Configurazione di SD-WAN cEdge Router per limitare l'accesso SSH

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Topologia](#)
[Procedura di limitazione dell'accesso SSH](#)
[Verifica connettività](#)
[Convalida lista di controllo dell'accesso](#)
[Configurazione lista di controllo dell'accesso](#)
[Configurazione su GUI vManage](#)
[Verifica](#)
[Informazioni correlate](#)
[Guida alla configurazione delle policy Cisco SD-WAN, Cisco IOS XE release 17.x](#)

Introduzione

Questo documento descrive il processo per limitare la connessione Secure Shell (SSH) al router Cisco IOS-XE® SD-WAN.

Prerequisiti

Requisiti

Per eseguire i test corretti è necessaria la connessione di controllo tra vManage e cEdge.

Componenti usati

Questa procedura non è limitata ad alcuna versione software nei dispositivi Cisco Edge o vManage, quindi tutte le versioni possono essere utilizzate per eseguire questa procedura. Tuttavia, questo documento è riservato esclusivamente ai router cEdge. Per la configurazione, è necessario:

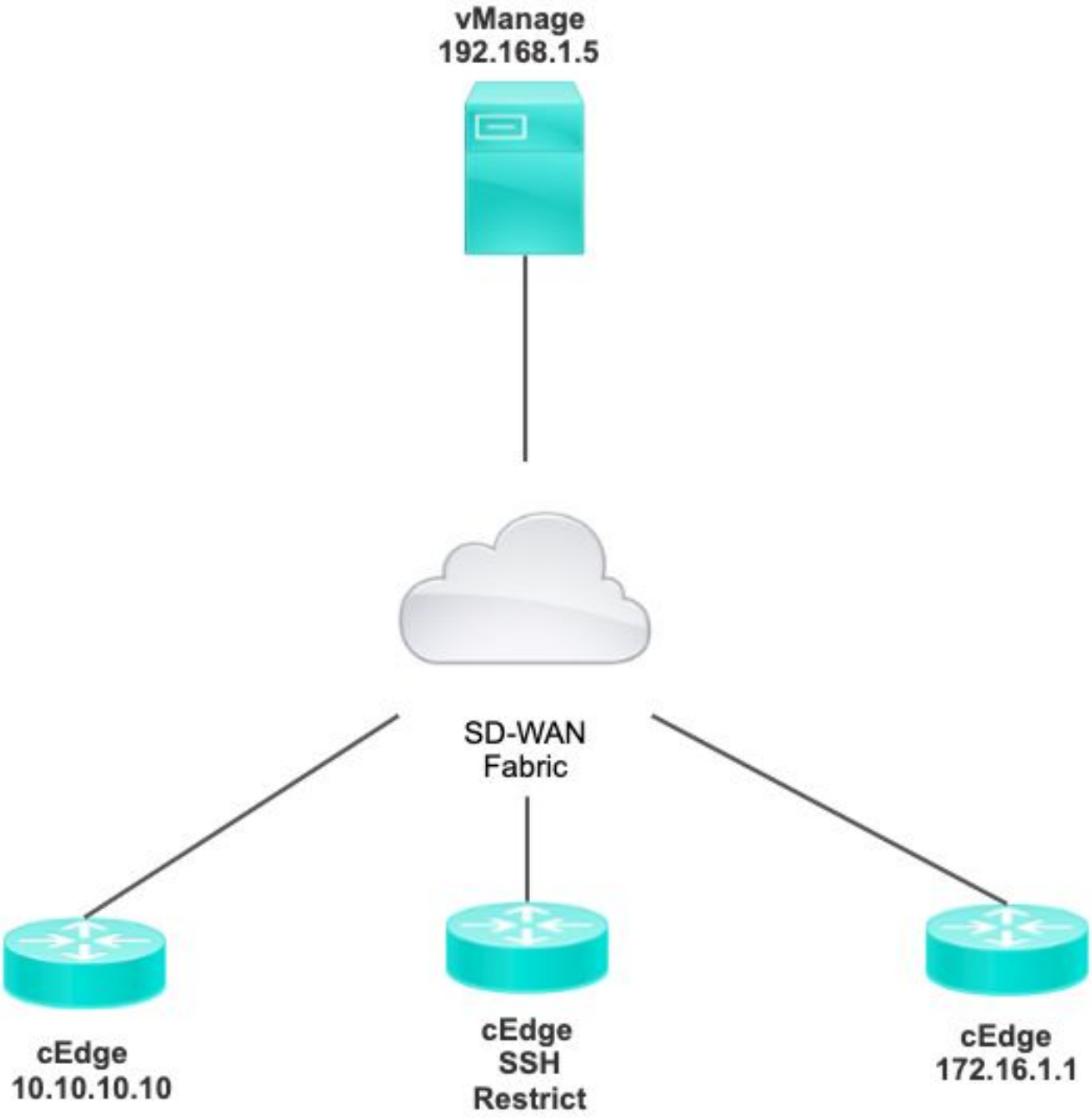
- Cisco cEdge Router (virtuale o fisico)
- Cisco vManage

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Lo scopo di questa dimostrazione è mostrare la configurazione su cEdge per limitare l'accesso SSH da cEdge 172.16.1.1 ma consentire l'accesso a cEdge 10.10.10.10 e vManage.

Topologia



Procedura di limitazione dell'accesso SSH

Verifica connettività

La verifica della connettività è necessaria per verificare che il router cEdge possa raggiungere

vManage. Per impostazione predefinita, vManage utilizza IP 192.168.1.5 per accedere ai dispositivi cEdge.

Dalla GUI di vManage, aprire il protocollo SSH su cEdge e verificare che l'indirizzo IP connesso disponga dell'output successivo:

```
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
```

Assicurarsi che vManage non utilizzi il tunnel, il sistema o l'indirizzo IP pubblico per accedere a cEdge.

Per confermare l'indirizzo IP usato per accedere a cEdge, usare il successivo elenco degli accessi.

```
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.
```

Convalida lista di controllo dell'accesso

Elenco degli accessi applicato alla linea VTY

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

Dopo aver applicato l'ACL, è possibile aprire nuovamente SSH da vManage a cEdge e visualizzare il messaggio successivo generato nei log.

Questo messaggio può essere visualizzato con il 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
```

Nel registro precedente è presente la porta 22 locale. Ciò significa che 192.168.1.5 ha provato ad aprire SSH su cEdge.

Ora che l'IP di origine è stato confermato come 192.168.1.5, è possibile configurare l'ACL con l'IP corretto per consentire a vManage di aprire la sessione SSH.

Configurazione lista di controllo dell'accesso

Se cEdge ha più sequenze, accertarsi di aggiungere la nuova sequenza all'inizio dell'ACL.

Prima:

```
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
```

Esempio di configurazione:

```
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.
```

Nuova sequenza:

```
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
```

Applicare l'ACL sulla linea 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
```

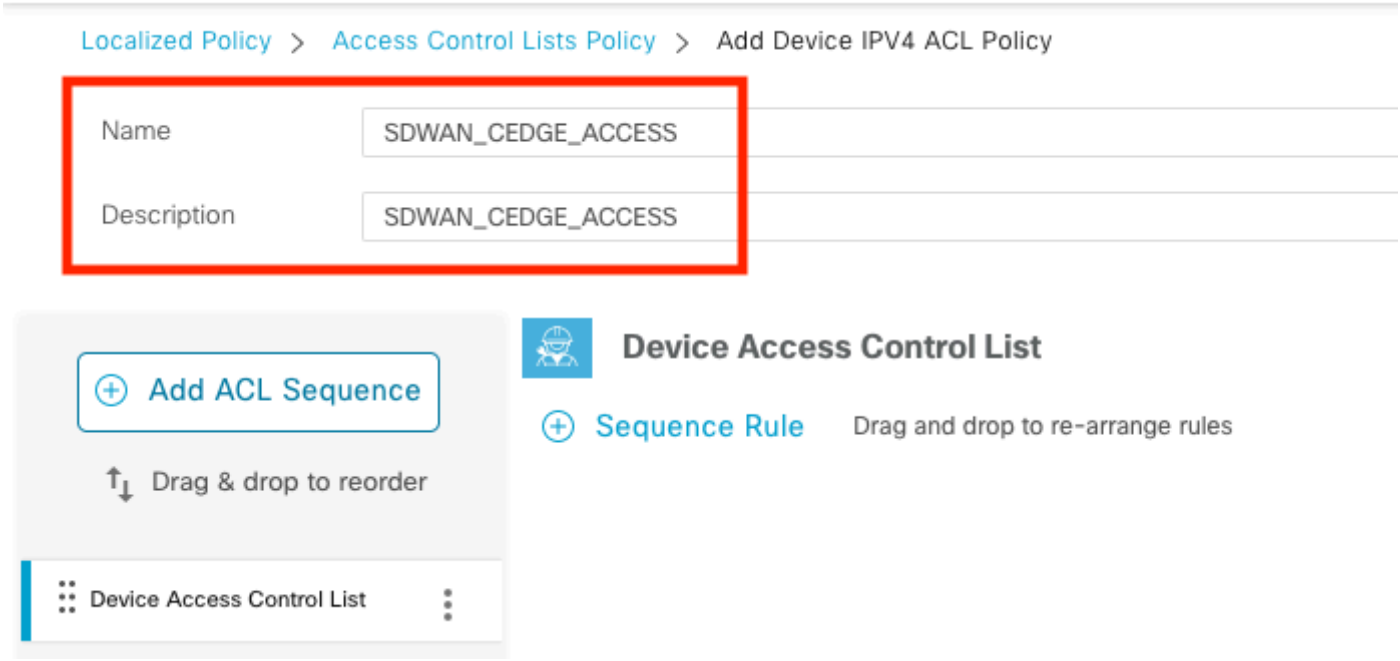
Configurazione su GUI vManage

Se al dispositivo cEdge è associato un modello, è possibile utilizzare la procedura successiva.

Passaggio 1. Creare un ACL

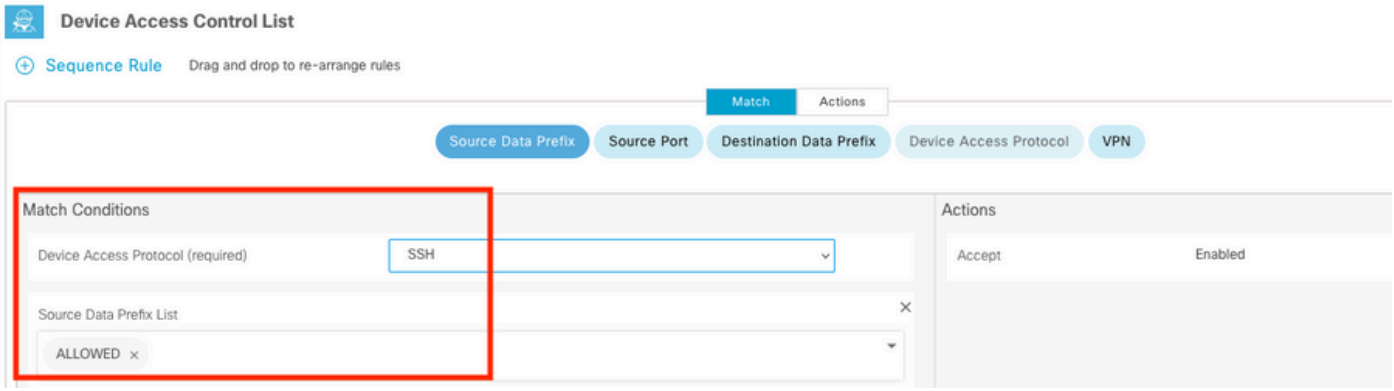
Selezionare **Configurazione > Opzioni personalizzate > Access Control List > Add Device Access Policy > Add ipv4 Device Access Policy**

Aggiungere il nome e la descrizione dell'ACL, fare clic su **Add ACL Sequence**, quindi selezionare **Sequence Rule**



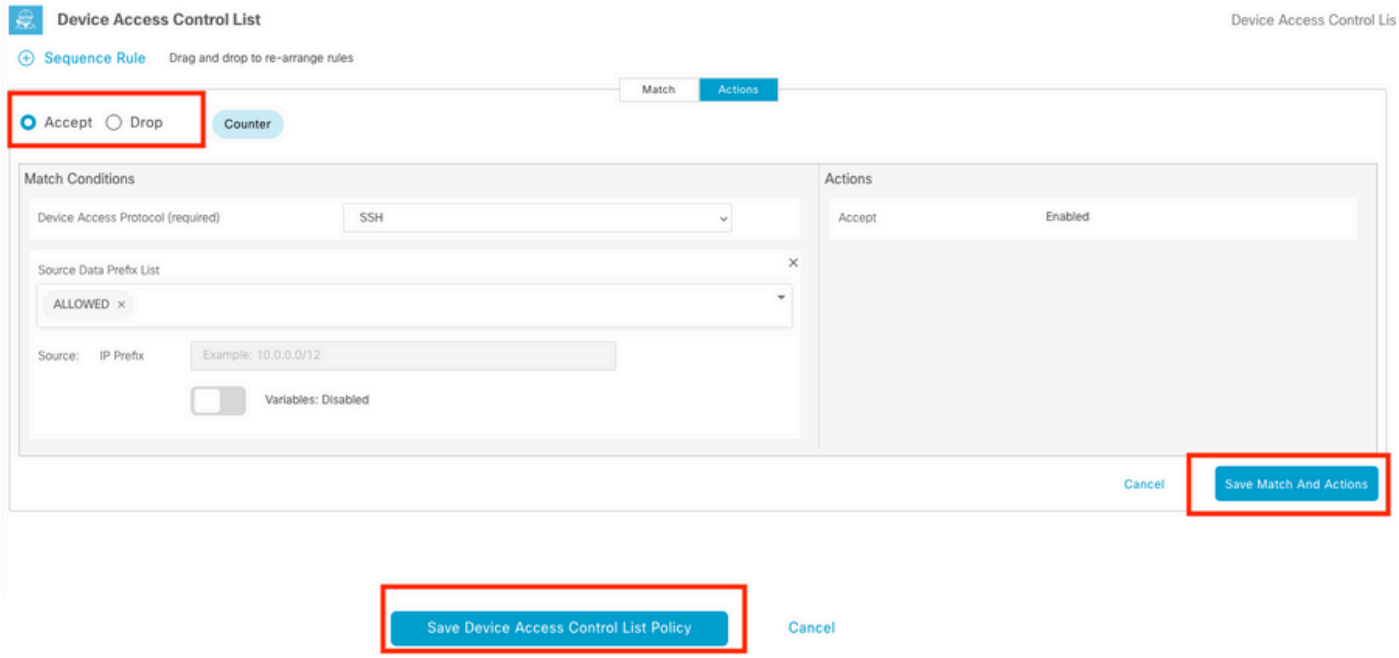
Selezionare **Device Access Protocol > SSH**

Selezionare quindi l'**elenco di prefissi dei dati di** origine.



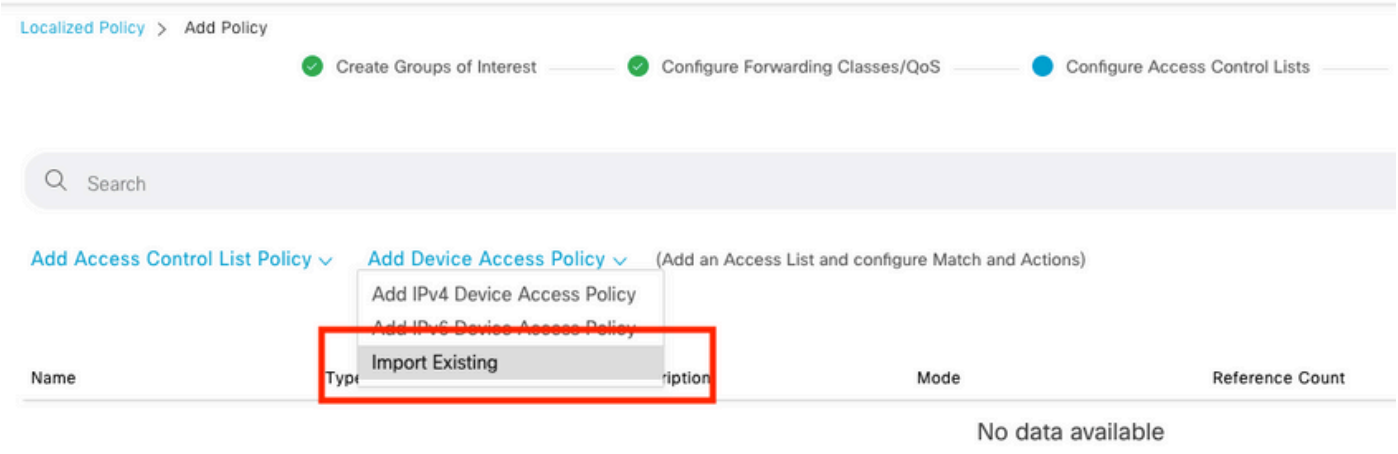
Fare clic su **Azioni**, selezionare **Accetta**, quindi fare clic su Save Match And Actions.

Infine, è possibile selezionare Save Device Access Control List Policy.

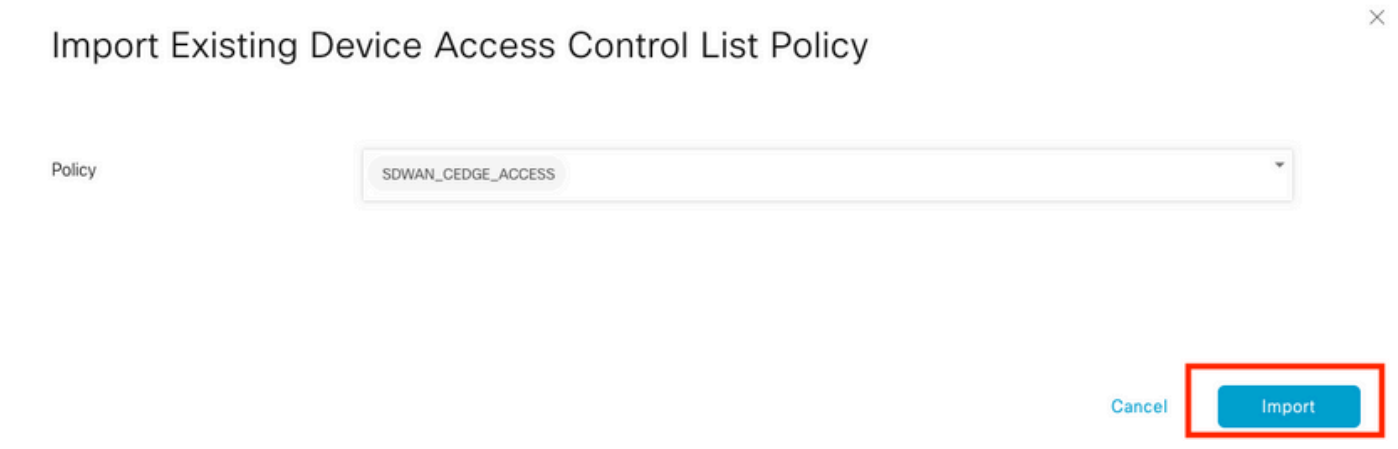


Passaggio 2. Crea criterio localizzato

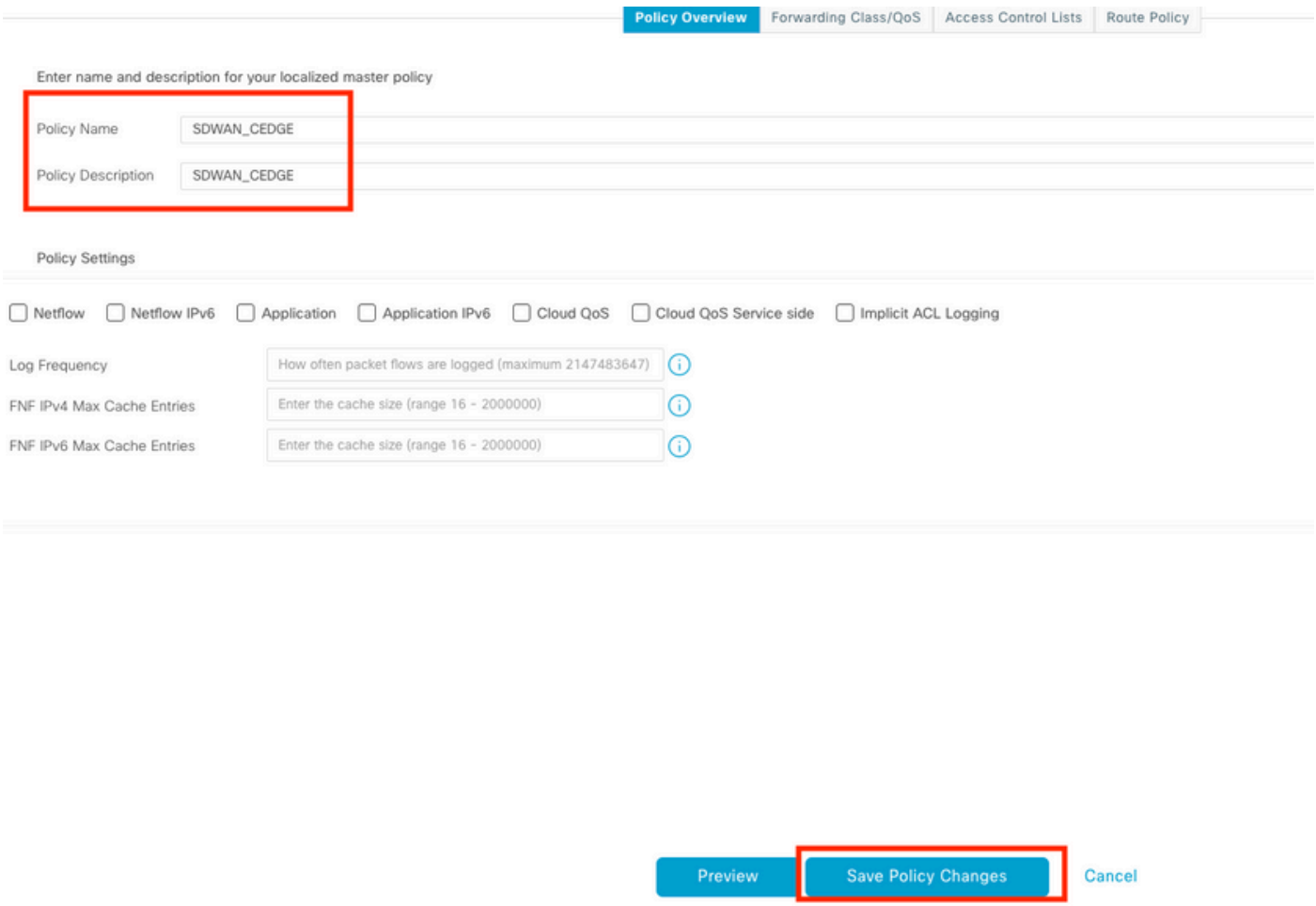
Passare a **Configurazione > Criteri localizzati > Aggiungi criterio > Configura elenco di controllo di accesso > Aggiungi criterio di accesso al dispositivo > Importa esistente**.



Selezionare l'**ACL** precedente e fare clic su **Importa**.

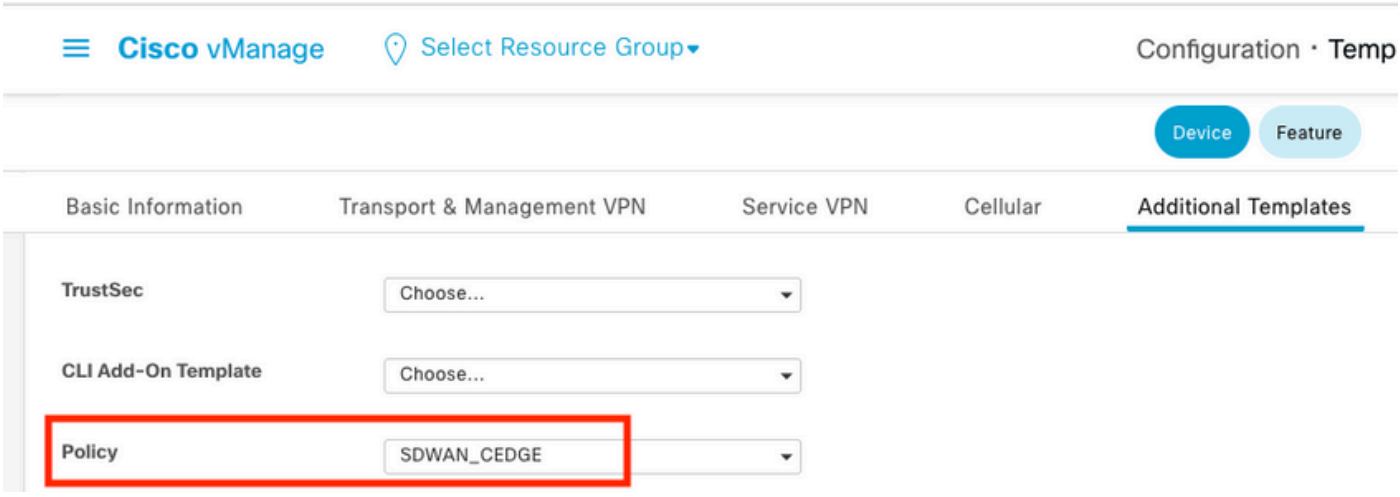


Aggiungere il nome e la descrizione del criterio, quindi fare clic su Save Policy Changes.



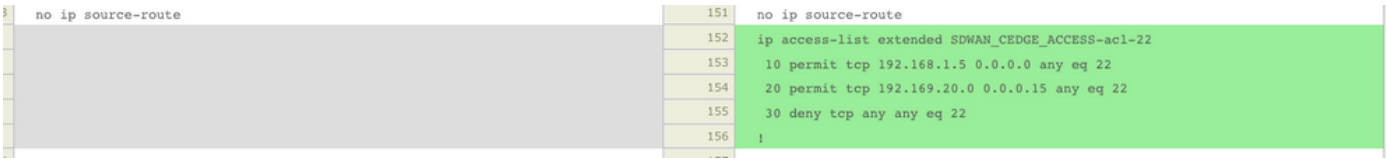
Passaggio 3. Collega il criterio localizzato al modello di dispositivo

Selezionare **Configurazione > Modello > Dispositivo > Selezionare il dispositivo e fare clic su > ... > Modifica > Modelli aggiuntivi > Criterio > SDWAN_CEDGE > Aggiorna**.



Prima di applicare il modello, è possibile verificare la differenza di configurazione.

Nuova configurazione ACL



ACL applicato alla riga 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
```

Verifica

Ora è possibile testare nuovamente l'accesso SSH a cEdge con i filtri precedenti da vManage con questo percorso: **Menu > Strumenti > Terminale SSH**.

Il router ha tentato di usare il protocollo SSH su 192.168.10.14m

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

Router#
```

Se si controllano i contatori ACL, è possibile verificare che la sequenza 30 abbia 1 corrispondenza e che la connessione SSH sia stata negata.

```
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)
```

Informazioni correlate

[Guida alla configurazione delle policy Cisco SD-WAN, Cisco IOS XE release 17.x]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).