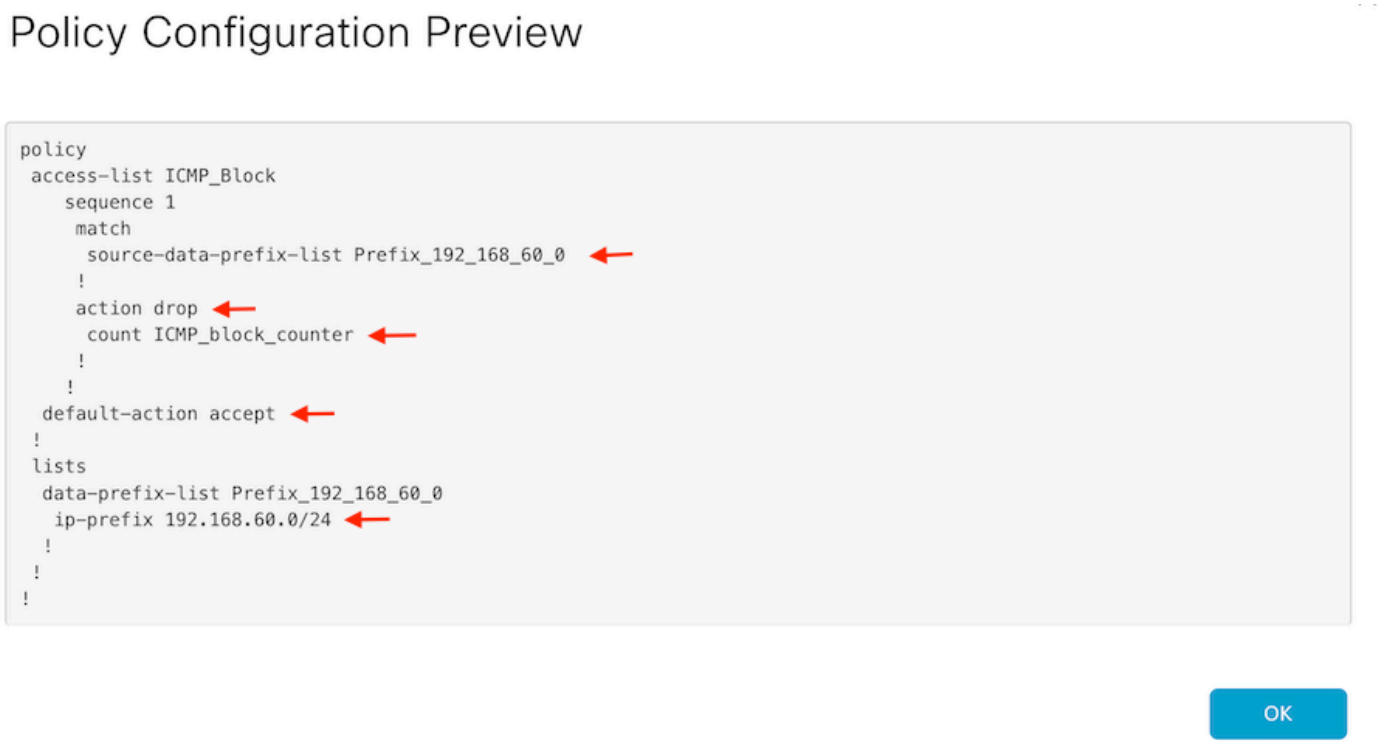
Etapa 7. Nomear a política

Clique em **Next** até **Policy Overview** e dê um nome a ela. Deixe os outros valores em branco. Clique em **Save Policy**



Para garantir que a política esteja correta, clique em **Preview**.

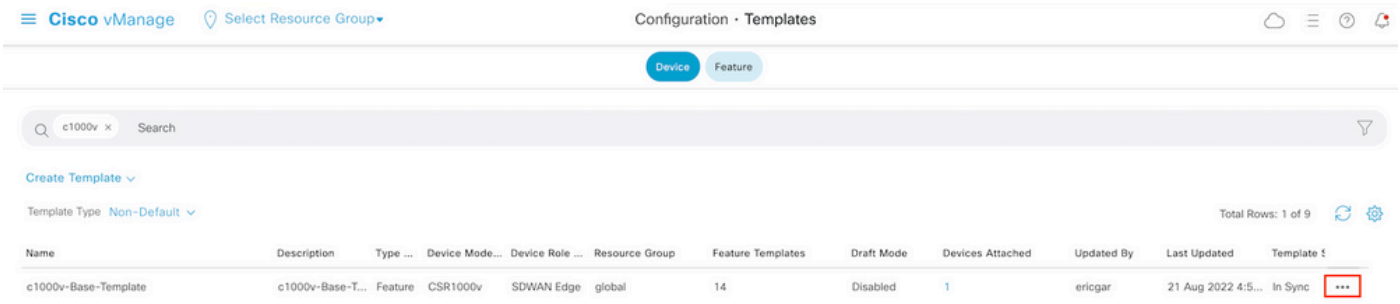
Verifique se a sequência e os elementos estão corretos na política.



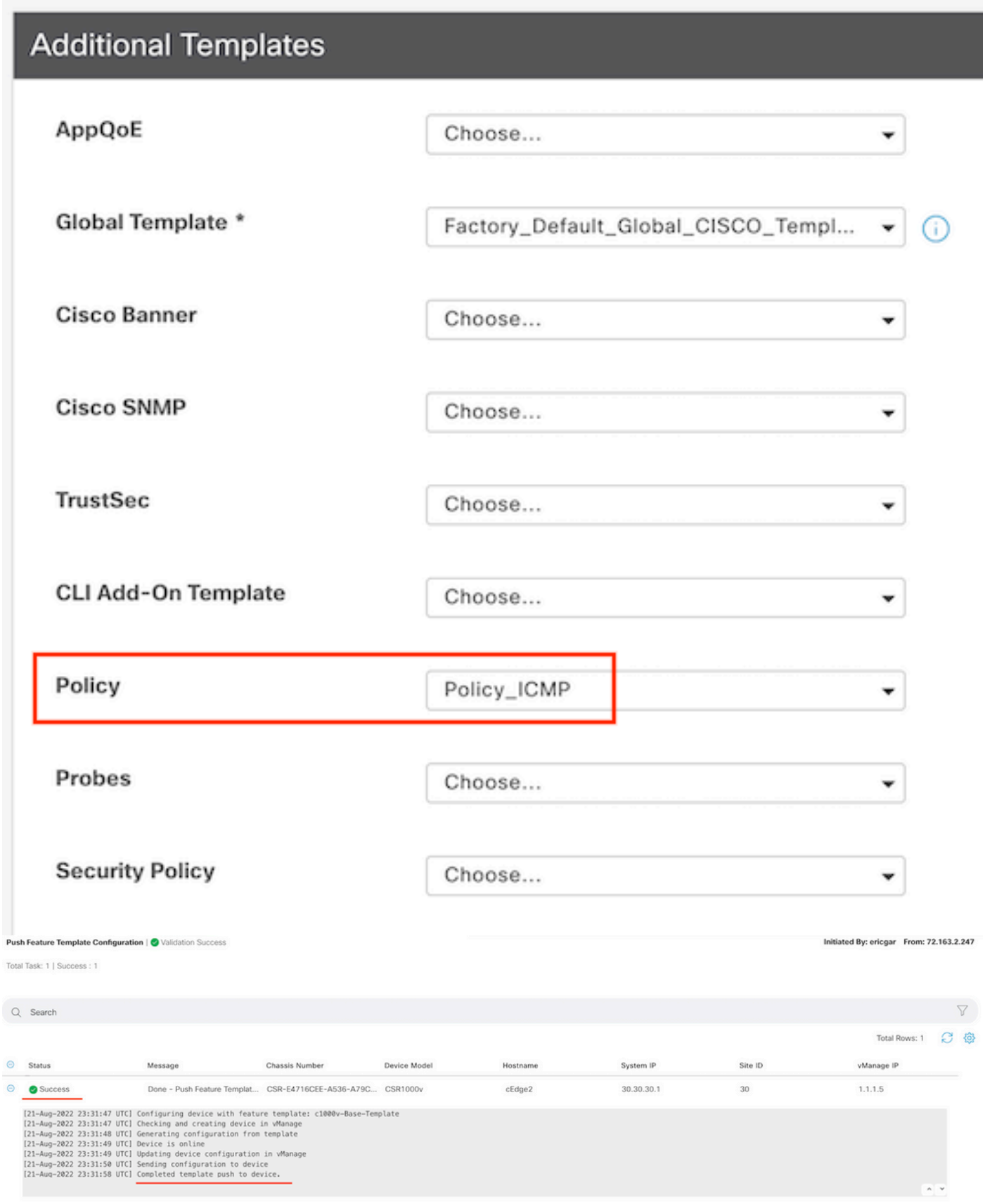
Copie o nome da ACL. É necessário dar mais um passo.

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.



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.

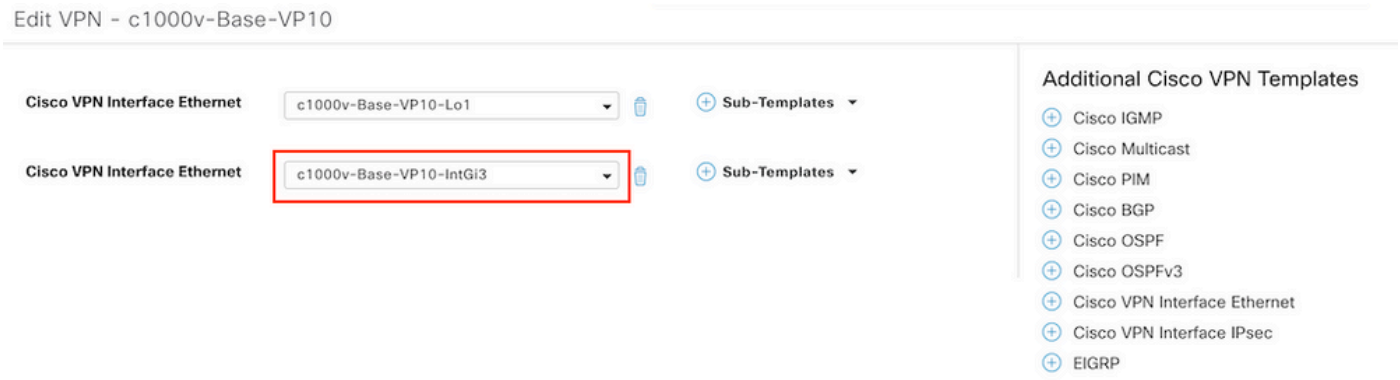
Etapa 9. Identifique o modelo de recurso da interface em que pretende aplicar a ação ao tráfego no modelo do dispositivo.

Éimportante 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).

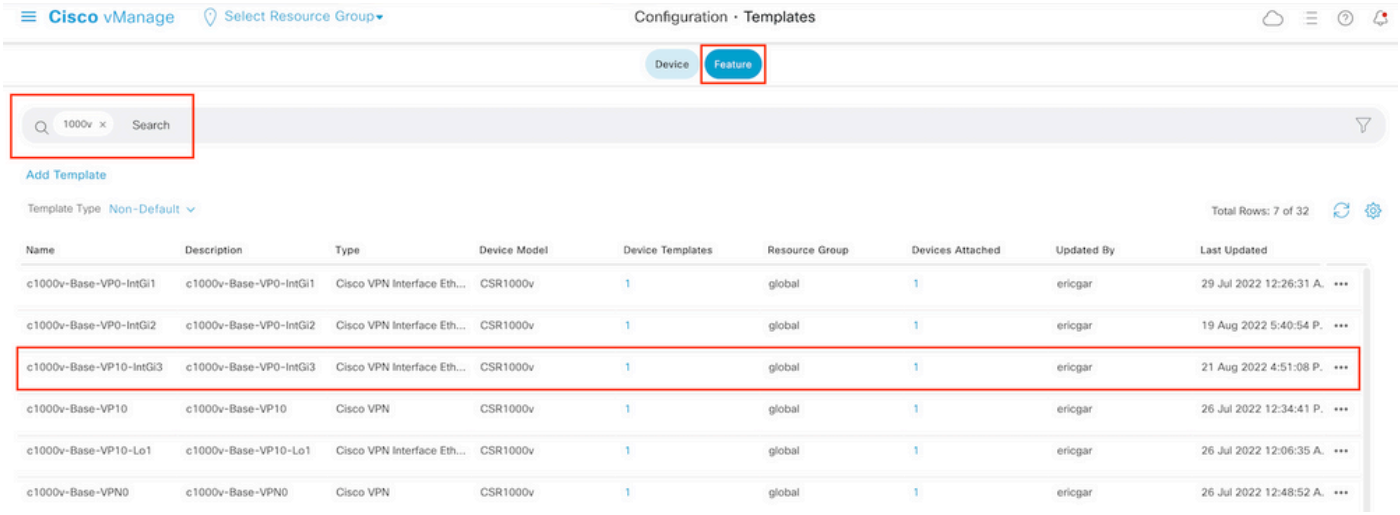
Navegue até a seção VPN de serviço e clique em **Edit** para acessar os modelos de VPN.

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

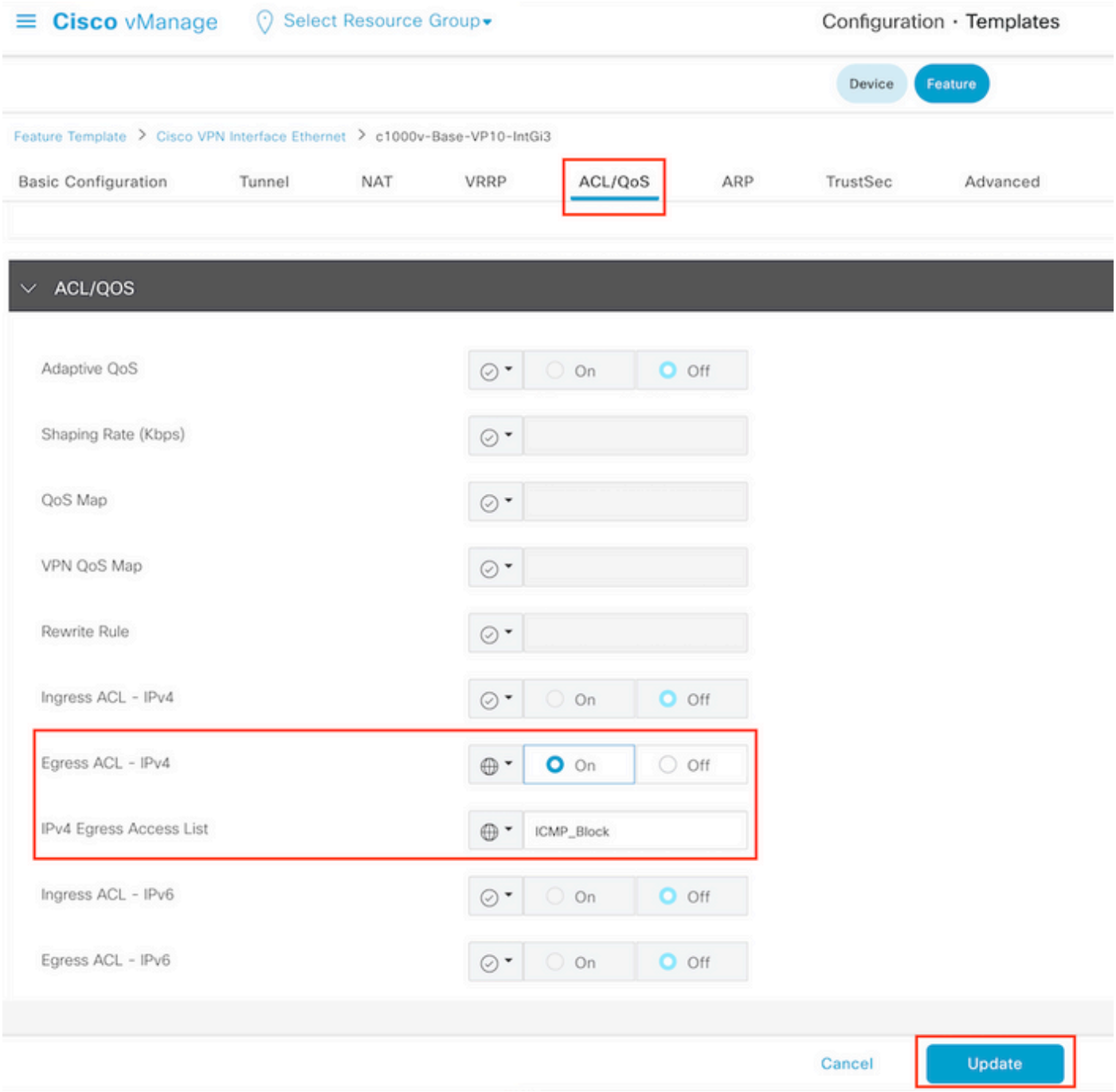


Etapa 10. Associe o nome da ACL à interface.

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



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



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.

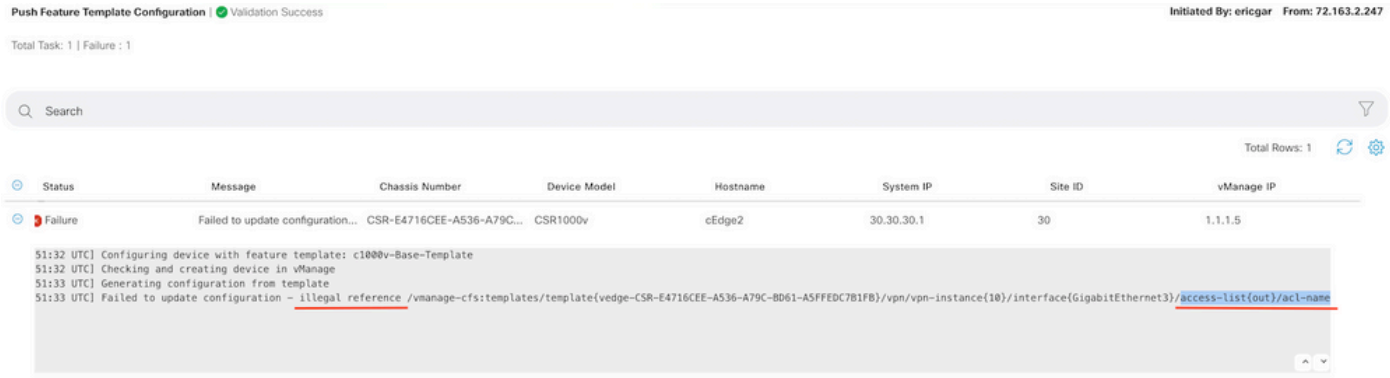
Comandos para verificação no vEdge

```
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.



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.