# SSHアクセスを制限するためのSD-WANエッジルータの設定

## 内容



## 概要

このドキュメントでは、Cisco IOS-XE® SD-WANルータへのセキュアシェル(SSH)接続を制限するプロセスについて説明します。

## 前提条件

### 要件

適切なテストを行うには、vManageとcEdge間のコントロール接続が必要です。

### 使用するコンポーネント

この手順は、Cisco EdgeまたはvManageデバイスのソフトウェアリリースに限定されるものではないため、これらの手順では、すべてのリリースを使用できます。ただし、このドキュメントはcEdgeルータ専用です。設定するには、次のものが必要です。

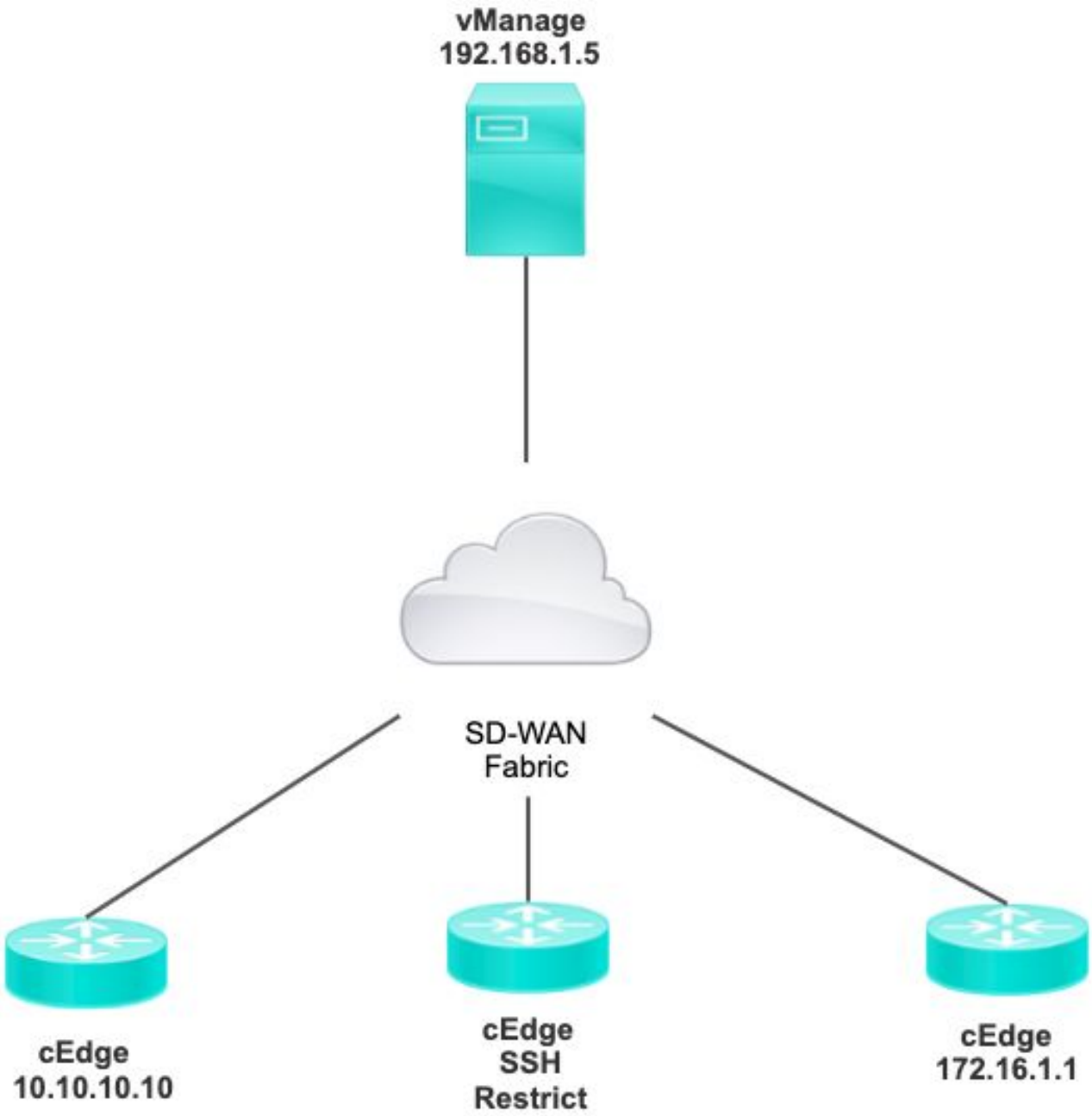
- Cisco cEdgeルータ（仮想または物理）
- Cisco vManage

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### 背景説明

このデモンストレーションの目的は、cEdge 172.16.1.1からのSSHアクセスを制限し、cEdge 10.10.10.10およびvManageを許可するcEdgeの設定を示すことです。

## トポロジ




## SSHアクセスの制限手順

### 接続の検証

cEdgeルータがvManageに到達できることを検証するには、接続の確認が必要です。 デフォルト

では、vManageはIP 192.168.1.5を使用してcEdgeデバイスにログインします。

vManage GUIで、SSHからcEdgeを開き、接続されたIPに次の出力があることを確認します。

```
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
```

vManageがトンネル、システム、またはパブリックIPアドレスを使用してcEdgeにログインしていないことを確認します。

cEdgeへのログインに使用するIPを確認するには、次のアクセスリストを使用します。

```
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.
```

## アクセスコントロールリストの検証

VTY回線に適用されるアクセスリスト

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

ACLが適用された後、vManageからcEdgeにSSHを再び開き、ログに次のメッセージが生成されるのを確認できます。

このメッセージは、**show logging**コマンドで表示できます。

```
*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
```

前のログでは、ローカルポート22を確認できます。これは、192.168.1.5がcEdgeへのSSHを開こうとしたことを意味します。

送信元IPが192.168.1.5であることを確認したので、vManageがSSHセッションを開くことができるように、正しいIPを使用してACLを設定できます。

## アクセスコントロールリストの設定

cEdgeに複数のシーケンスがある場合は、必ずACLの先頭に新しいシーケンスを追加してください。

変更前：

```
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
```

設定例：

```
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.
```

新しいシーケンス：

```
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
```

VTY回線にACLを適用します。

```
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
```

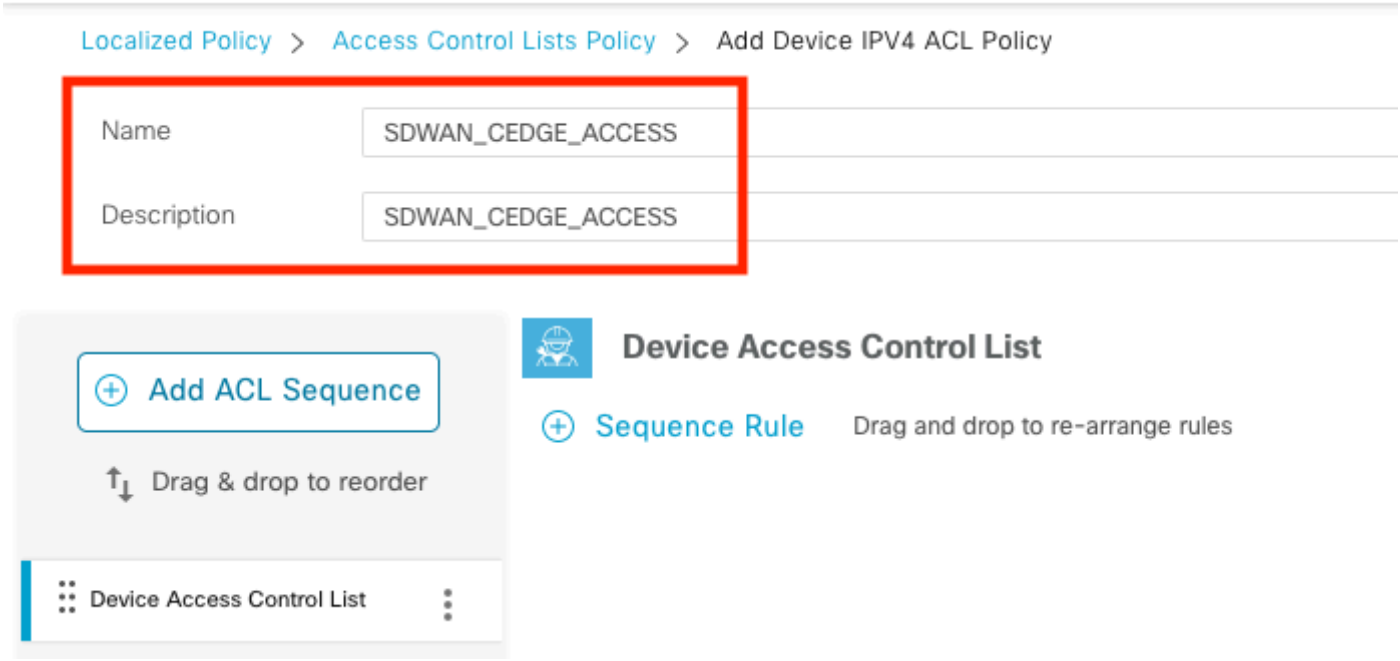
## vManage GUIでの設定

cEdgeデバイスにテンプレートが添付されている場合は、次の手順を実行できます。

**ステップ 1：**ACLの作成

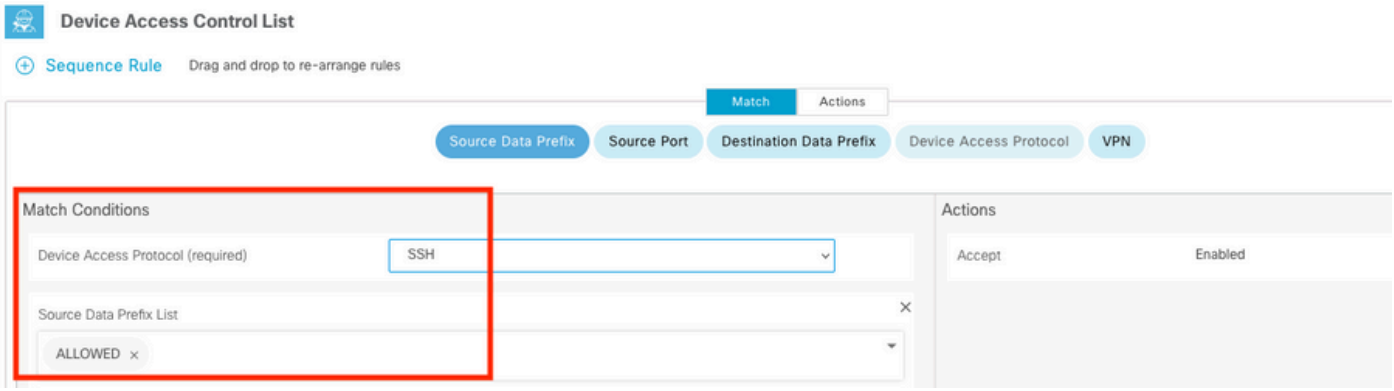
[Configuration] > [Custom Options] > [Access Control List] > [Add Device Access Policy] > [Add ipv4 Device Access Policy] に移動します。

ACLの名前と説明を追加し、[Add ACL Sequence] をクリックして、[Sequence Rule] を選択します



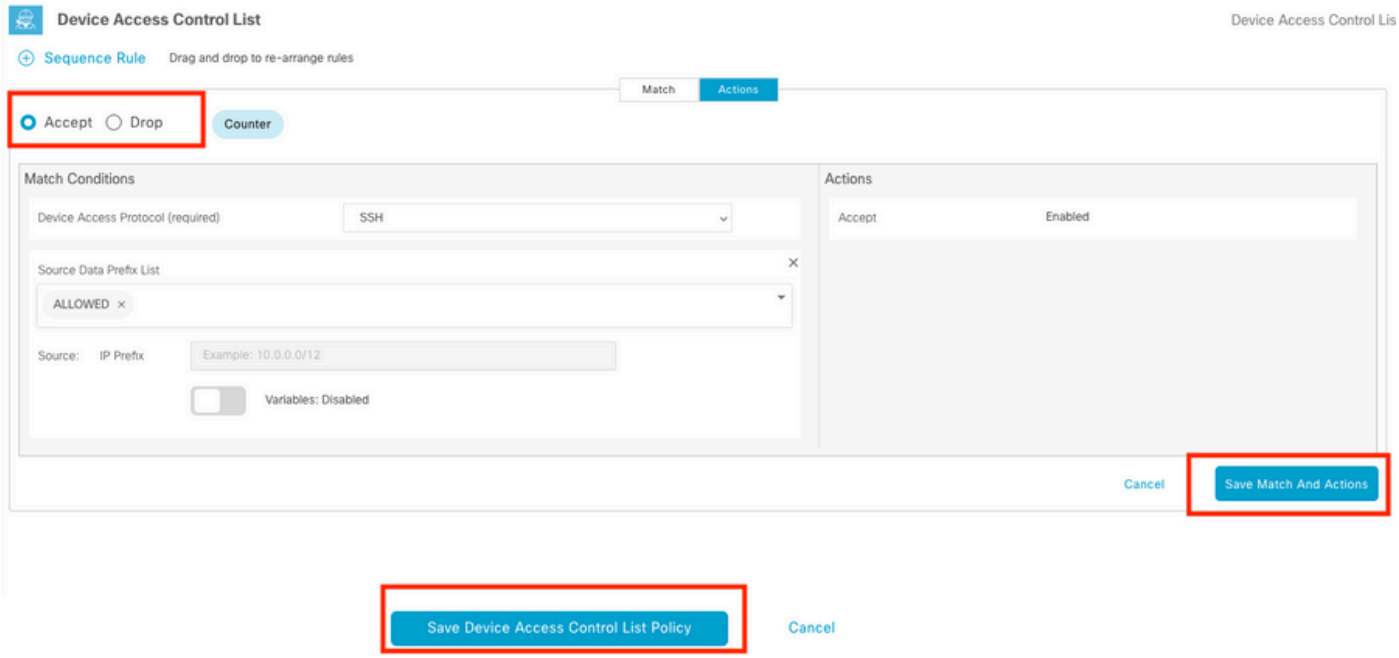

[Device Access Protocol] > [SSH] を選択します

次に、送信元の[Data Prefix List] を選択します。



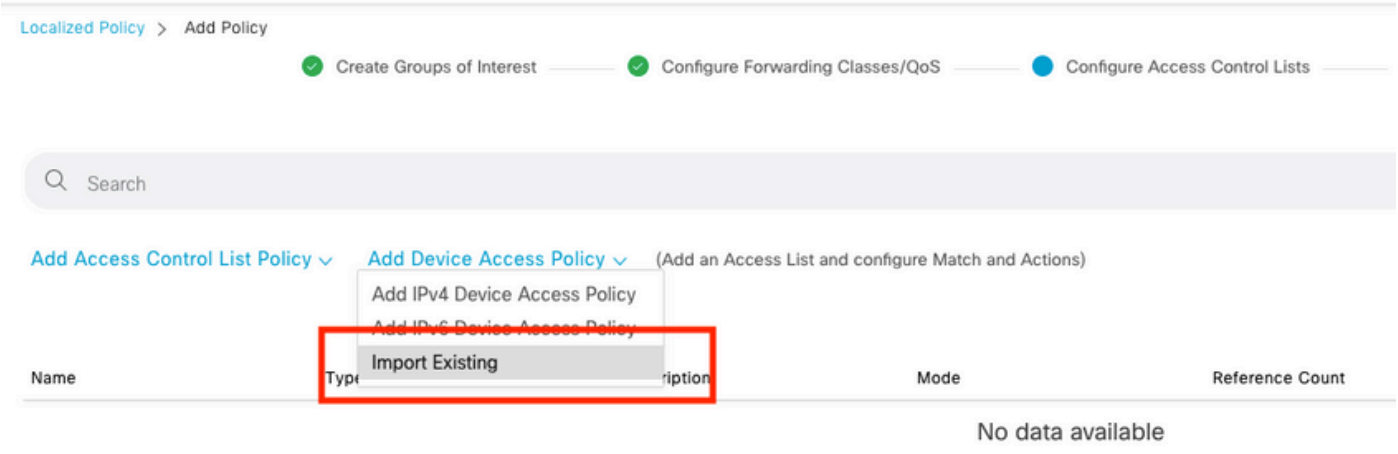

**Actions**をクリックし、**Accept**を選択してから、 Save Match And Actions.

最後に、 Save Device Access Control List Policy.

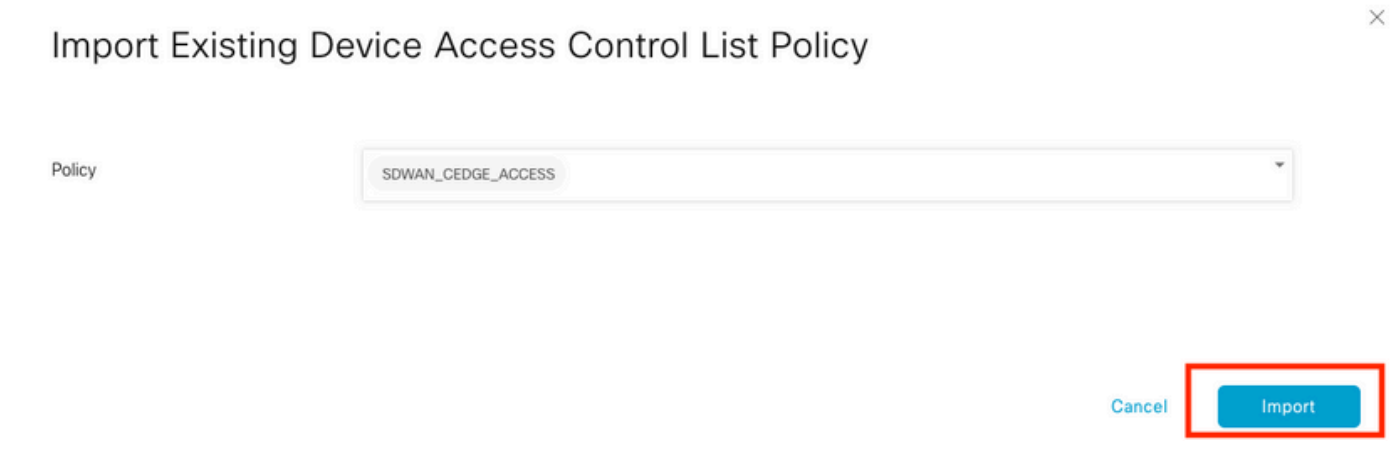



**ステップ 2 : ローカライズされたポリシーの作成**

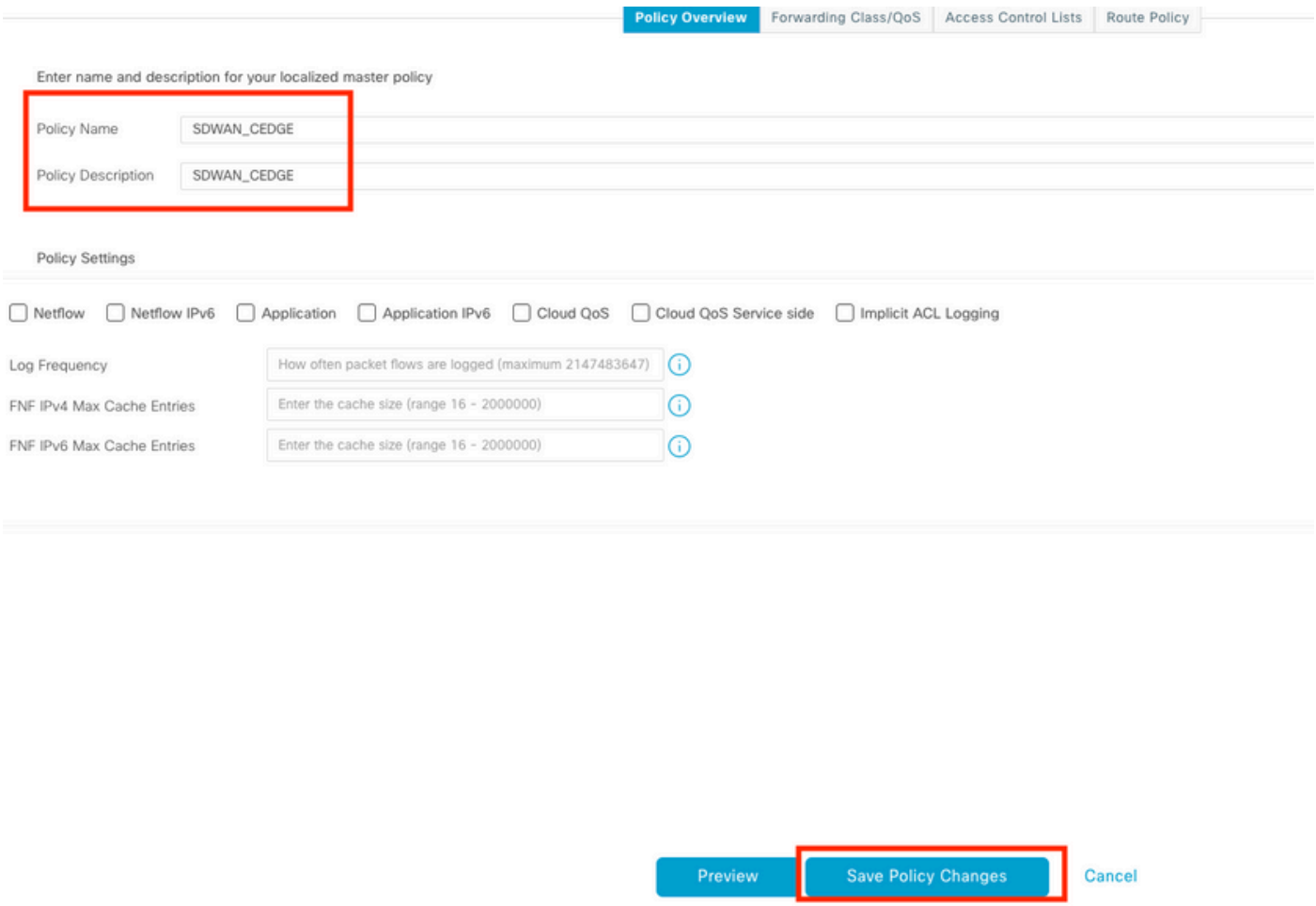
[Configuration] > [Localized Policy] > [Add Policy] > [Configure Access Control List] > [Add Device Access Policy] > [Import Existing] に移動します。




前のACLを選択し、Importをクリックします。

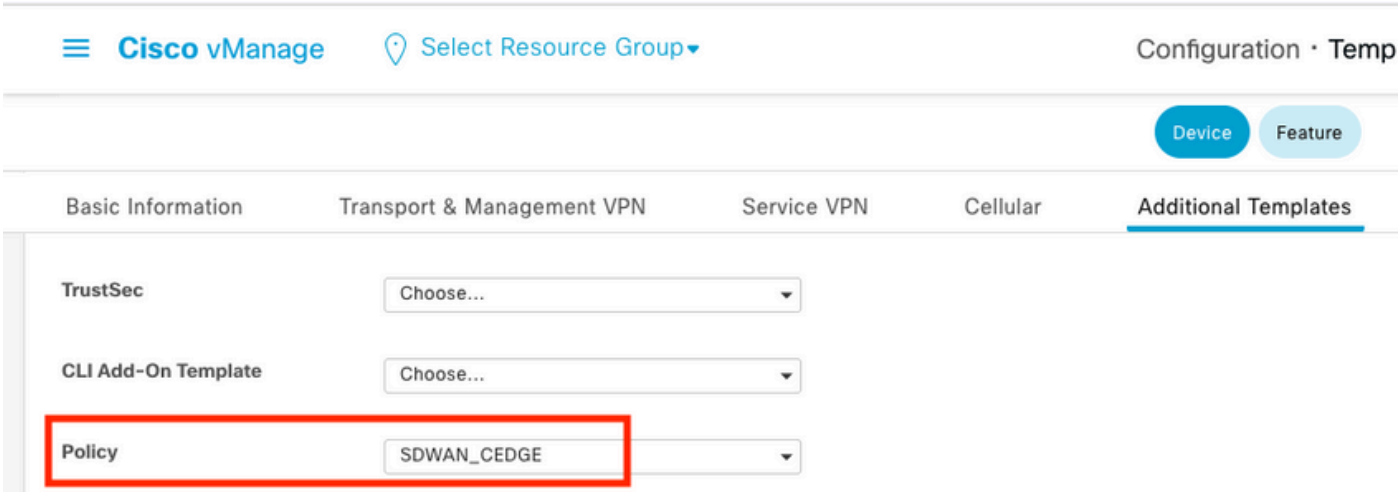



[Policy Name]と[Policy Description]を追加し、 Save Policy Changes.



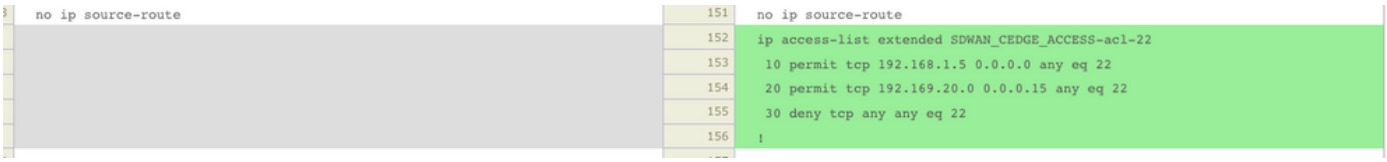

**ステップ 3**：ローカライズされたポリシーをデバイステンプレートに適用する

[Configuration] > [Template] > [Device] > [Select the Device]に移動し、[...] > [Edit] > [Additional Templates] > [Policy] > [SDWAN_CEDGE] > [Update] をクリックします。

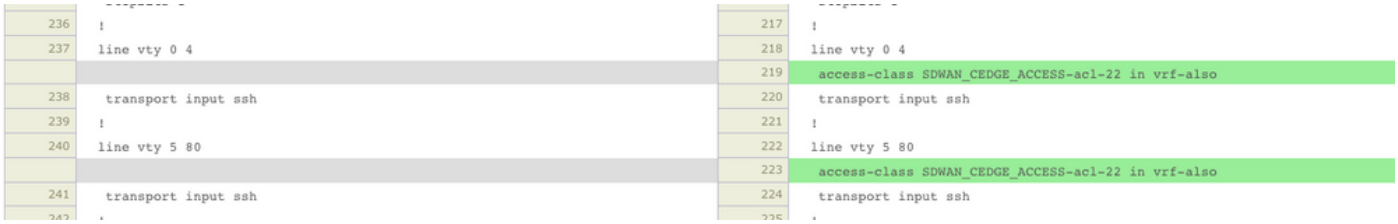



テンプレートをプッシュする前に、設定の違いを確認できます。

新しいACL設定



回線vtyに適用されるACL




## 確認

vManageの以前のフィルタを使用してcEdgeへのSSHアクセスを再びテストするには、次のパスを使用します。**[Menu] > [Tools] > [SSH Terminal]** 。

ルータは192.168.10.114mにSSH接続を試みた

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

Router#
```

ACLカウンタを確認すると、Seq 30に1つの一致があり、SSH接続が拒否されたことを確認できます。

```
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)
```

## 関連情報

[Cisco SD-WANポリシー設定ガイド、Cisco IOS XEリリース17.x]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。