使用vManage策略配置ACL以阻止/匹配边缘上的流量

目录

简介

本文档介绍使用本地化策略和访问控制列表(ACL)阻止/匹配cEdge中的过程。

先决条件

要求

建议掌握下列主题的相关知识：

- 思科软件定义的广域网(SD-WAN)
- Cisco vManage
- cEdge命令行界面(CLI)

使用的组件

本文档基于以下软件和硬件版本：

- c8000v版本17.3.3
- vManage 20.6.3版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

有多种不同的场景需要使用本地方法来阻止、允许或匹配流量。每种方法都控制对路由器的访问

，或确保数据包到达设备并被处理。

边缘路由器可通过CLI或vManage配置本地化策略，以匹配流量条件并定义操作。

以下是一些本地化策略特征的示例：

匹配条件：

- 差分服务代码点(DSCP)
- 数据包长度
- 协议
- 源数据前缀
- 源端口
- 目标数据前缀
- 目标端口

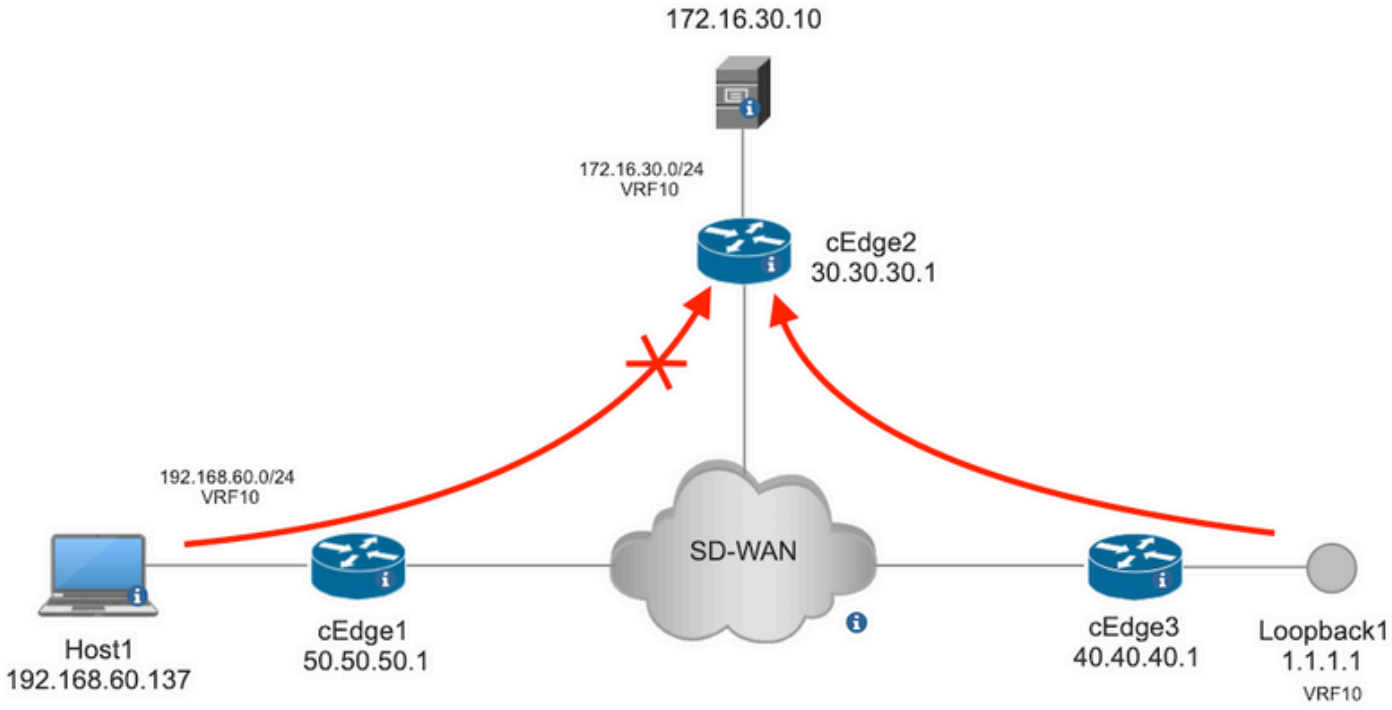
操作:

- Accept（接受）其他：计数器， DSCP， logs， nexthop， mirror list， class， policer
- 丢弃 其他：计数器、日志

配置

网络图

在本例中，目的是以出口方式阻止cEdge2中网络192.168.20.0/24的流量，并允许来自cEdge3环回接口的ICMP。



从Host1 ping cEdge2中的服务器。

```
[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
```

从cEdge3 ping cEdge2中的服务器。

```
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
```

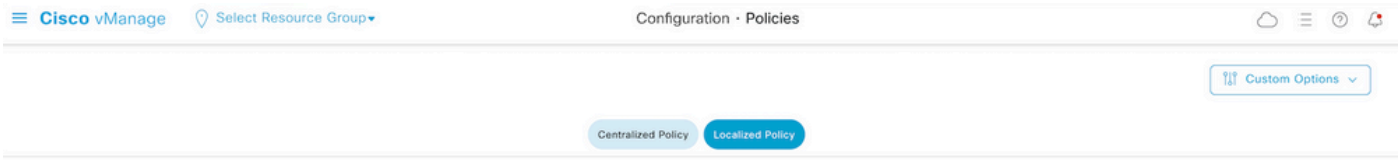
前提条件：

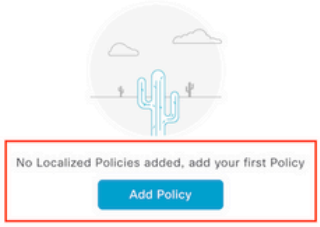
- cEdge2必须附加设备模板。
- 所有cEdge都必须激活控制连接。
- 所有cEdge必须激活双向转发检测(BFD)会话。
- 所有终端必须具有重叠管理协议(OMP)路由才能到达服务VPN10端网络。

配置

步骤1.添加本地化策略。

在Cisco vManage中，导航至 **Configuration > Policies > Localized Policy**.点击 **Add Policy**





步骤2.创建目标匹配的兴趣组。

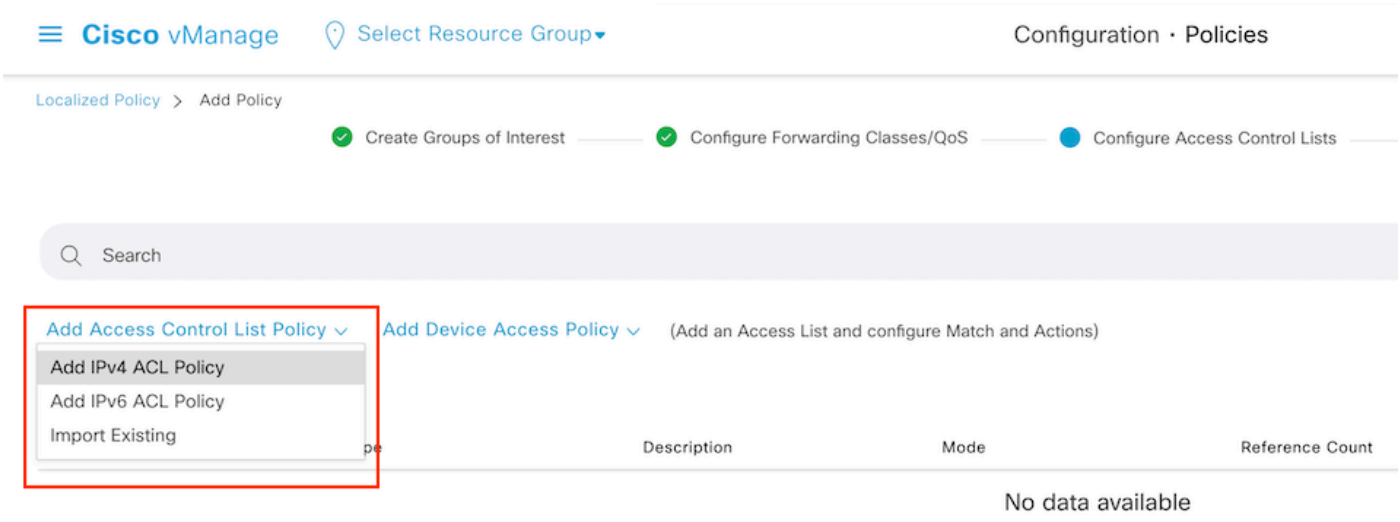
点击 **Data Prefix** 在左侧菜单中选择 **New Data Prefix List.**

为匹配条件指定名称，定义Internet协议，并添加数据前缀。

点击 **Add** 然后 **Next** 直到 **Configure Access Control List** 显示。

步骤3.创建访问列表以应用匹配条件。

选择 **Add IPv4 ACL Policy** 从 **Add Access Control List Policy** 下拉菜单。

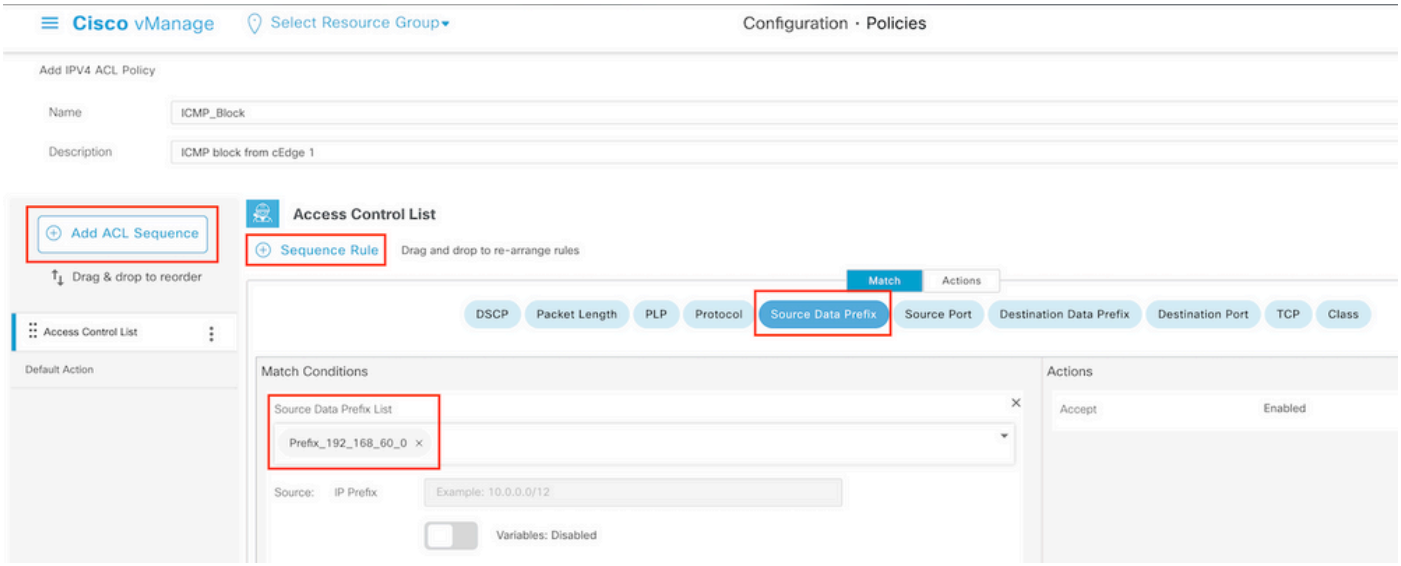


注意：本文档基于访问控制列表策略，不得与设备访问策略相混淆。设备访问策略仅在本地服务(如简单网络管理协议(SNMP)和安全套接字外壳(SSH))的控制计划中起作用，而访问控制列表策略对不同服务和匹配条件而言是灵活的。

步骤4.定义ACL序列

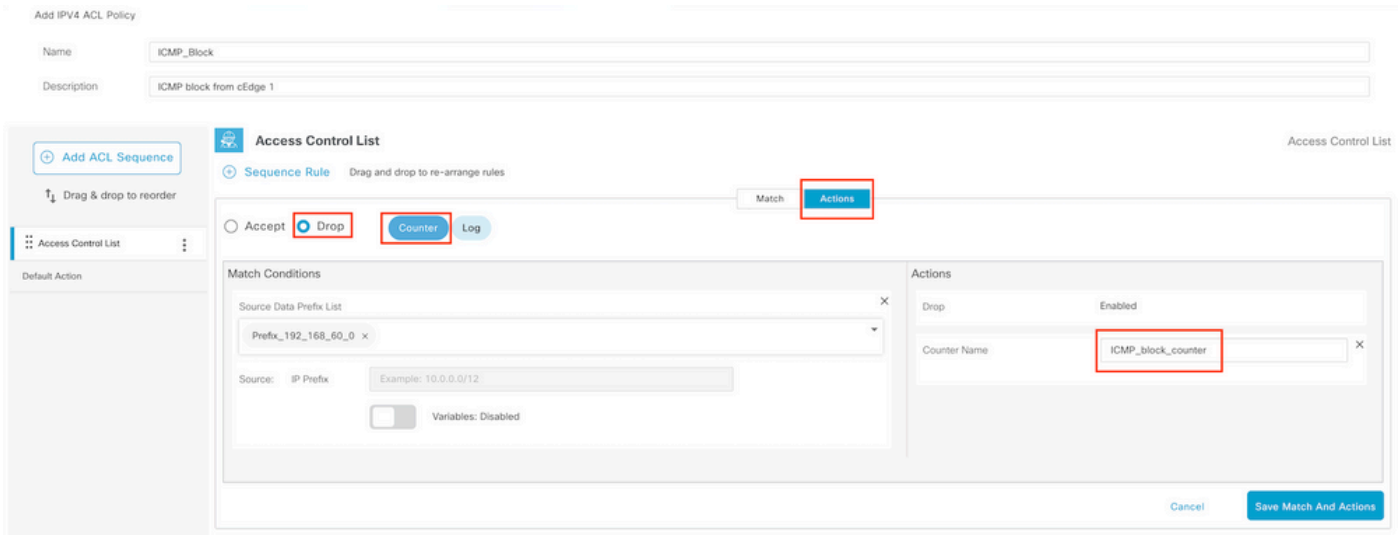
在ACL配置屏幕中，命名ACL并提供说明。点击 **Add ACL Sequence** 然后 **Sequence Rule.**

在匹配条件菜单中，选择 **Source Data Prefix** 然后从 **Source Data Prefix List** 下拉菜单。

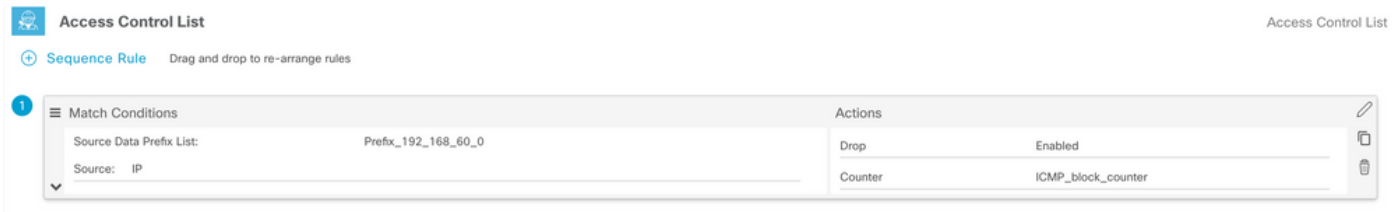


步骤5.定义序列的操作并为其命名

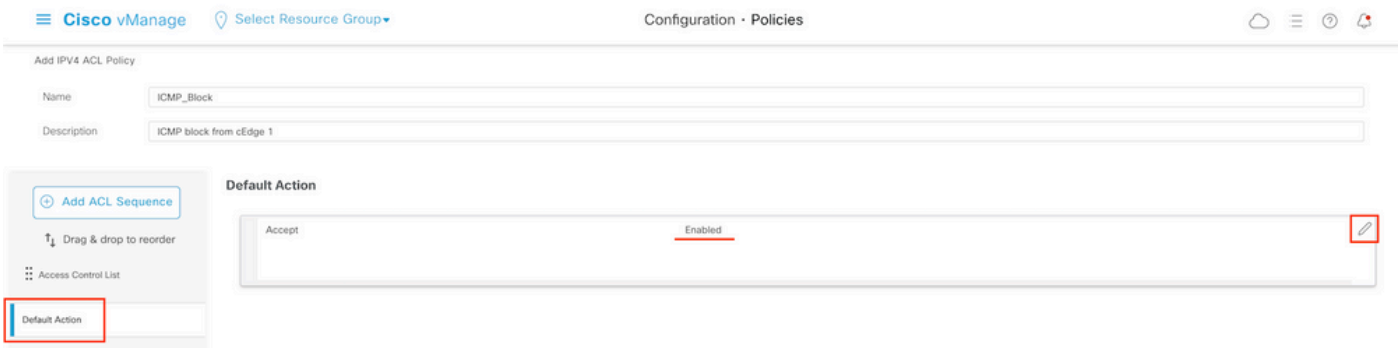
导航至 **Action** 选择 **Drop,** 并点击 **Save Match** 和 **Actions.**



注意：此操作仅与序列本身相关联，而不与完整的本地化策略相关联。



步骤6.在左侧菜单中，选择 **Default Action** ,点击 **Edit,** 选择 **Accept.**

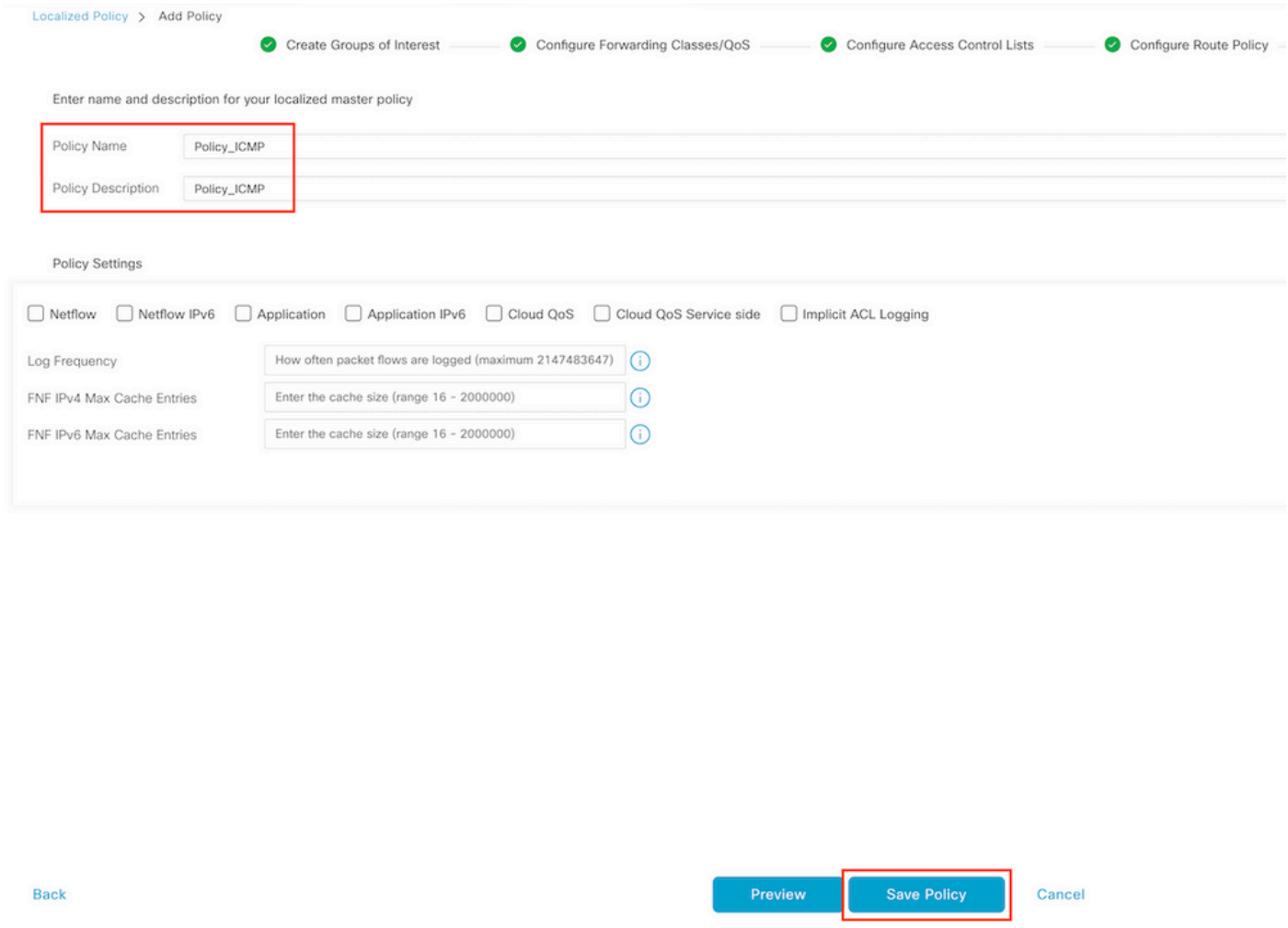


注意：此默认操作位于本地化策略的结尾。请勿使用**drop**，否则，所有流量都会受到影响并导致网络中断。

点击 **Save Access Control List Policy.**

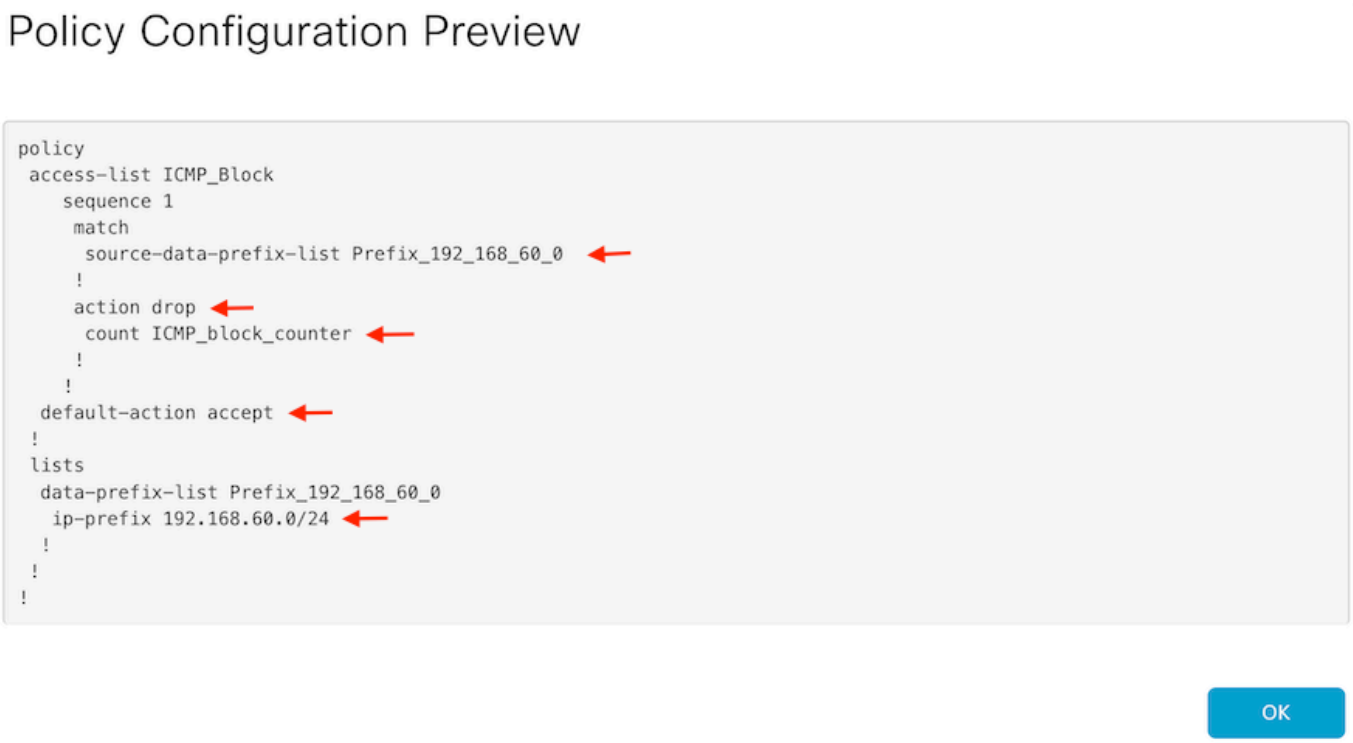
步骤7.命名策略

点击 **Next** 直到 **Policy Overview** 并命名。将其他值留空。点击 **Save Policy**



要确保策略正确，请单击 **Preview.**

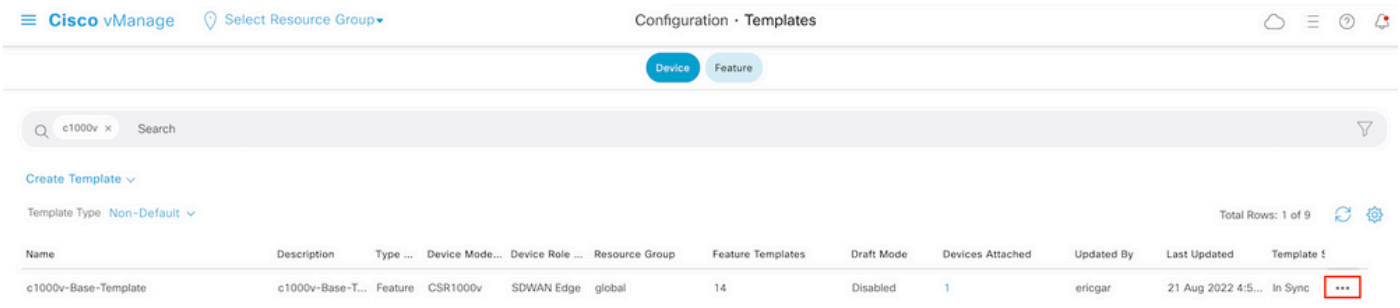
验证策略中的顺序和元素是否正确。



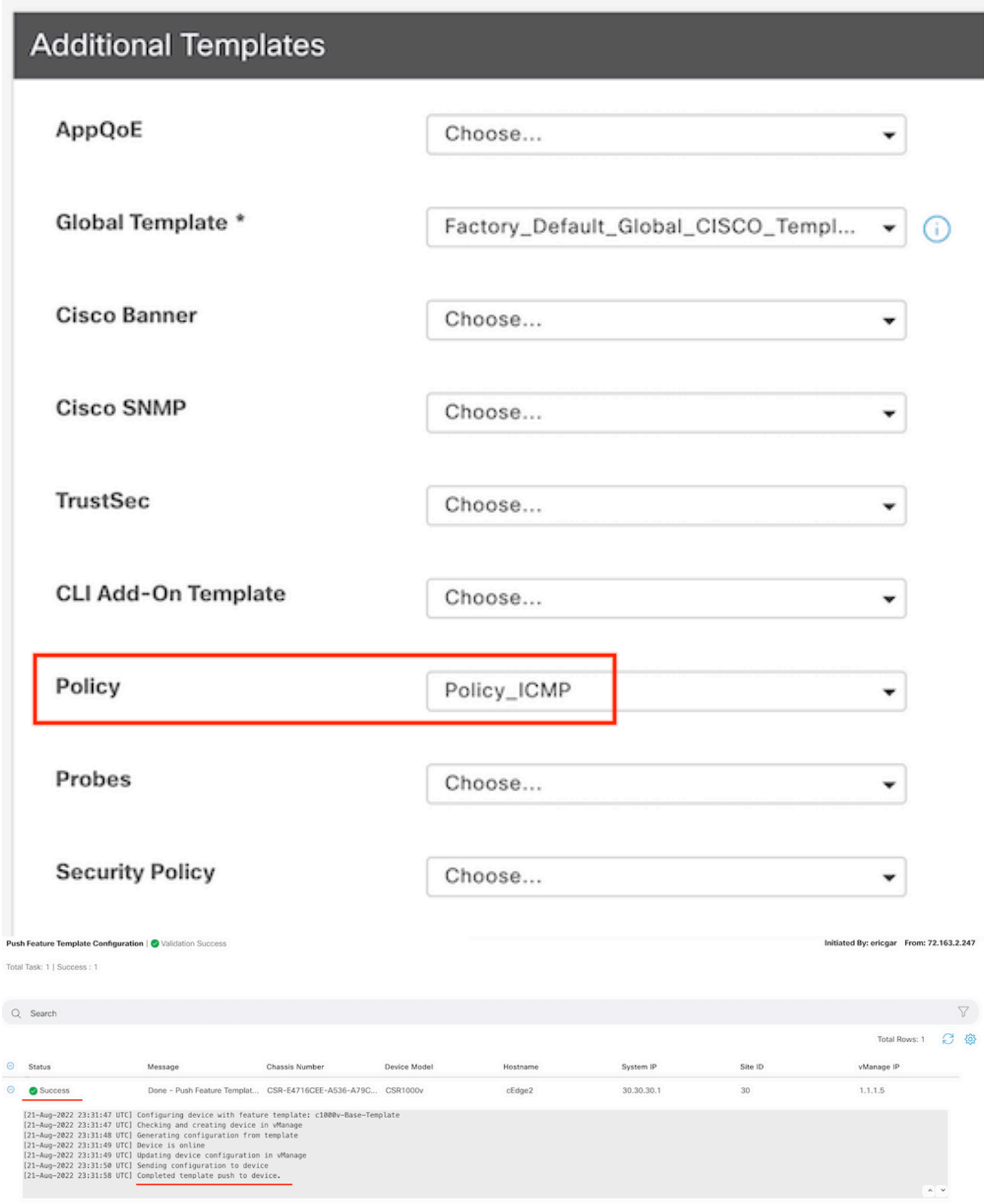
复制ACL名称。这是进一步操作所必需的。

步骤8.将本地化策略与设备模板关联。

找到连接到路由器的设备模板，单击三个点，然后单击 **Edit**.



选择 **Additional Templates** 并将本地化策略添加到策略字段，然后点击 **Update > Next > Configure Devices** 将配置推送到cEdge。



注意：此时，vManage基于创建的策略构建ACL并将更改推送到cEdge，不过它不与任何接口关联。因此，它对流量没有任何影响。

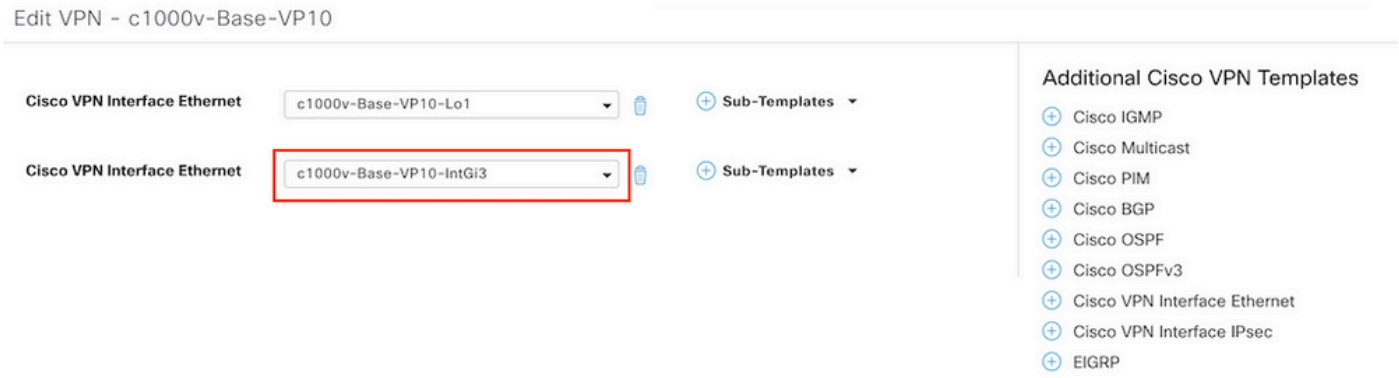
第9步：确定接口的功能模板，在该模板中将操作应用于设备模板中的流量。

找到需要阻止流量的功能模板非常重要。

在本示例中，GigabitEthernet3接口属于虚拟专用网络3（虚拟转发网络3）。

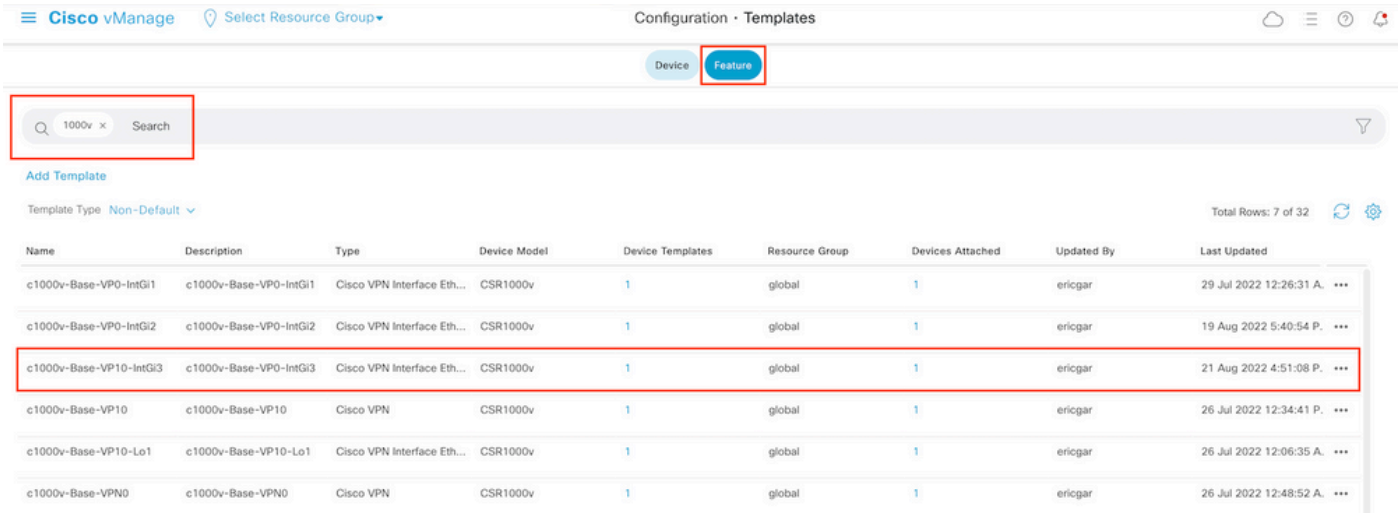
导航到服务VPN部分并单击 **Edit** 访问VPN模板。

在本示例中，GigabitEthernet3接口附加c1000v-Base-VP10-IntGi3功能模板。

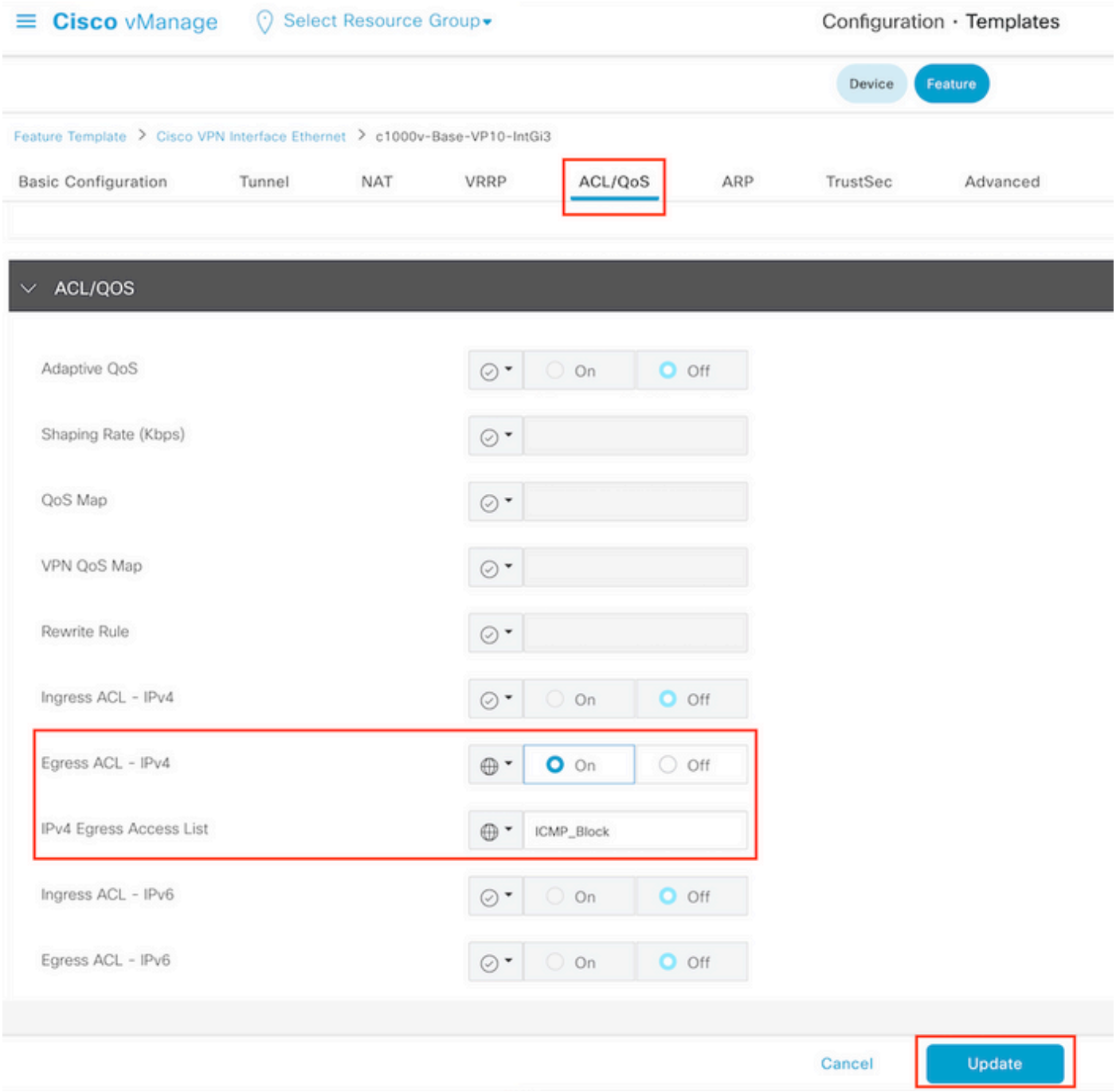


步骤10.将ACL名称与接口关联。

导航至 **Configuration > Templates > Feature.** 过滤模板并单击 **Edit**



点击 **ACL/QoS** 并启用要阻止流量的方向。写下步骤7中复制的ACL名称。单击 **Update** 并推动变革。



注意：此本地化策略创建流程也适用于vEdge，因为两个架构的vManage策略结构相同。不同部分由设备模板提供，用于构建与cEdge或vEdge兼容的配置结构。

验证

步骤1.检验路由器中的配置是否正确

```
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
```

步骤2.从cEdge1的服务网络中的Host1，向cEdge2中的服务器发送5条ping消息

```
[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
```

> **注意**：在本示例中，host1是Linux计算机。“ — I”表示ping离开路由器的接口，“ — c”表示ping消息的数量。

步骤3.从cEdge2检验ACL计数器

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

根据策略中的定义，计数器与来自网络192.168.60.0/24的五(5)个数据包匹配。

步骤4.从cEdge3向服务器172.16.30.10发送4条ping消息

```
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
```

由于网络不同(在本例中为1.1.1.1/32)，且策略中没有与数据包匹配的条件而通过路由器传送到服务器的数据包。

步骤5.再次检验cEdge2中的ACL计数器。

```
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的计数器随cEdge3发送的5个数据包递增。

要清除计数器，请运行 **clear sdwan policy access-list** 命令。

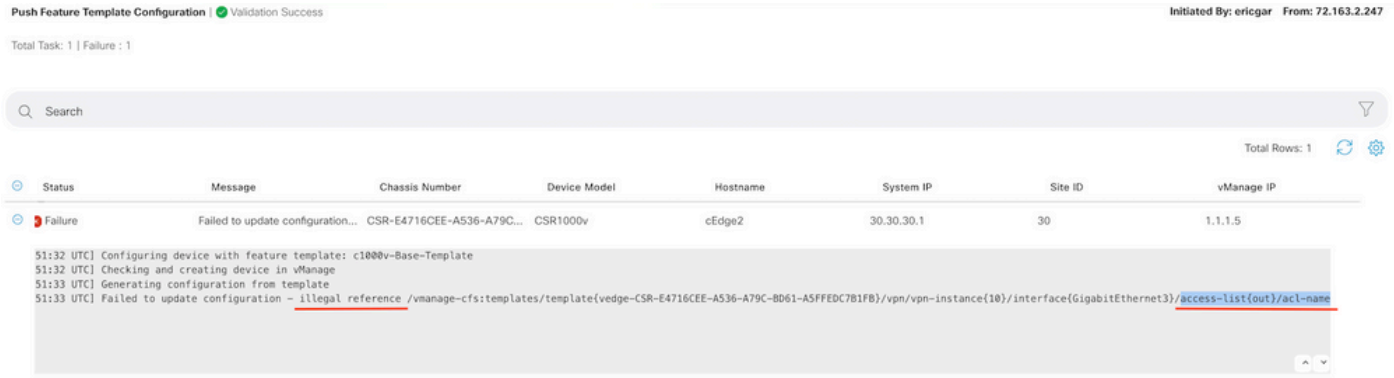
用于在vEdge中进行验证的命令

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

故障排除

Error:在接口中非法引用ACL名称

必须首先将包含ACL的策略附加到设备模板。之后，可以在接口的功能设备模板中指定ACL名称。



相关信息

- [Cisco SD-WAN策略配置指南，Cisco IOS XE版本17.x]
- [技术支持和文档 - Cisco Systems]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。