配置SD-WAN cEdge路由器以限制SSH访问

目录

简介

本文档介绍限制与Cisco IOS-XE® SD-WAN路由器的安全外壳(SSH)连接的过程。

先决条件

要求

需要控制vManage和cEdge之间的连接，才能进行正确的测试。

使用的组件

此过程不限于Cisco Edge或vManage设备中的任何软件版本，因此所有版本都可用于执行这些步骤。但是，本文档仅适用于cEdge路由器。要进行配置，需要执行以下操作：

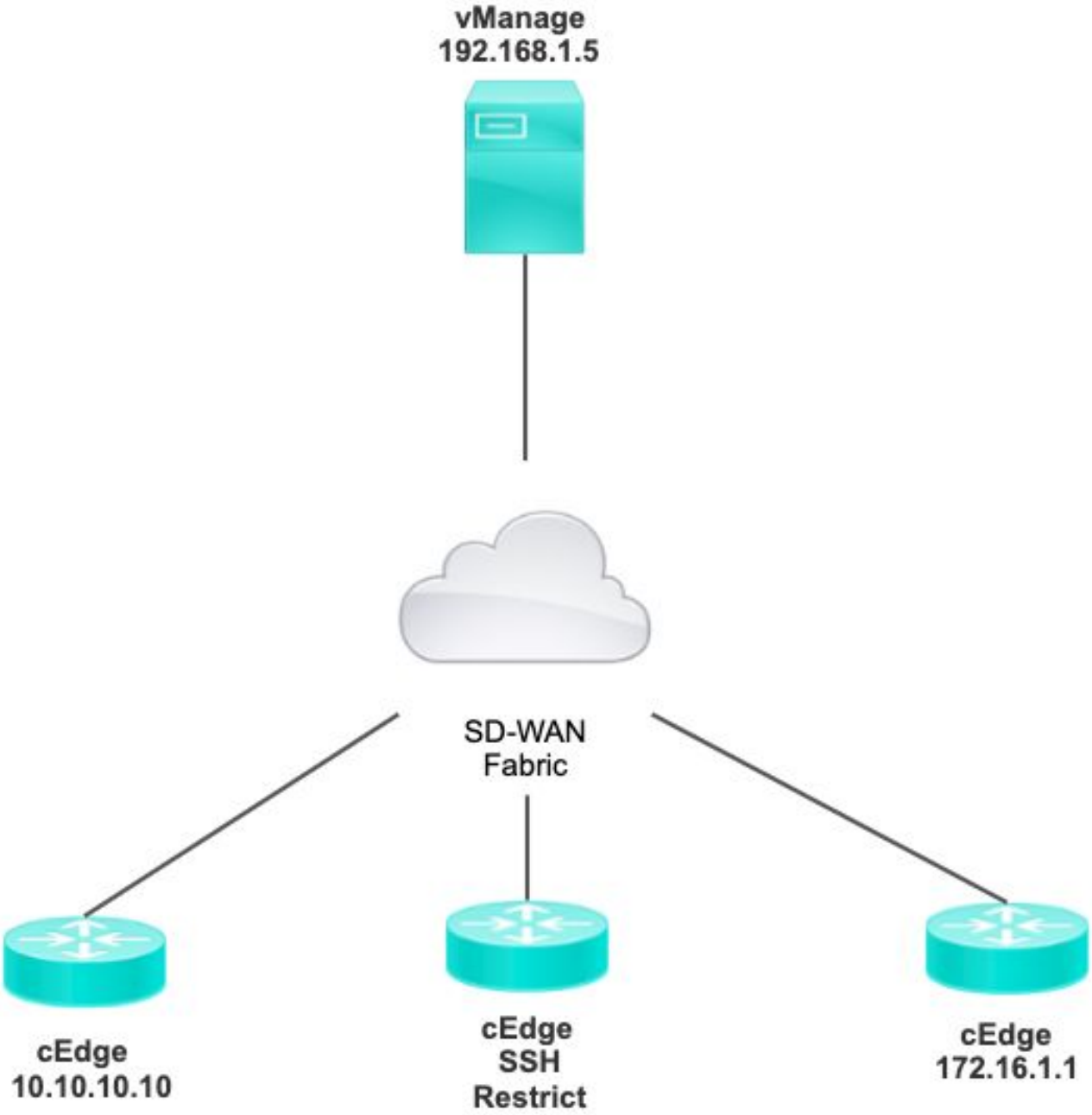
- Cisco cEdge路由器（虚拟或物理）
- Cisco vManage

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。

背景信息

本演示的目的是显示cEdge上的配置，以限制从cEdge 172.16.1.1进行SSH访问，但允许cEdge 10.10.10.10和vManage。

拓扑



限制SSH访问过程

连接验证

需要验证连接，以验证cEdge路由器可以访问vManage。 默认情况下，vManage使用IP 192.168.1.5登录到cEdge设备。

在vManage GUI中，打开SSH到cEdge，并确保连接的IP具有下一个输出：

```
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
```

确保vManage不使用隧道、系统或公共ip地址登录cEdge。

要确认用于登录cEdge的IP，您可以使用下一个访问列表。

```
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.
```

访问控制列表验证

在VTY线路上应用的访问列表

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

应用ACL后，您可以从vManage再次打开SSH到cEdge，并查看日志中生成的下一条消息。

此消息可以通过命令show logging看到。

```
*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
```

在上一个日志中，您可以看到本地端口22。这意味着192.168.1.5尝试打开到cEdge的SSH。

现在您已确认源IP为192.168.1.5，您可以使用正确的IP配置ACL，以允许vManage能够打开SSH会话。

访问控制列表配置

如果cEdge具有多个序列，请确保在ACL的顶部添加新序列。

攻击前：

```
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
```

配置示例：

```
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.
```

新序列：

```
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
```

在VTY线路上应用ACL。

```
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
```

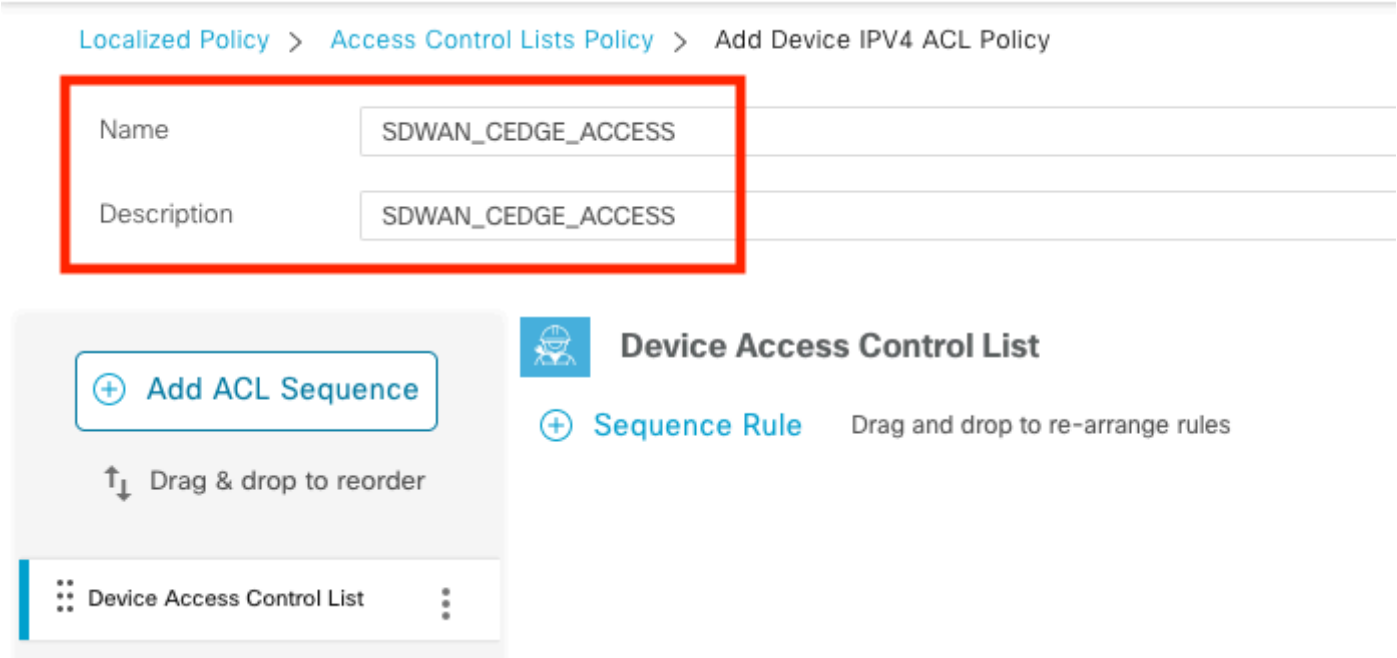
vManage GUI上的配置

如果cEdge设备连接了模板，则可以使用下一过程。

步骤1:创建ACL

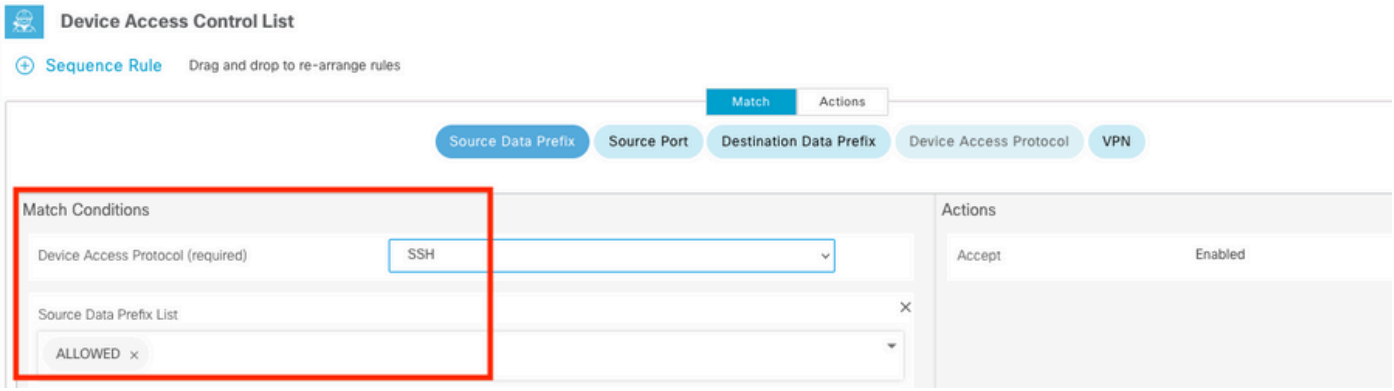
导航到**配置>自定义选项>访问控制列表>添加设备访问策略>添加ipv4设备访问策略**

添加ACL的名称和说明，然后点击**添加ACL序列**，然后选择**序列规则**



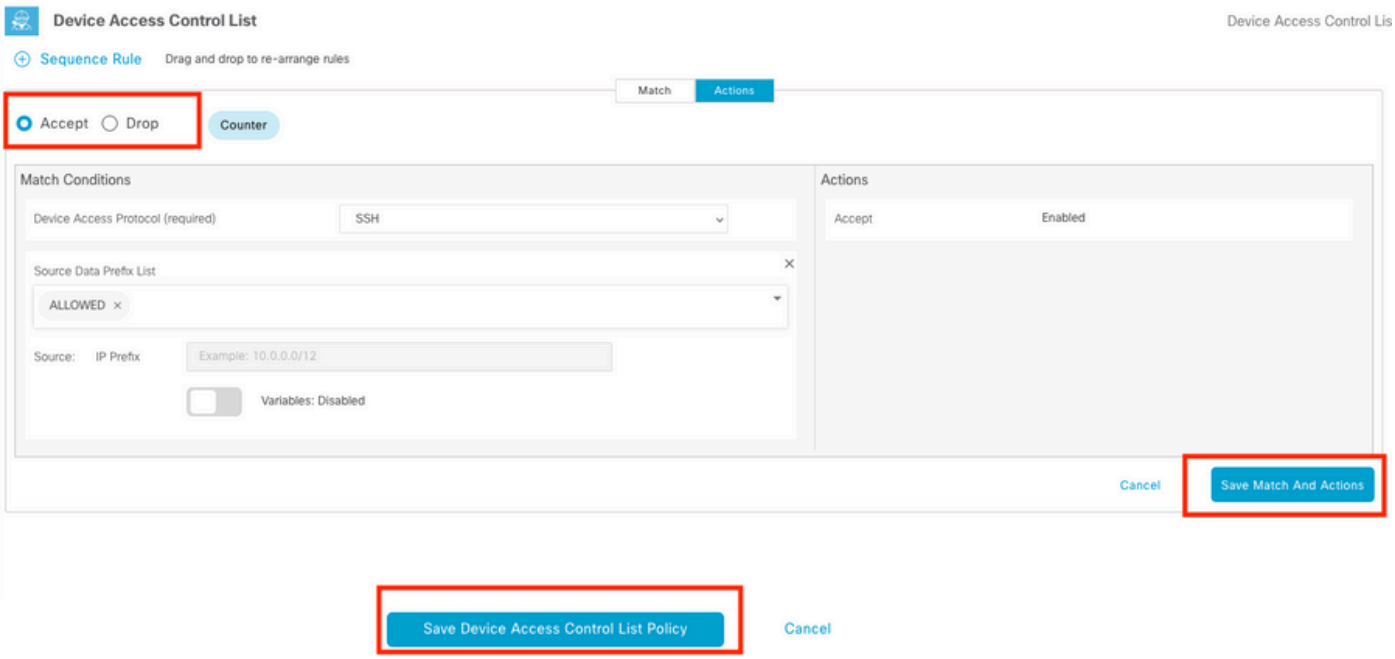
选择Device Access Protocol >SSH

然后选择源数据**前缀列表**。



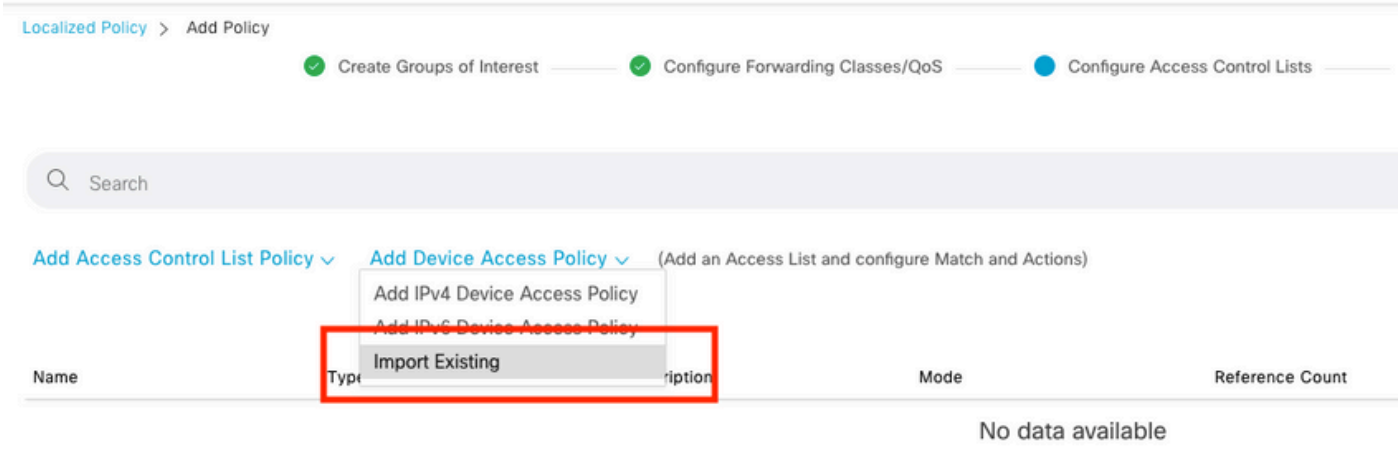
单击**操作**，选择**接受**，然后单击 Save Match And Actions.

最后，您可以选择 Save Device Access Control List Policy.

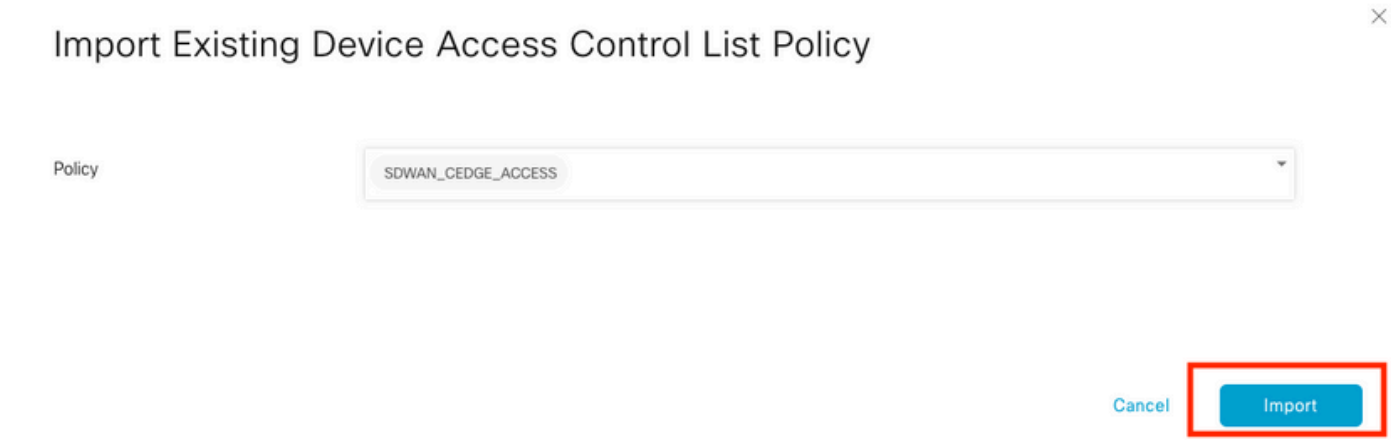


第二步：创建本地化策略

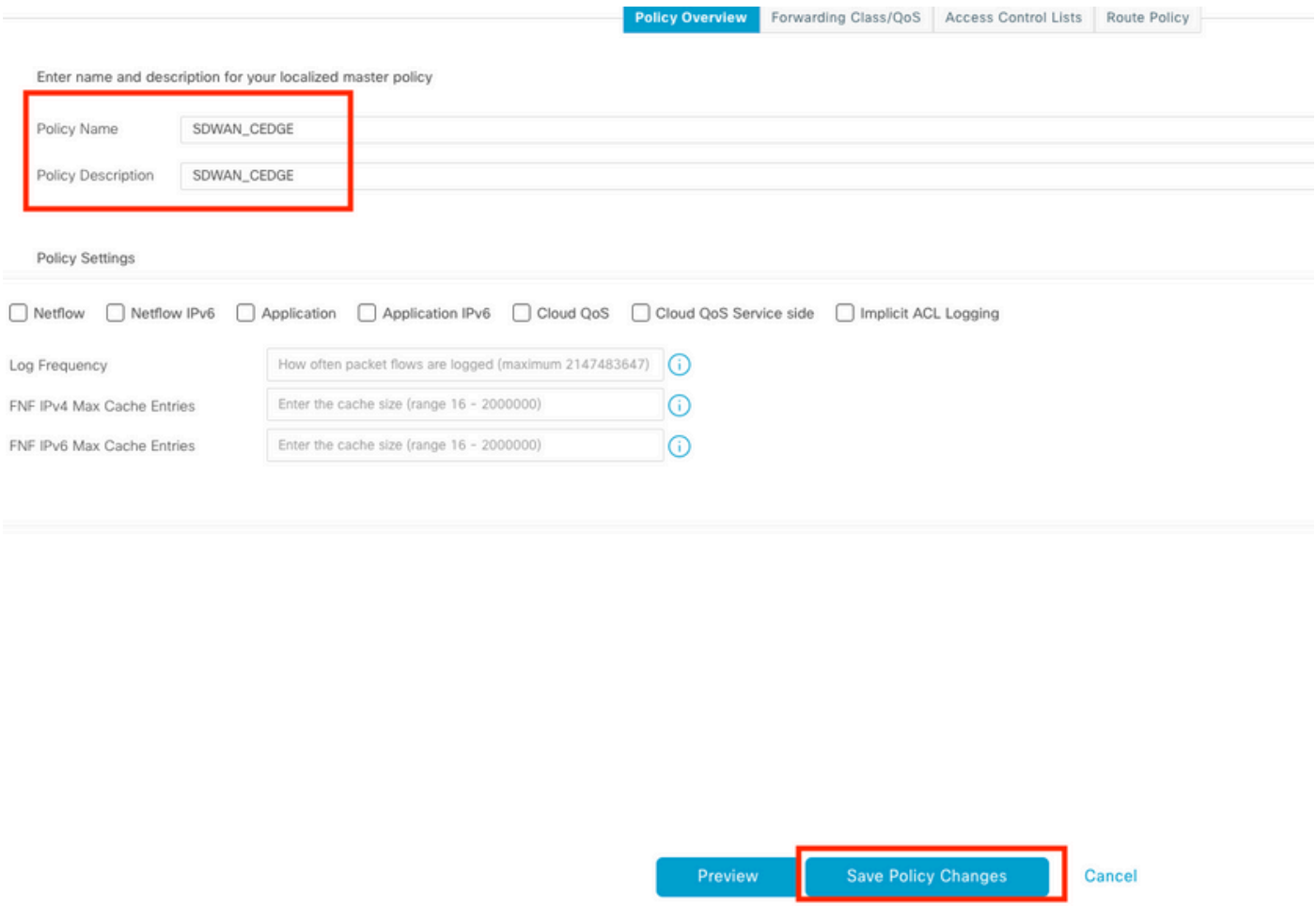
导航到**Configuration > Localized Policy > Add Policy > Configure Access Control List > Add Device Access Policy > Import Existing**。



选择上一个**ACL**，然后单击**Import**。

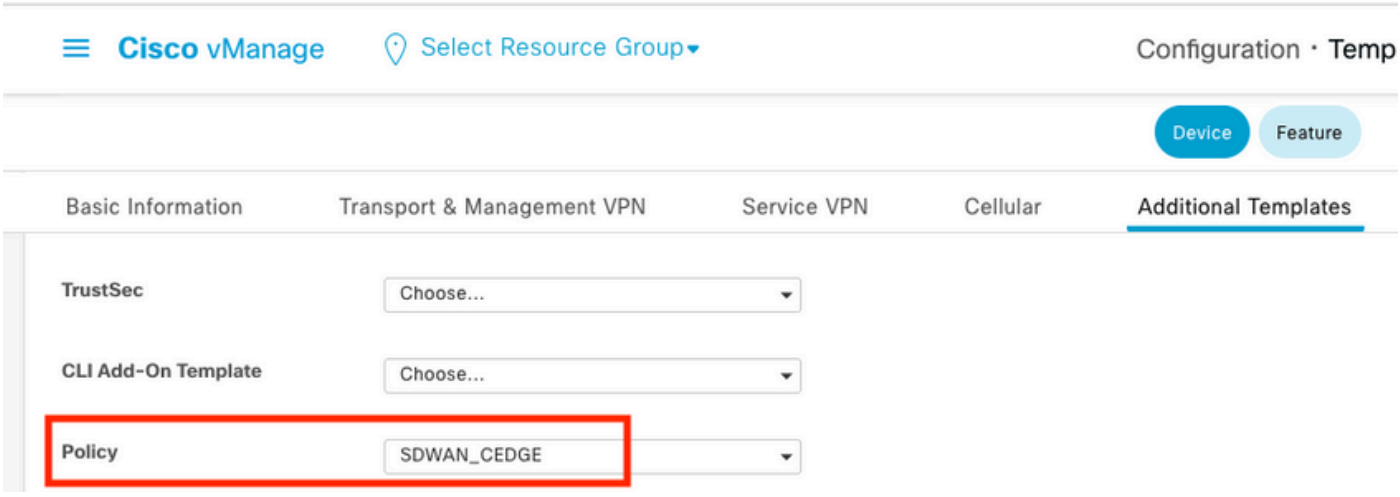


添加Policy Name和Policy Description，然后单击 Save Policy Changes.



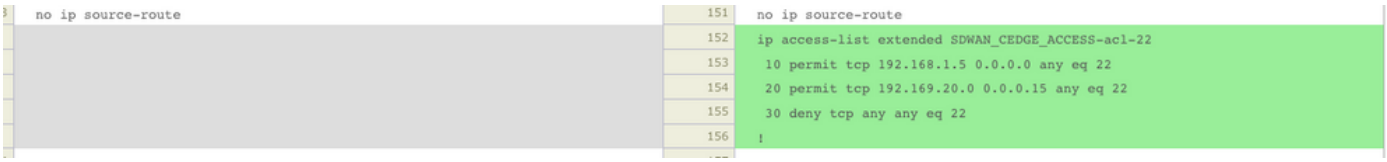
第三步：将本地化策略附加到设备模板

导航到Configuration > Template > Device > Select the Device并单击> ... > Edit > Additional Templates > Policy > SDWAN_CEDGE > Update。



在推送模板之前，您可以验证配置差异。

新的ACL配置



应用于线路vty的ACL

```
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
```

确认

现在，您可以使用此路径**Menu > Tools > SSH Terminal**再次使用之前的vManage过滤器测试对cEdge的SSH访问。

路由器尝试通过SSH连接到192.168.10.114m

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

Router#
```

如果检查ACL计数器，您可以确认序列30有1个匹配项，并且SSH连接被拒绝。

```
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)
```

相关信息

[Cisco SD-WAN策略配置指南，Cisco IOS XE版本17.x]

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）。