# Configuración de ACL para bloquear/hacer coincidir el tráfico en las fronteras con la política vManage

## Contenido



## Introducción

Este documento describe el proceso para bloquear/hacer coincidir en un cEdge con una política localizada y una Lista de control de acceso (ACL) .

## Prerequisites

### Requirements

Cisco recomienda conocer estos temas:

- Red de área extensa definida por software de Cisco (SD-WAN)
- Cisco vManage
- Interfaz de línea de comandos (CLI) de cEdge

### Componentes Utilizados

Este documento se basa en estas versiones de software y hardware:

- c8000v versión 17.3.3
- vManage versión 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Background

Hay diferentes escenarios que requieren un método local para bloquear, permitir o hacer coincidir el tráfico. Cada método controla el acceso al router o garantiza que los paquetes lleguen al dispositivo y se procesen.

Los routers cEdge proporcionan la capacidad de configurar una política localizada a través de CLI o vManage para que coincida con las condiciones del tráfico y defina una acción.

Estos son algunos ejemplos de características de políticas localizadas:

#### Condiciones de coincidencia:

- Punto de código de servicios diferenciados (DSCP)
- Longitud del paquete
- Protocolo
- Prefijo de datos de origen
- Puerto de Origen
- Prefijo de datos de destino
- Puerto de Destino

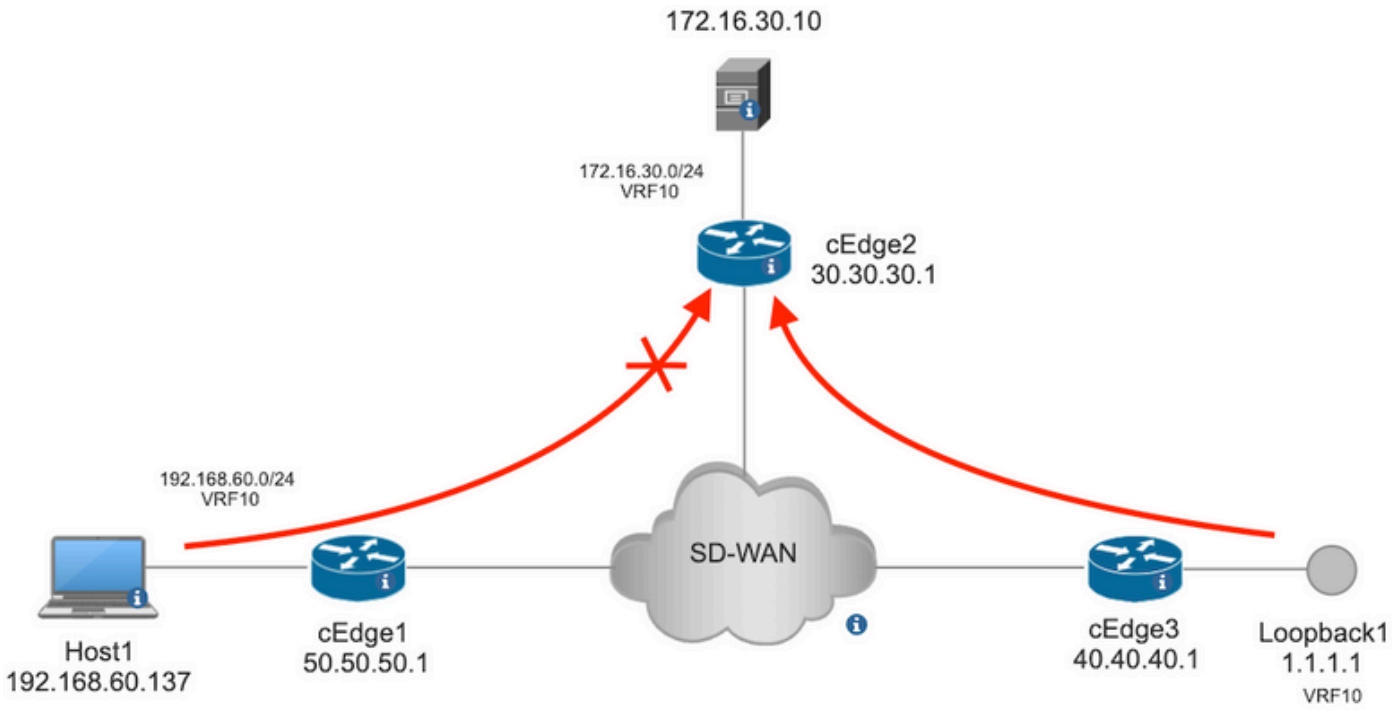
#### Acciones:

- Aceptar Adicional: counter, DSCP, logs, nexthop, mirror list, class, policer
- Abandonar Adicional: contador, registro

# Configurar

## Diagrama de la red

Para este ejemplo, la intención es bloquear el tráfico de la red 192.168.20.0/24 en cEdge2 en base a la salida y permitir el ICMP de la interfaz de loopback cEdge3.




Verificación de ping del Host1 al Servidor en 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
```

Verificación de ping desde cEdge3 al servidor en 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
```

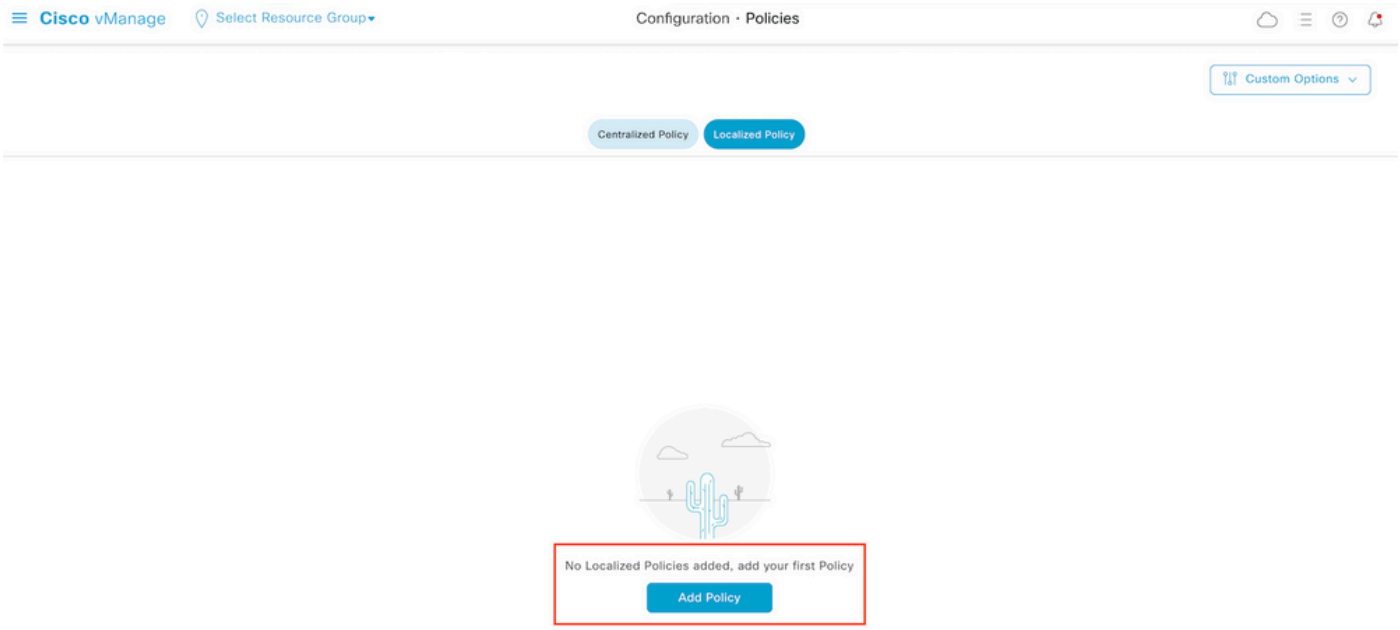
### Condiciones previas:

- cEdge2 debe tener una plantilla de dispositivo conectada.
- Todas las aristas deben tener conexiones de control activas.
- Todas las aristas deben tener activas sesiones de detección de reenvío bidireccional (BFD).
- Todos los switches deben tener rutas de protocolo de administración de superposición (OMP) para alcanzar las redes del lado VPN10 del servicio.

## Configuraciones

**Paso 1**. Agregue la política localizada.

En Cisco vManage, vaya a **Configuration > Policies > Localized Policy**. Haga clic **Add Policy**




**Paso 2.** Crear grupos de interés para la coincidencia deseada.

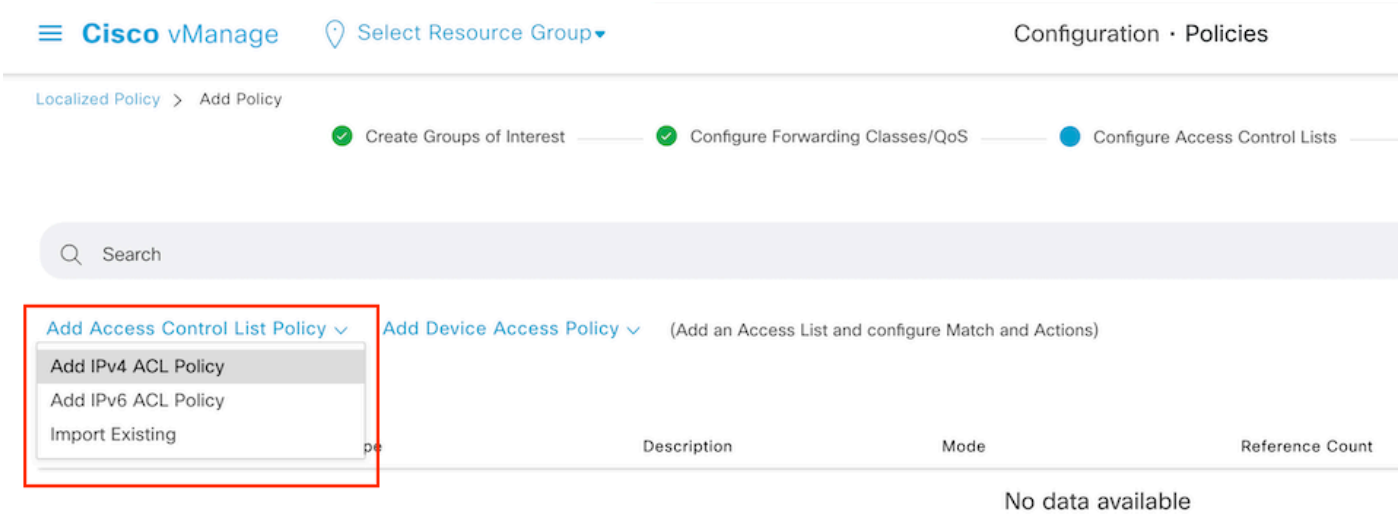
Haga clic **Data Prefix** en el menú de la izquierda y seleccione **New Data Prefix List.**

Dé un nombre a la condición de coincidencia, defina el protocolo de Internet y agregue un prefijo de datos.

Haga clic **Add** y luego **Next** hasta **Configure Access Control List** se muestra.


**Paso 3.** Cree la lista de acceso para aplicar la condición de coincidencia.

Seleccionar **Add IPv4 ACL Policy** desde **Add Access Control List Policy** menú desplegable.

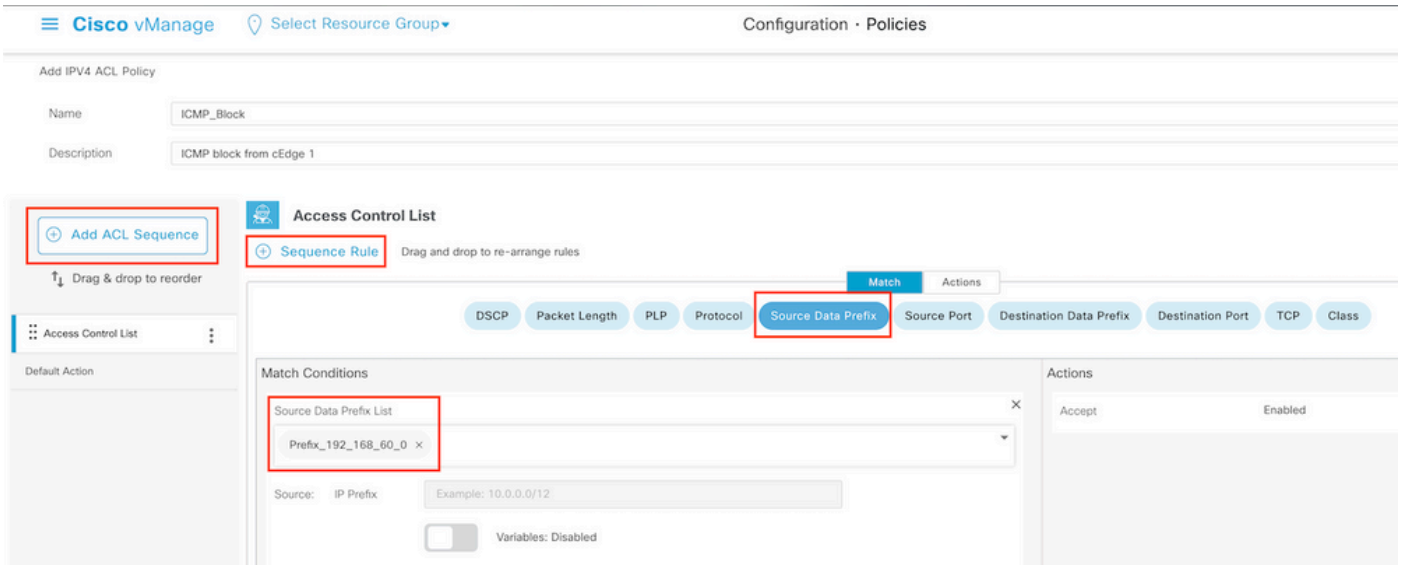



**Nota:** Este documento se basa en la política de la lista de control de acceso y no debe confundirse con una política de acceso del dispositivo. La política de acceso del dispositivo actúa en el plan de control para los servicios locales, como el protocolo simple de administración de red (SNMP) y Secure Socket Shell (SSH), solamente, mientras que la política de la lista de control de acceso es flexible para diferentes servicios y condiciones de coincidencia.

**Paso 4.** Defina la secuencia ACL

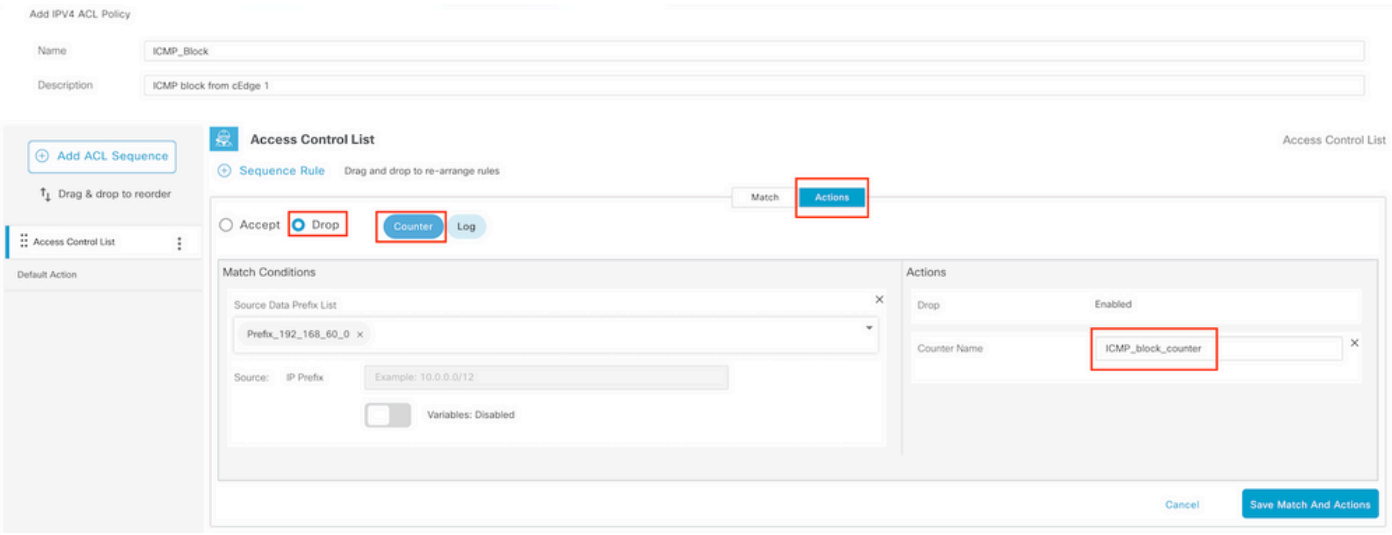
En la pantalla ACL configuration (Configuración de ACL), asigne un nombre a la ACL y proporcione una descripción. Haga clic **Add ACL Sequence** y luego **Sequence Rule.**

En el menú de condiciones de coincidencia, seleccione **Source Data Prefix** y, a continuación, elija la lista de prefijos de datos en el **Source Data Prefix List** menú desplegable.

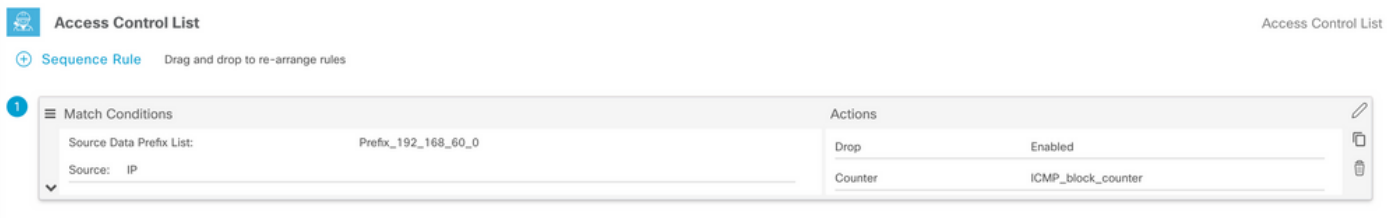



**Paso 5.** Defina la acción para la secuencia y asígnele un nombre

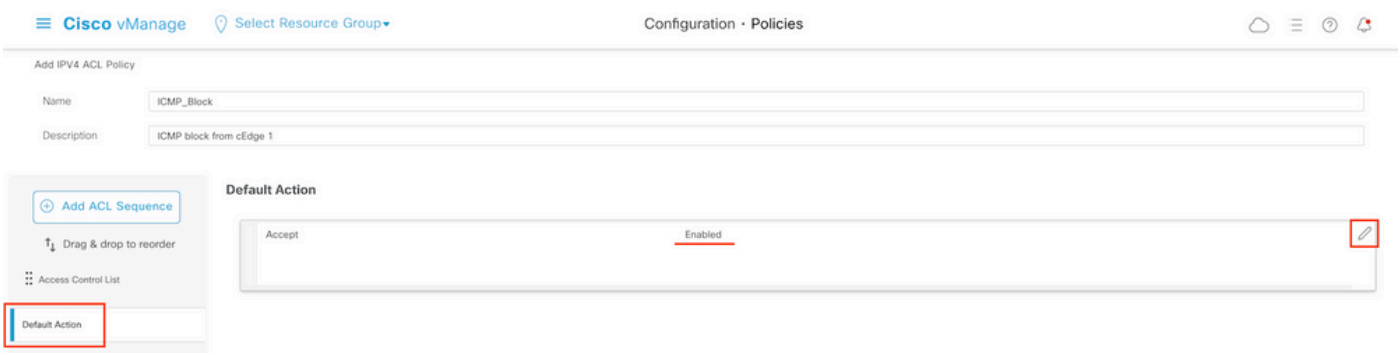
Vaya a **Action** seleccionar **Drop**, y haga clic en **Save Match** y **Actions**.




**Nota:** Esta acción está asociada exclusivamente a la secuencia en sí, no a la política localizada completa.




**Paso 6.** En el menú de la izquierda, seleccione **Default Action** ,clic **Edit,** y elija **Accept**.

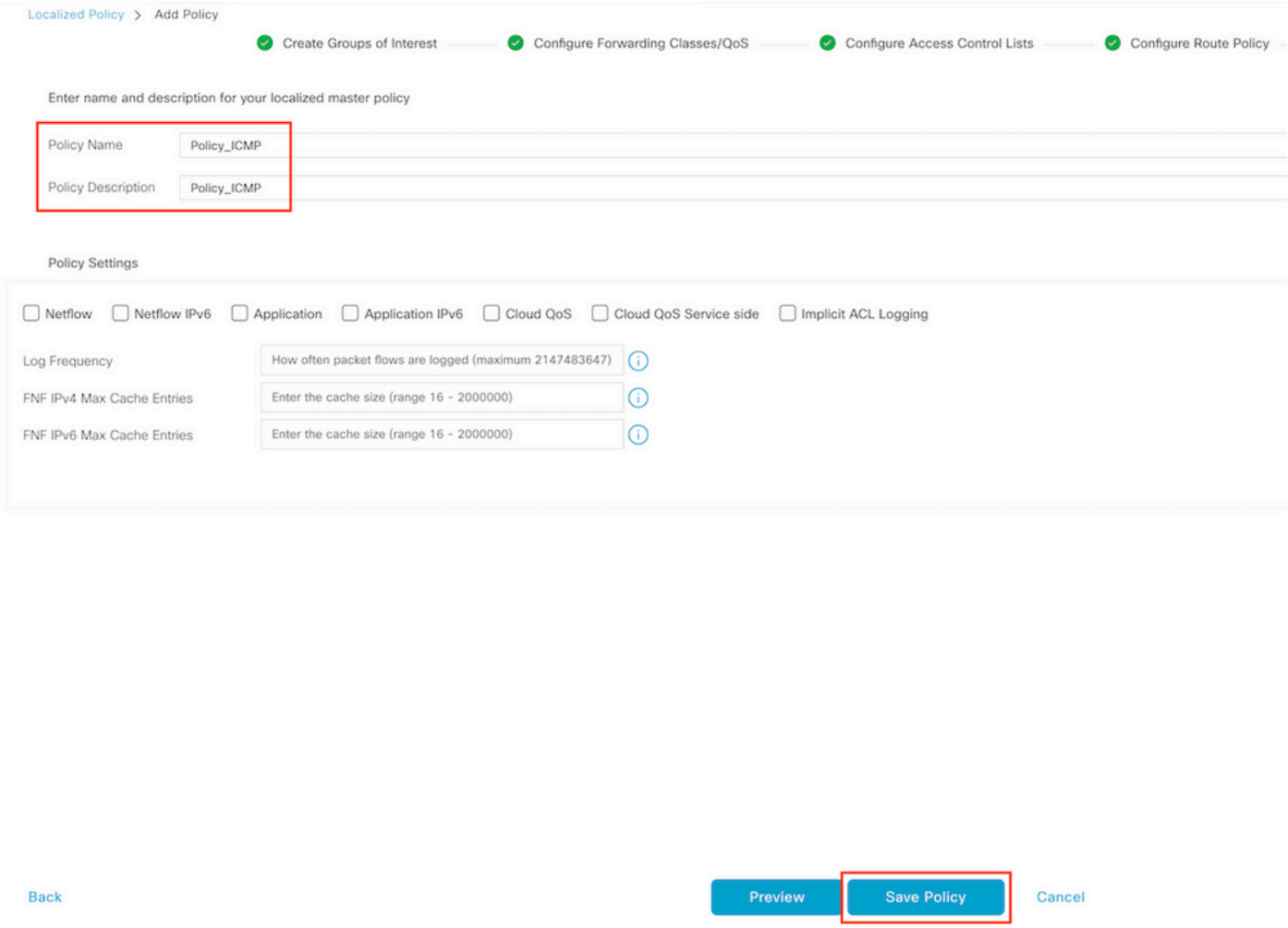



**Nota:** Esta acción predeterminada se encuentra al final de la política localizada. No utilice **drop**, de lo contrario, todo el tráfico puede verse afectado y provocar una interrupción en la red.

Haga clic **Save Access Control List Policy.**

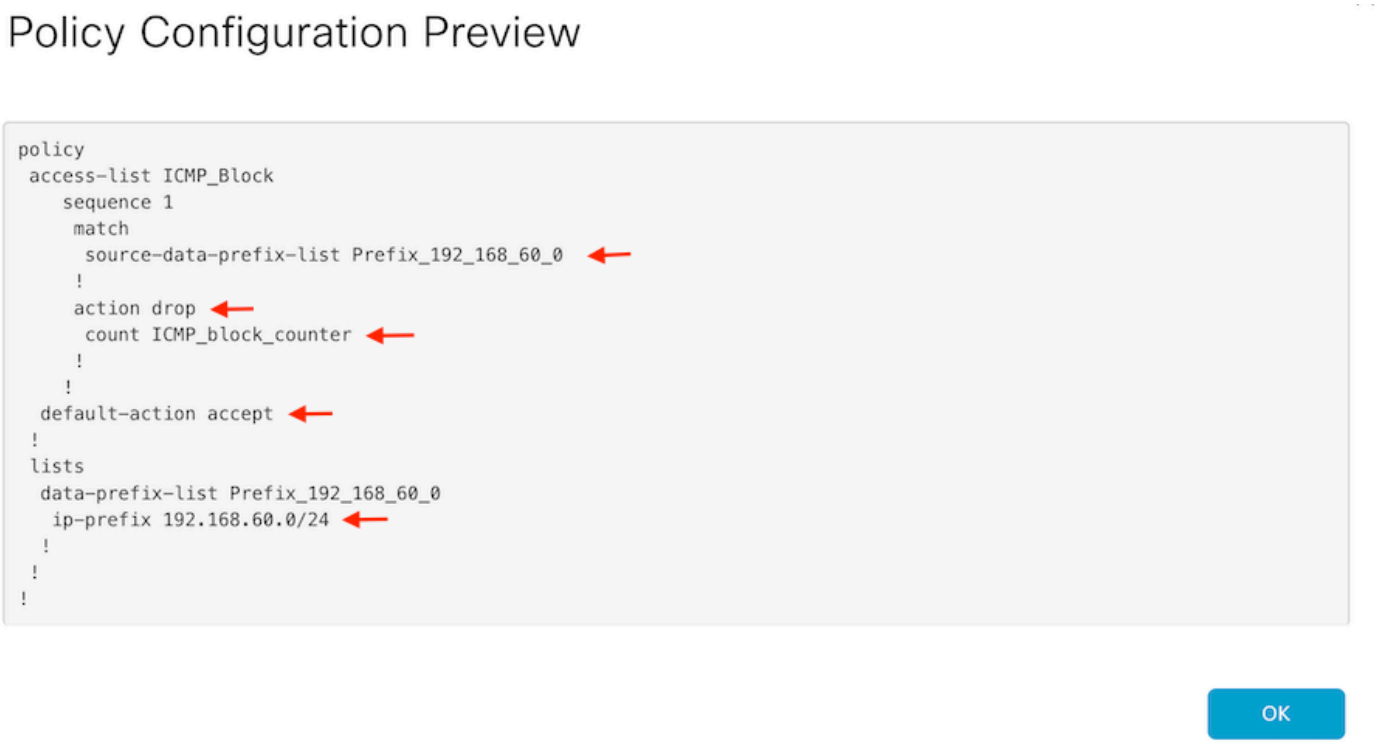

**Paso 7.** Asigne un nombre a la política

Haga clic **Next** hasta **Policy Overview** y ponle nombre. Deje los otros valores en blanco. Haga clic **Save Policy**




Para asegurarse de que la directiva es correcta, haga clic en **Preview**.

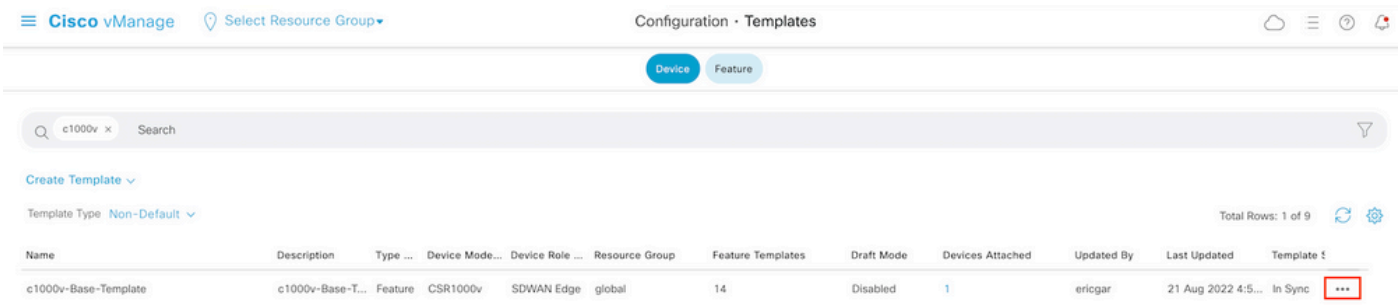

Compruebe que la secuencia y los elementos son correctos en la directiva.



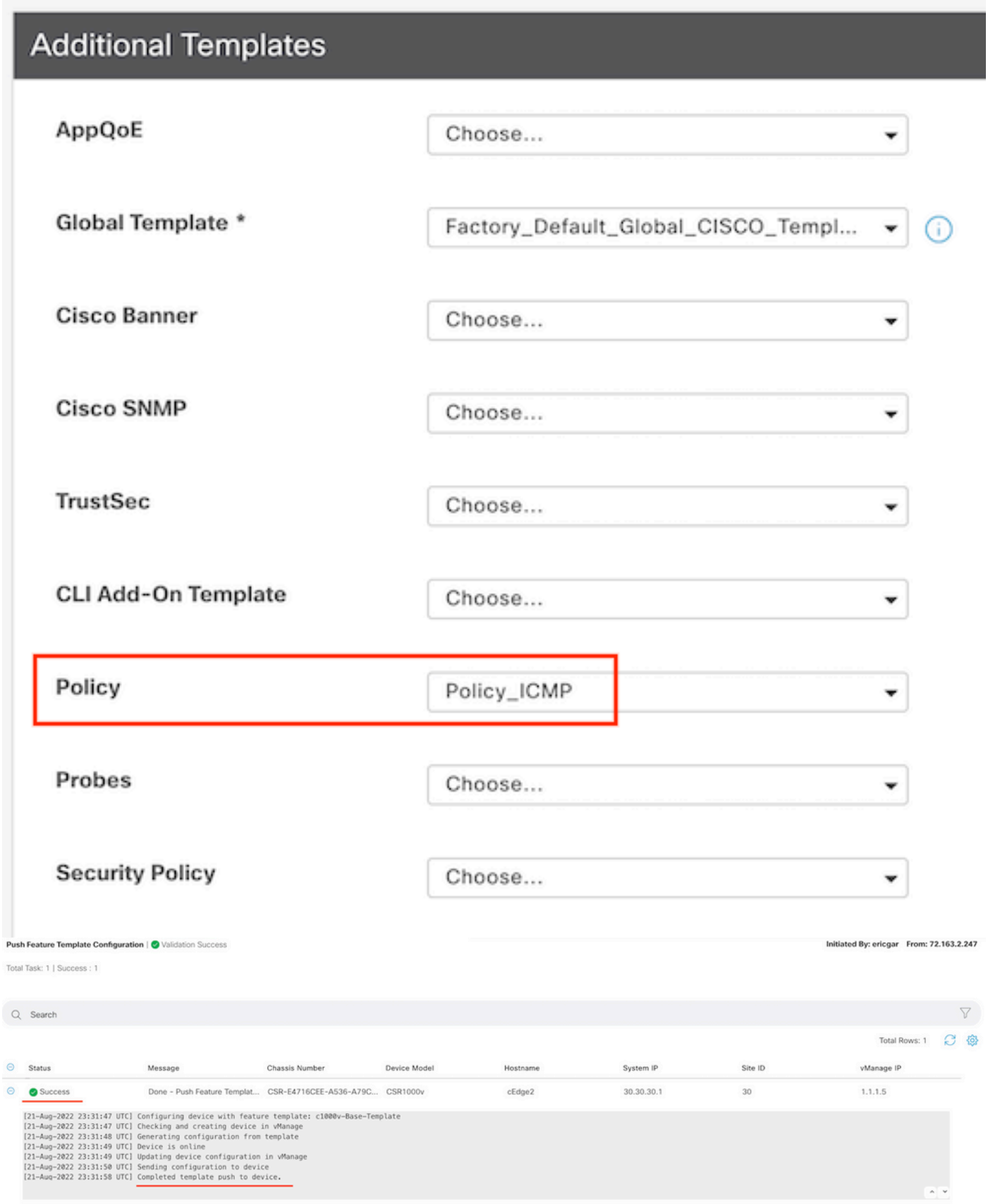

Copie el nombre de ACL. Se requiere en otro paso.

**Paso 8.** Asocie la política localizada con la plantilla de dispositivo.

Busque la plantilla de dispositivo conectada al router, haga clic en los tres puntos y, a continuación, haga clic en **Edit**.




Seleccionar **Additional Templates** y agregue la directiva traducida al campo de directiva y haga clic en **Update > Next > Configure Devices** para enviar la configuración al extremo c.




**Nota:** En este momento, vManage crea la ACL basándose en la política creada y envía los cambios al extremo, aunque no está asociada a ninguna interfaz. Por lo tanto, no tiene ningún efecto en el flujo de tráfico.

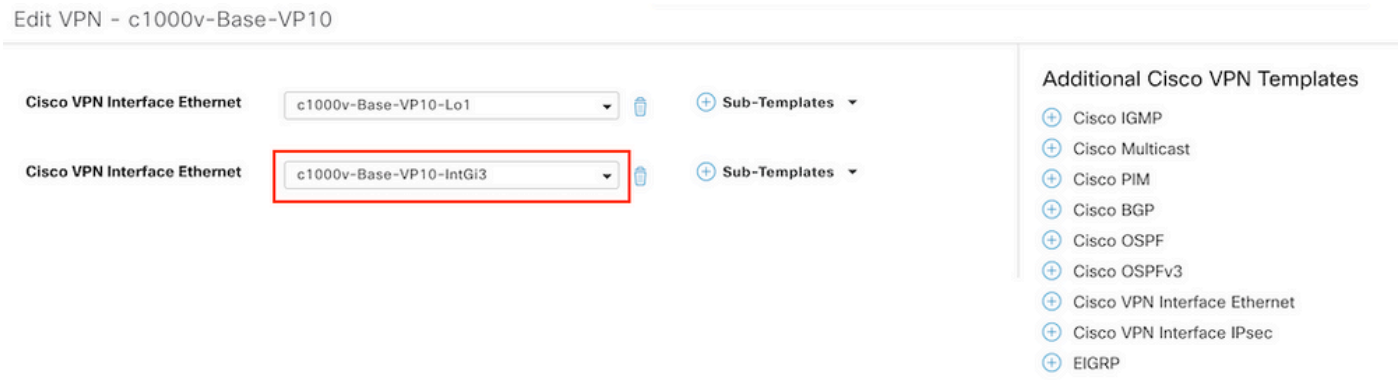
**Paso 9.** Identifique la plantilla de función de la interfaz donde se pretende aplicar la acción al tráfico en la plantilla de dispositivo.

Es importante localizar la plantilla de función en la que debe bloquearse el tráfico.

En este ejemplo, la interfaz GigabitEthernet3 pertenece a la Red privada virtual 3 (Red de reenvío virtual 3).

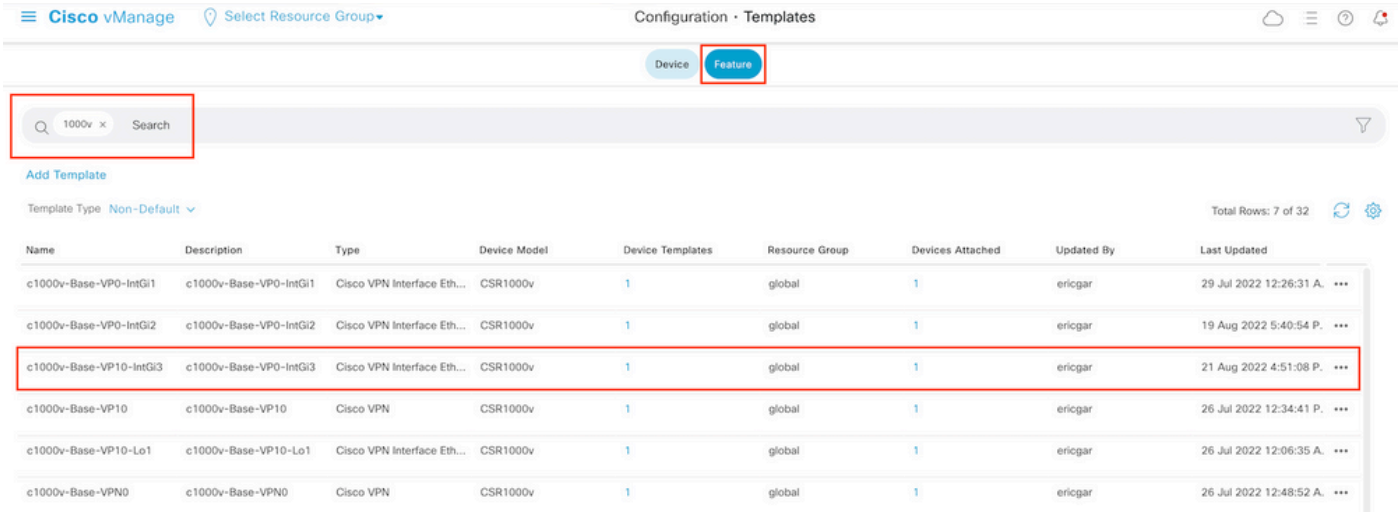
Vaya a la sección VPN de servicio y haga clic en **Edit** para acceder a las plantillas VPN.

En este ejemplo, la interfaz GigabitEthernet3 tiene adjunta la plantilla de función c1000v-Base-VP10-IntGi3.

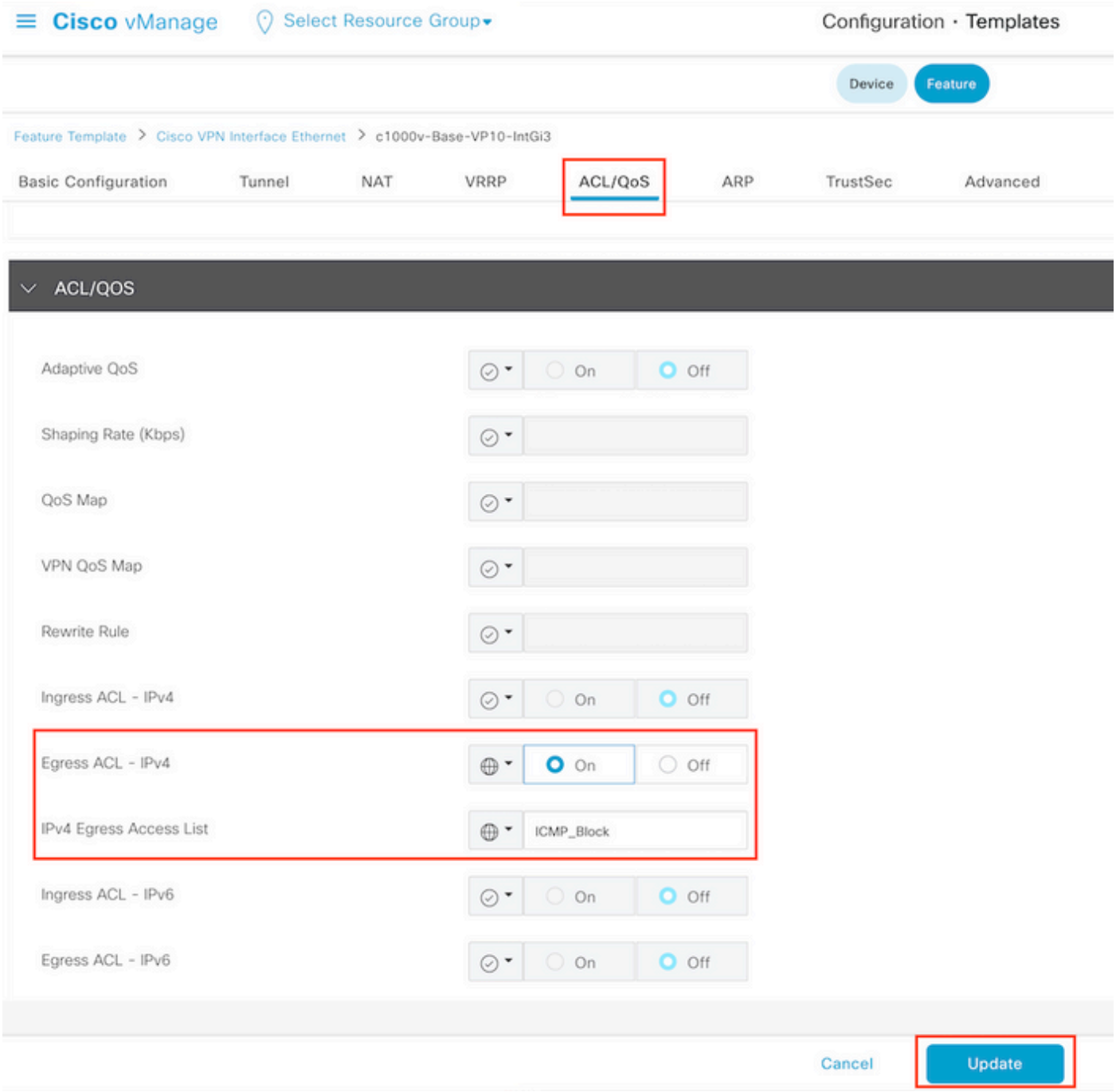



**Paso 10.** Asocie el nombre de ACL con la interfaz.

Vaya a **Configuration > Templates > Feature.** Filtre las plantillas y haga clic en **Edit**




Haga clic **ACL/QoS** y activar la dirección en la que se bloqueará el tráfico. Escriba el nombre de ACL copiado en el paso 7. Haga clic en **Update** y presione los cambios.




**Nota**: Este proceso de creación de políticas adaptadas también funciona para vEdges porque la estructura de políticas de vManage es la misma para ambas arquitecturas. La parte diferente la proporciona la plantilla de dispositivo que crea una estructura de configuración compatible con cEdge o vEdge.

# Verificación

**Paso 1.** Verifique las configuraciones correctamente en el 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
```

**Paso 2.** Desde el Host1 que está en la red de servicio de cEdge1, envíe 5 mensajes ping al servidor en 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:** Para este ejemplo, host1 es una máquina Linux. "-I" representa las interfaces donde el ping sale del router y "-c" representa el número de mensajes ping.

**Paso 3.** En cEdge2, verifique los contadores de 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
```

El contador coincidió con cinco (5) paquetes que vinieron de la red 192.168.60.0/24, como se define en la política.

**Paso 4.** Desde cEdge3, envíe 4 mensajes ping al 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
```

Los paquetes pasaron a través del router al servidor porque la red es diferente (en este caso es 1.1.1.1/32) y no hay ninguna condición coincidente para ello en la política.

**Paso 5**. Verifique nuevamente los contadores de ACL en 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
```

El contador de default_action_count aumentó con los 5 paquetes enviados por cEdge3.

Para borrar contadores, ejecute **clear sdwan policy access-list** comando.

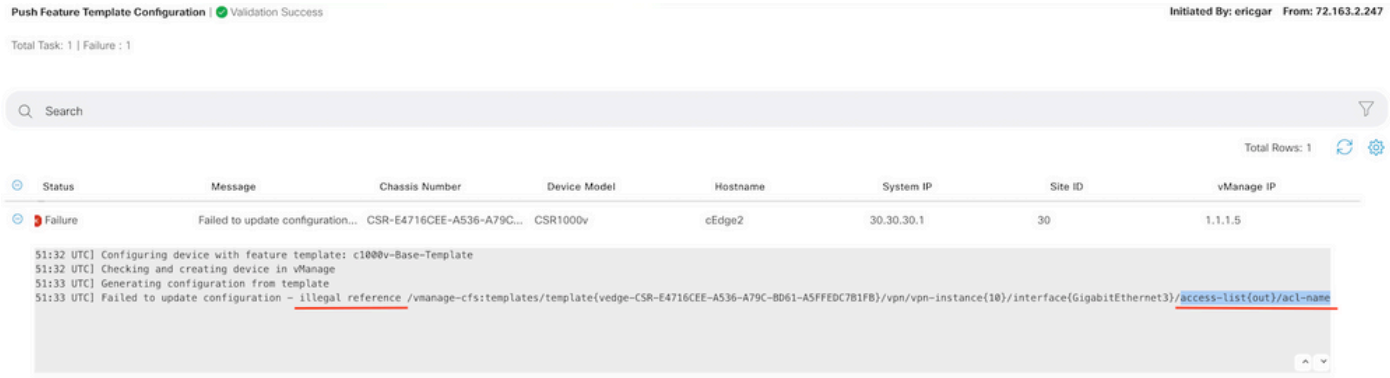
Comandos para la verificación en vEdge

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

# Troubleshoot

**Error:** Referencia no válida al nombre de ACL en la interfaz

La política que contiene la ACL debe asociarse primero a la plantilla de dispositivo. Después de esto, el nombre de ACL se puede especificar en la plantilla de dispositivo de función de la interfaz.




# Información Relacionada

- Guía de Configuración de Políticas de Cisco SD-WAN, Cisco IOS XE Release 17.x
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).