Configuración del router de extremo SD-WAN para restringir el acceso SSH

Contenido

Introducción

Este documento describe el proceso para restringir la conexión de Secure Shell (SSH) al router SD-WAN Cisco IOS-XE®.

Prerequisites

Requirements

Se requiere controlar la conexión entre vManage y cEdge para realizar las pruebas adecuadas.

Componentes Utilizados

Este procedimiento no se limita a ninguna versión de software de los dispositivos Cisco Edge o vManage, por lo que todas las versiones se pueden utilizar para seguir estos pasos. Sin embargo, este documento es exclusivo para los routers cEdge. Para realizar la configuración, es necesario:

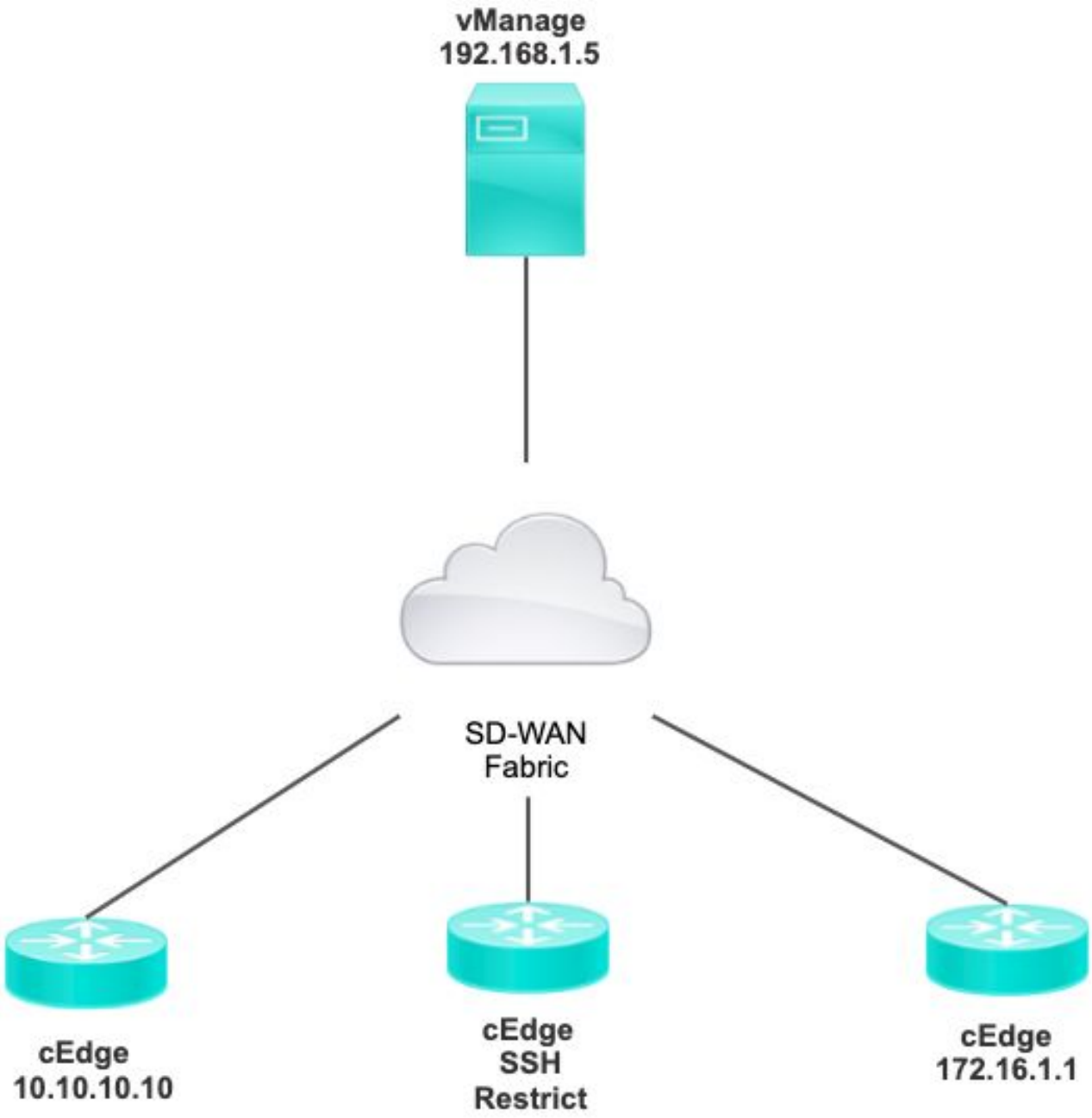
- Router Cisco Edge (virtual o físico)
- Cisco vManage

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El propósito de esta demostración es mostrar la configuración en cEdge para restringir el acceso SSH desde cEdge 172.16.1.1 pero permitir cEdge 10.10.10.10 y vManage.

Topología



Restringir Procedimiento de Acceso SSH

Verificación de conectividad

Es necesaria la verificación de la conectividad para validar que el router cEdge puede alcanzar

vManage. De forma predeterminada, vManage utiliza IP 192.168.1.5 para iniciar sesión en los dispositivos cEdge.

En la GUI de vManage, abra SSH en cEdge y asegúrese de que la IP que estaba conectada tenga el siguiente resultado:

```
cEdge#show
users

Line       User       Host(s)              Idle
Location
*866 vty 0 admin      idle             00:00:00
192.168.1.5
Interface  User         Mode         Idle     Peer Address
```

Asegúrese de que vManage no utiliza el túnel, sistema o dirección IP pública para iniciar sesión en cEdge.

Para confirmar la IP que se utiliza para iniciar sesión en cEdge, puede utilizar la siguiente lista de acceso.

```
cEdge#show run  | section access
ip access-list extended VTY_FILTER_SHH
5 permit ip any any log                <<<< with this sequence you can verify the IP of the
device that tried to access.
```

Validación de lista de control de acceso

Lista de acceso aplicada en la línea VTY

```
cEdge#show sdwan running-config | section vty
line vty 0 4
access-class VTY_FILTER_SSH in vrf-also
transport input ssh
```

Después de aplicar la ACL, puede volver a abrir SSH desde vManage a cEdge y ver el siguiente mensaje generado en los registros.

Este mensaje se puede ver con el comando: **show logging**.

```
*Jul 13 15:05:47.781: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Tadmin] [Source:
192.168.1.5] [localport: 22] at 15:05:47 UTC Tue Jul 13 2022
```

En el registro anterior, puede ver el puerto local 22. Significa que 192.168.1.5 intentó abrir SSH a cEdge.

Ahora que ha confirmado que la IP de origen es 192.168.1.5, puede configurar la ACL con la IP correcta para permitir que vManage pueda abrir la sesión SSH.

Configuración de Lista de Control de Acceso

Si cEdge tiene varias secuencias, asegúrese de agregar la nueva secuencia en la parte superior de ACL.

Antes:

```
cEdge#show access-list VTY_FILTER_SSH
Extended IP access list VTY_FILTER_SSH
10 permit tcp 10.10.10.10 0.0.0.15 any eq 22 100 deny   ip any any log
```

Ejemplo de configuración:

```
cEdge#config-transaction
cEdgeconfig)# ip access-list
cEdge(config)# ip access-list extended VTY_FILTER_SSH
cEdge(config-ext-nacl)# 5 permit ip host 192.168.1.5 any log
cEdgeconfig-ext-nacl)# commit
Commit complete.
```

Nueva secuencia:

```
cEdge#show access-list VTY_FILTER_SSH
Extended IP access list VTY_FILTER_SSH
5 permit ip host 192.168.1.5 any log   <<<< New sequence to allow vManage to SSH 10 permit
tcp 10.10.10.10 0.0.0.15 any eq 22  100 deny   ip any any log   <<<< This sequence deny all
other SSH connections
```

Aplique ACL en la línea VTY.

```
cEdge#show sdwan running-config | section vty
line vty 0 4    access-class VTY_FILTER_SSH in vrf-also  transport input ssh
!
                                          line vty 5 80
                                            access-class VTY_FILTER_SSH in vrf-also transport
input ssh
```

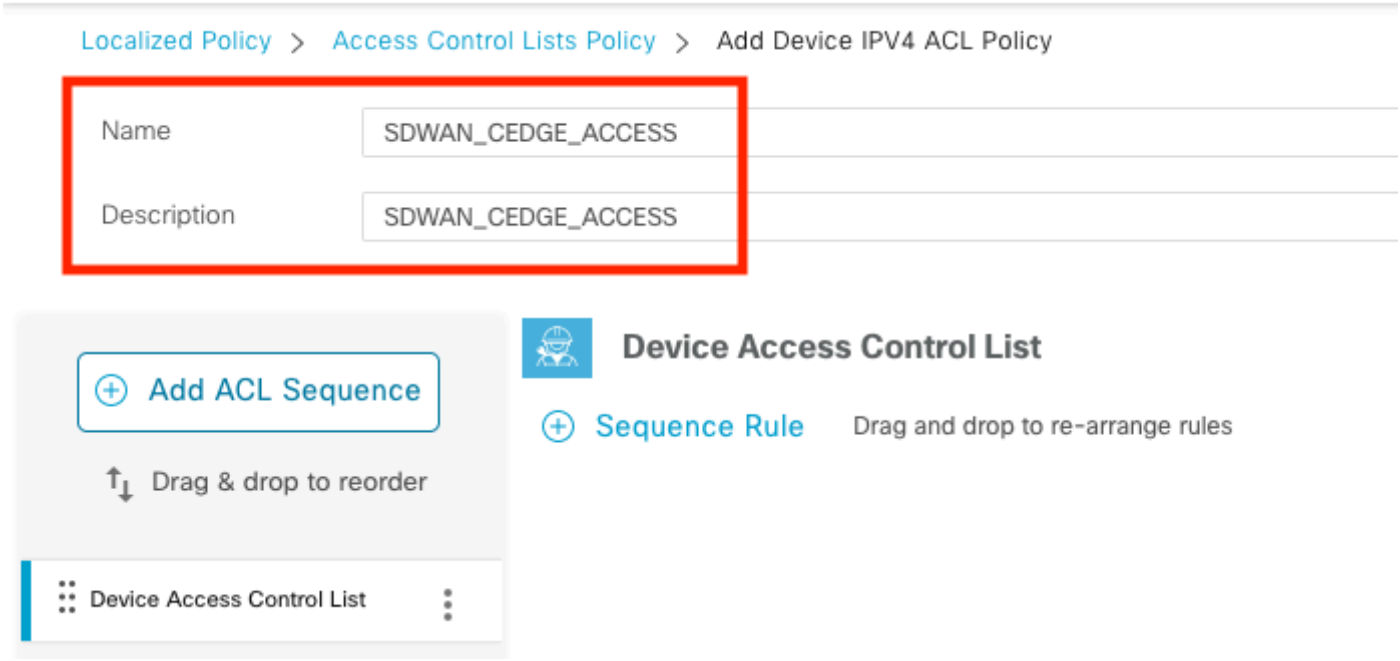
Configuración en la GUI de vManage

Si el dispositivo cEdge tiene una plantilla conectada, puede utilizar el siguiente procedimiento.

Paso 1. Cree una ACL

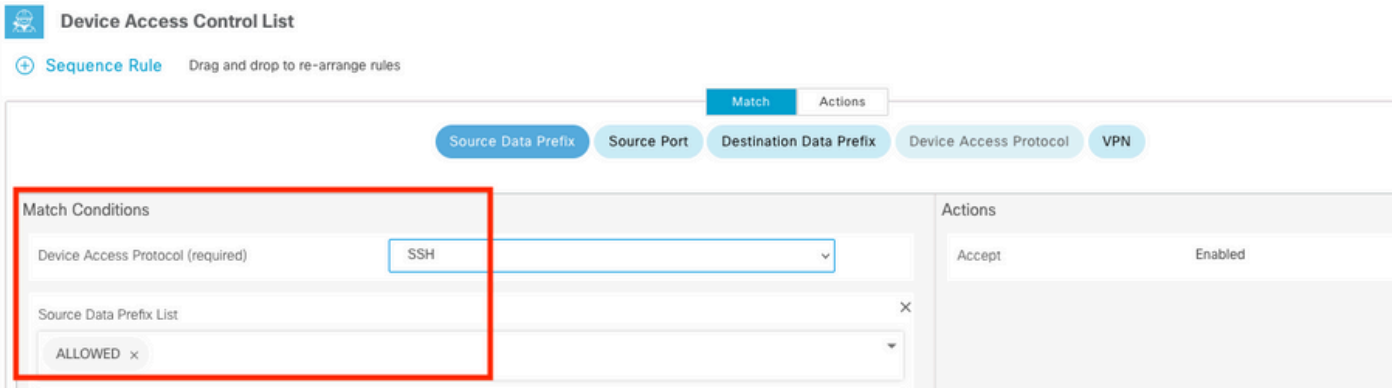
Vaya a **Configuración > Opciones personalizadas > Lista de control de acceso > Agregar política de acceso de dispositivo > Agregar política de acceso de dispositivo ipv4**

Agregue el nombre y la descripción de la ACL y haga clic en **Add ACL Sequence** y luego seleccione **Sequence Rule**



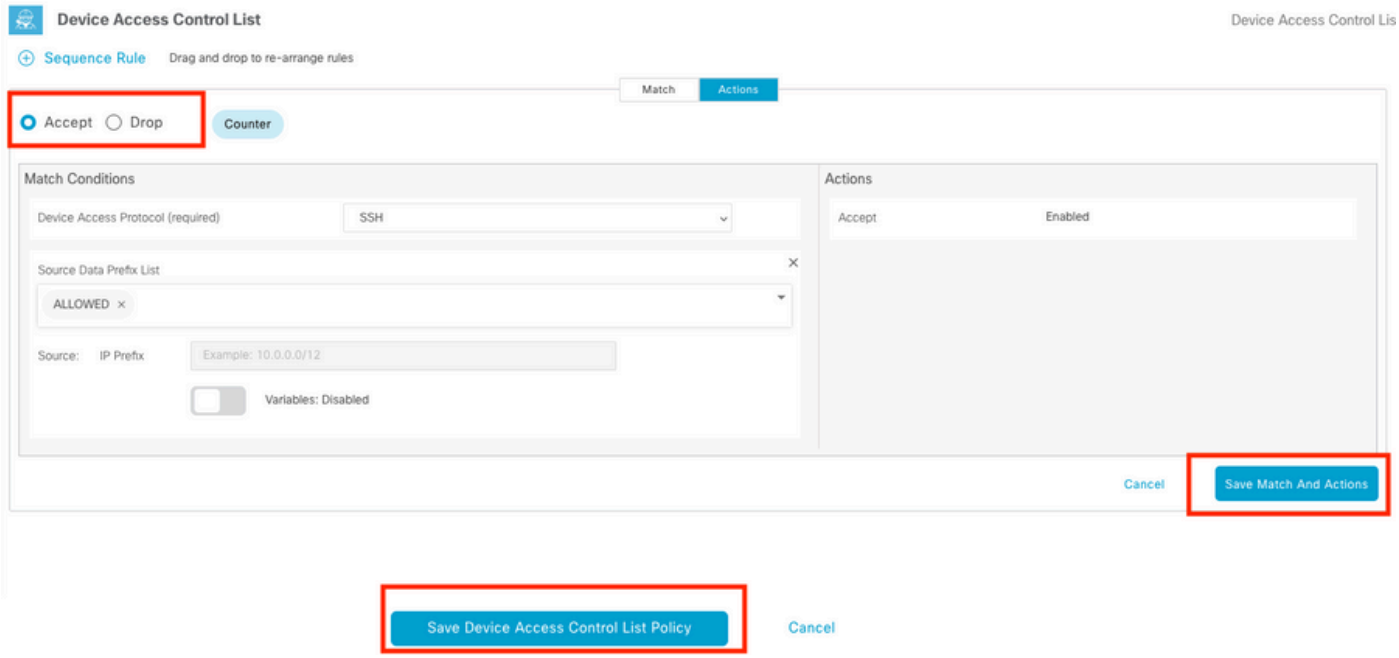
Seleccione **Device Access Protocol >SSH**

A continuación, seleccione la **Lista de prefijos de datos de** origen.



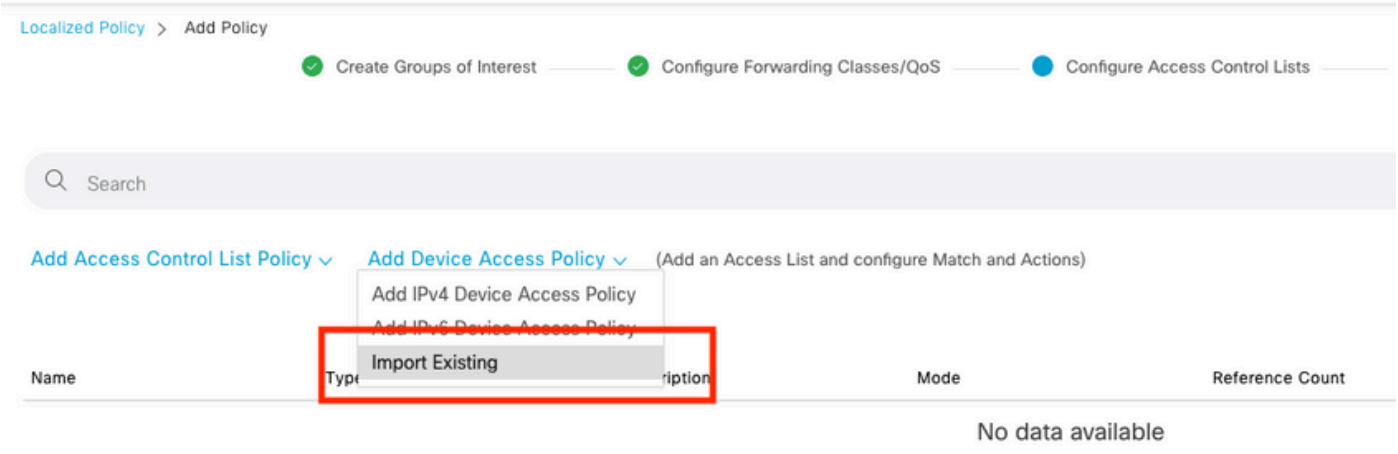
Haga clic en **Acciones**, seleccione **Aceptar**, y luego haga clic en Save Match And Actions.

Por último, puede seleccionar Save Device Access Control List Policy.

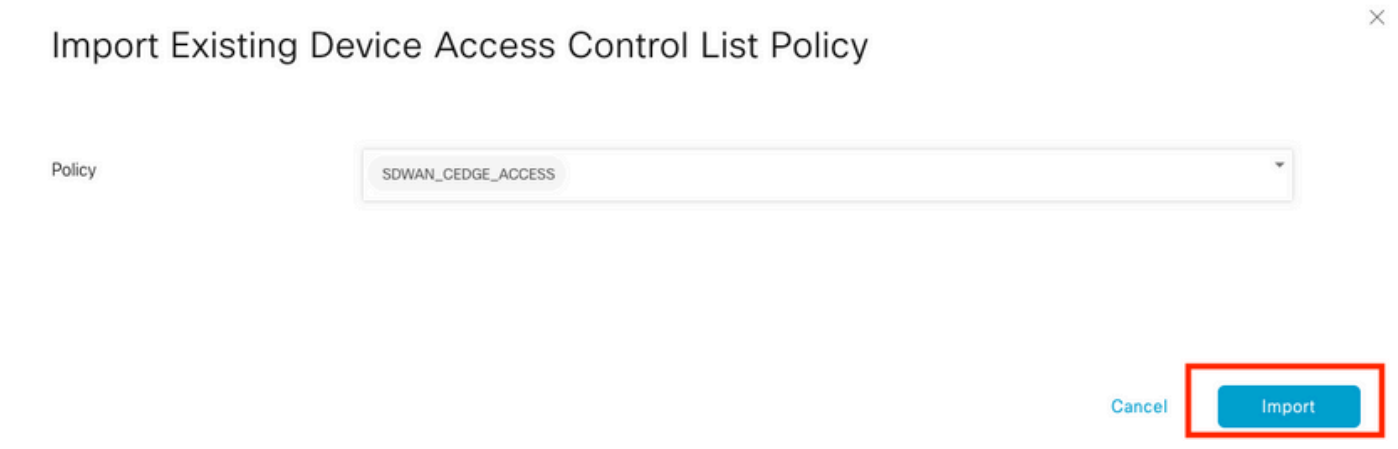


Paso 2. Crear política localizada

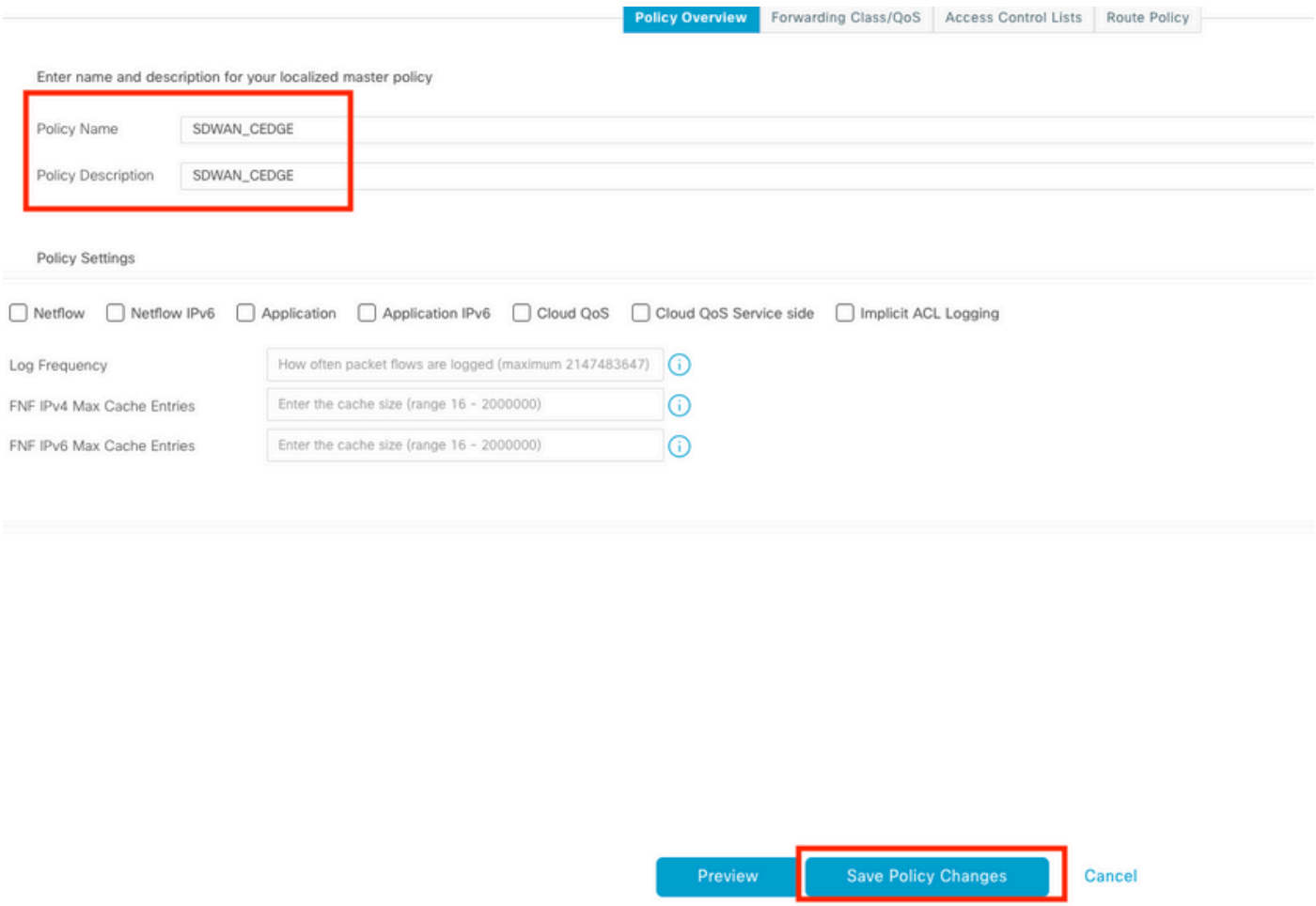
Vaya a **Configuration > Localized Policy > Add Policy > Configure Access Control List > Add Device Access Policy > Import Existing**.



Seleccione la **ACL** anterior y haga clic en **Importar**.

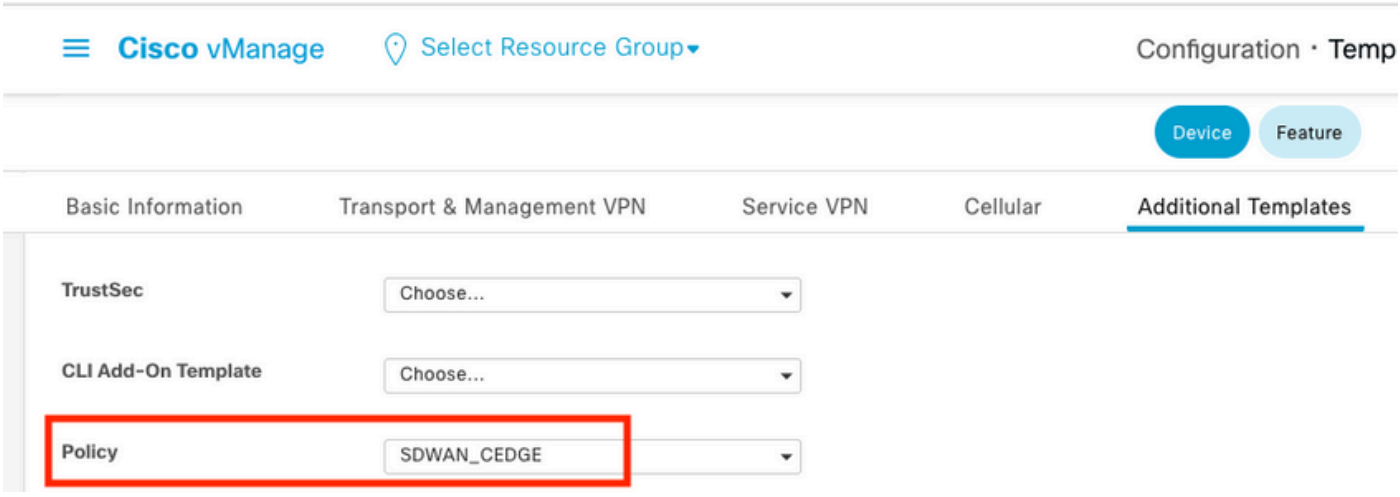


Agregue el nombre y la descripción de la directiva y haga clic en Save Policy Changes.



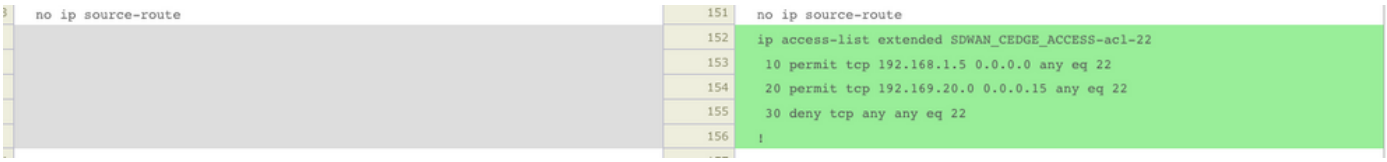
Paso 3. Adjuntar la política localizada a la plantilla del dispositivo

Vaya a **Configuration > Template > Device > Select the Device y haga clic en > ... > Edit > Additional Templates > Policy > SDWAN_CEDGE > Update**.



Antes de insertar la plantilla, puede verificar la diferencia de configuración.

Nueva configuración de ACL



ACL aplicada a la línea vty

```
236 !
237 line vty 0 4
238  transport input ssh
239 !
240 line vty 5 80
241  transport input ssh
```

```
217 !
218 line vty 0 4
219  access-class SDWAN_CEDGE_ACCESS-acl-22 in vrf-also
220  transport input ssh
221 !
222 line vty 5 80
223  access-class SDWAN_CEDGE_ACCESS-acl-22 in vrf-also
224  transport input ssh
```

Verificación

Ahora puede volver a probar el acceso SSH a cEdge con filtros anteriores de vManage con esta ruta: **Menu > Tools > SSH Terminal**.

El router intentó establecer SSH en 192.168.10.114m

```
Router#ssh 192.168.10.114
% Connection refused by remote host

Router#
```

Si verifica los contadores de ACL, puede confirmar que la Seq 30 tiene 1 coincidencia y que se denegó la conexión SSH.

```
c8000v-1#   sh access-lists
Extended IP access list SDWAN_CEDGE_ACCESS-acl-22
    10 permit tcp host 192.168.1.5 any eq 22
    20 permit tcp 192.169.20.0 0.0.0.15 any eq 22
    30 deny tcp any any eq 22 (1 match)
```

Información Relacionada

[Guía de Configuración de Políticas de Cisco SD-WAN, Cisco IOS XE Release 17.x]

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).