SD-WAN cEdge router configureren om SSH-toegang te beperken

Inhoud

Inleiding

Dit document beschrijft het proces om de verbinding van Secure Shell (SSH) te beperken tot Cisco IOS-XE® SD-WAN router.

Voorwaarden

Vereisten

Om de juiste tests te kunnen uitvoeren, is een regelverbinding tussen vManager en cEdge vereist.

Gebruikte componenten

Deze procedure is niet beperkt tot enige softwarerelease in Cisco Edge- of vManager-apparaten, dus alle releases kunnen bij deze stappen worden gebruikt. Dit document is echter exclusief voor cEdge-routers. Om te configureren hebt u dit nodig:

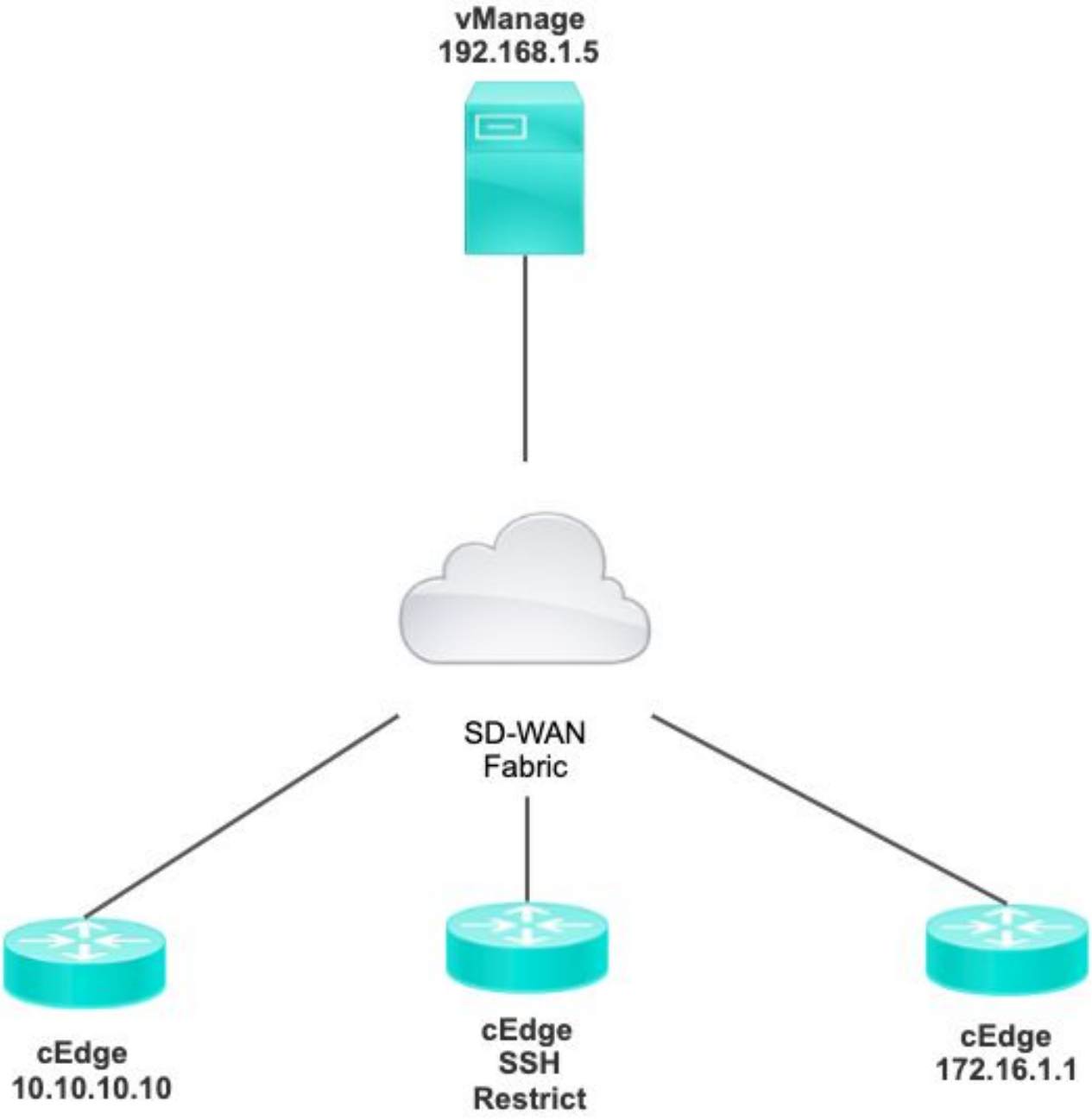
- Cisco cEdge-router (virtueel of fysiek)
- Cisco vManager

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het doel van deze demonstratie is de configuratie op cEdge te tonen om de toegang tot SSH van cEdge 172.16.1.1 te beperken, maar cEdge 10.10.10.10 en vManager toe te staan.

Topologie



Toegangsprocedure voor SSH beperken

Connectiviteitsverificatie

Verificatie van de connectiviteit is nodig om te valideren dat de cEdge-router de vManager kan

bereiken. Standaard gebruikt vManager IP 192.168.1.5 om in te loggen op cEdge-apparaten.

Open vanuit vManager GUI SSH naar cEdge en zorg ervoor dat het aangesloten IP de volgende uitvoer heeft:

```
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
```

Zorg ervoor dat vManager de tunnel, het systeem of het publieke IP-adres niet gebruikt om in te loggen op cEdge.

Om de IP te bevestigen die wordt gebruikt om in te loggen op cEdge, kunt u de volgende toegangslijst gebruiken.

```
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.
```

Validering van toegangscontrolelijst

Toegangslijst toegepast op VTY-lijn

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

Nadat de ACL is toegepast, kunt u SSH opnieuw openen van vManager naar cEdge en het volgende bericht zien dat wordt gegenereerd in de logbestanden.

Dit bericht kan met opdracht worden gezien: **toon het registreren**.

```
*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
```

In het vorige logbestand ziet u Local poort 2. Het betekent dat 192.168.1.5 geprobeerd heeft om SSH open te stellen voor cEdge.

Nu u hebt bevestigd dat IP-bron 192.168.1.5 is, kunt u de ACL met de juiste IP configureren zodat vManager SSH-sessie kan openen.

Configuratie van toegangscontrolelijst

Als cEdge meerdere sequenties heeft, moet u de nieuwe sequentie boven aan ACL toevoegen.

Voor:

```
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
```

Configuratievoorbeeld:

```
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.
```

Nieuwe sequentie:

```
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
```

ACL toepassen op VTY-lijn.

```
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
```

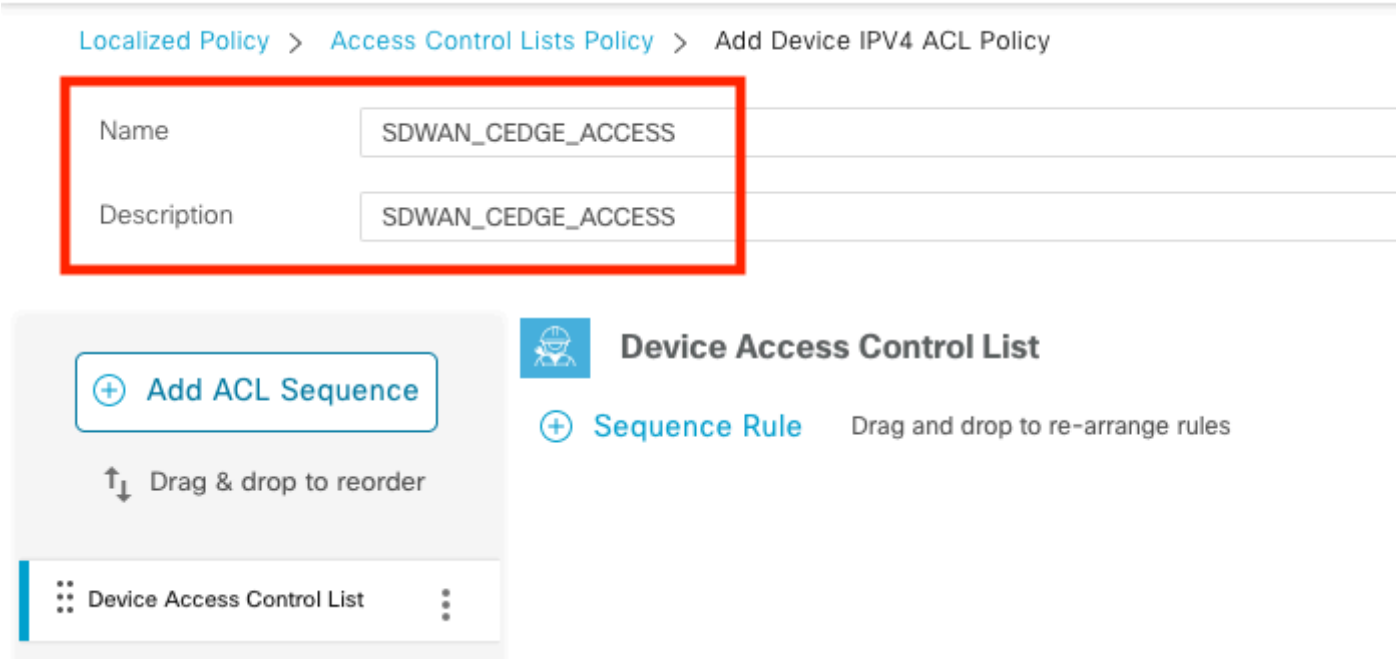
Configuratie op vManager GUI

Als het cEdge-apparaat een sjabloon heeft aangesloten, kunt u de volgende procedure gebruiken.

Stap 1. Maak een ACL

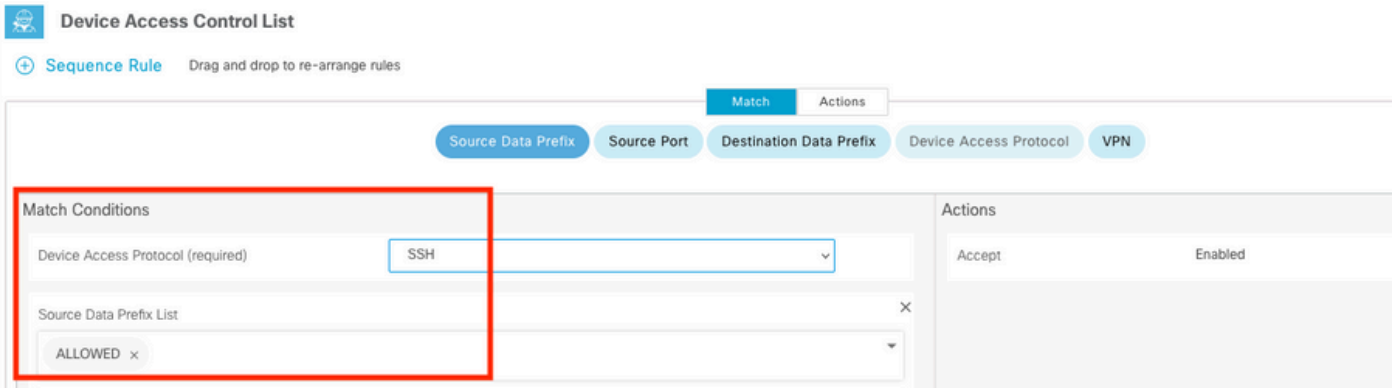
Navigeer naar **Configuratie > Aangepaste opties > Toegangscontrolelijst > Toegangsbeleid voor apparaat toevoegen > Toegangsbeleid voor apparaat toevoegen**

Voeg de naam en de beschrijving van ACL toe en klik op **Add ACL Sequence** en selecteer vervolgens **Sequence Rule**



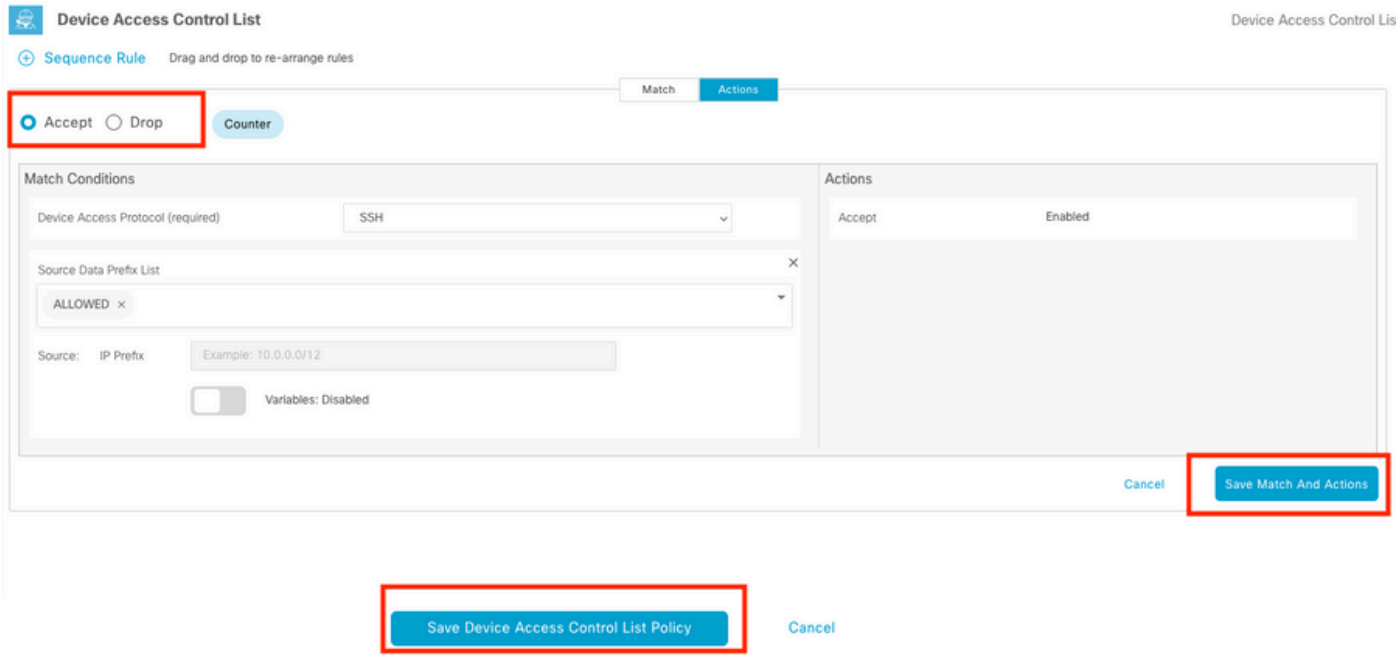
Selecteer **Apparaattoegangsprotocol >SSH**

Selecteer vervolgens de **prefixlijst** bron **gegevens**.



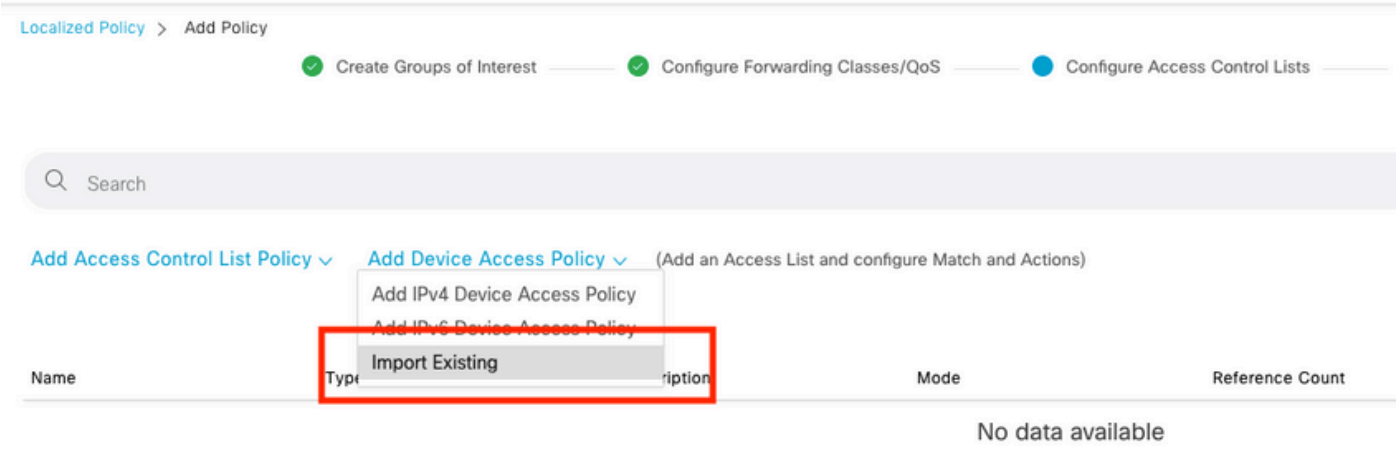
Klik op **Handelingen**, selecteer **Akkoord** en klik vervolgens op Save Match And Actions.

Ten slotte kunt u Save Device Access Control List Policy.

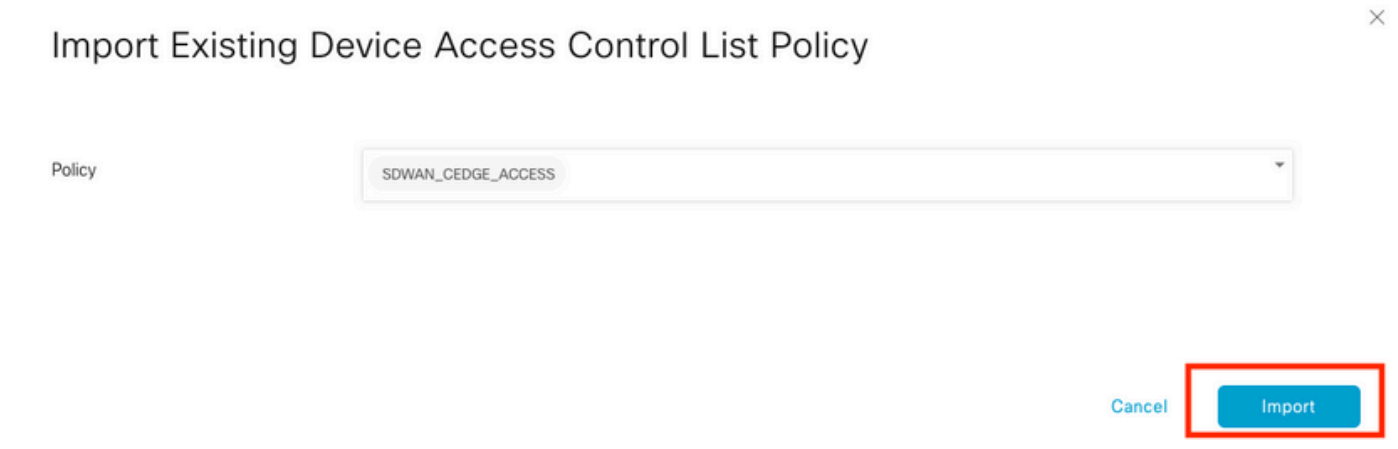


Stap 2. Gelokaliseerd beleid maken

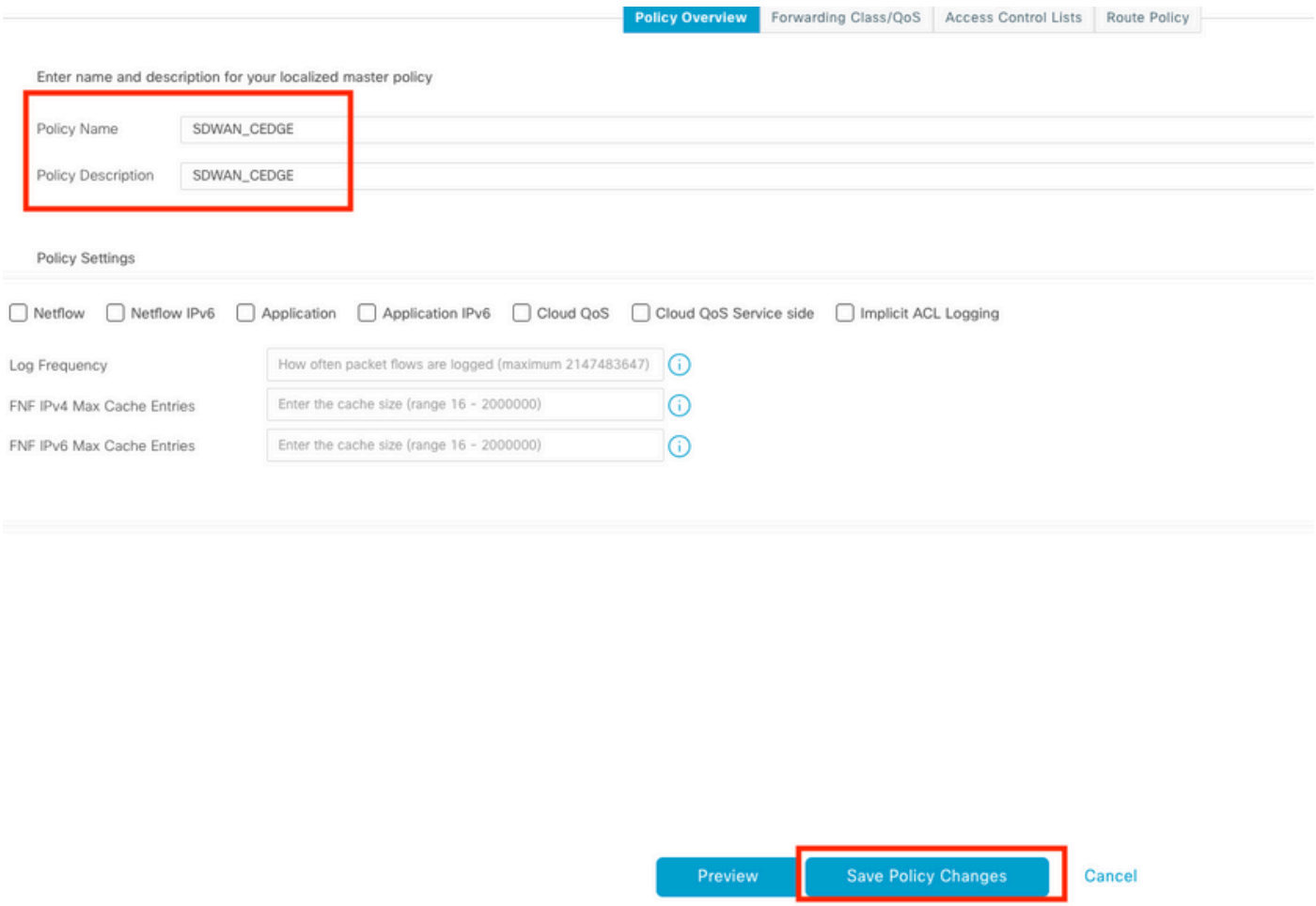
Navigeer naar **Configuration > Localized Policy > Add Policy > Configure Access Control List > Add Device Access Policy > Import Existing**.



Selecteer vorige **ACL** en klik op **Importeren**.

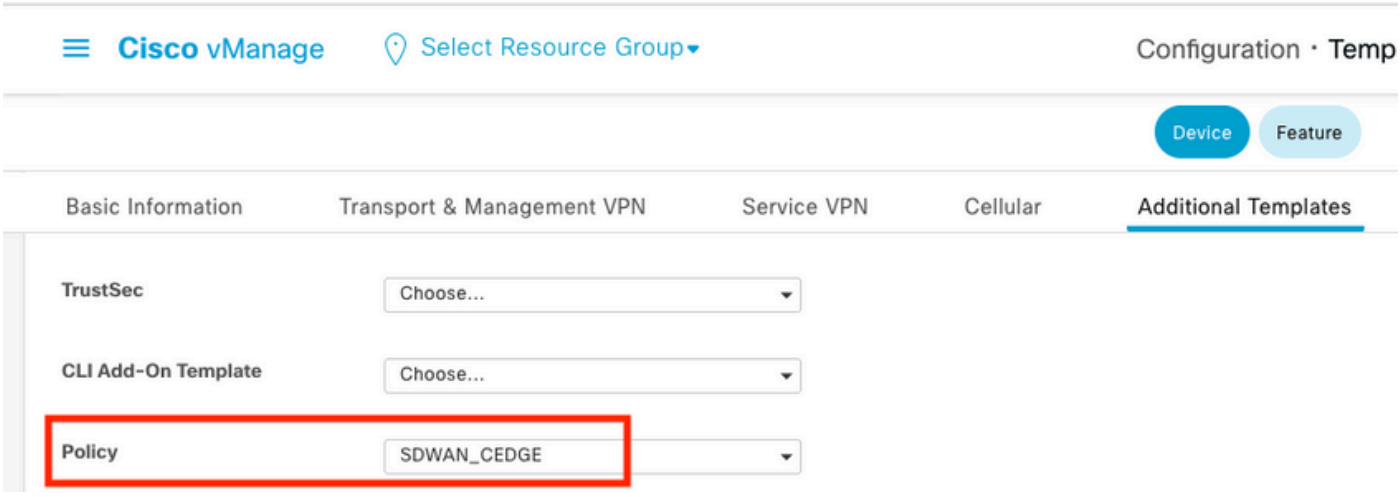


Voeg de beleidsnaam en de beleidsbeschrijving toe en klik vervolgens op Save Policy Changes.



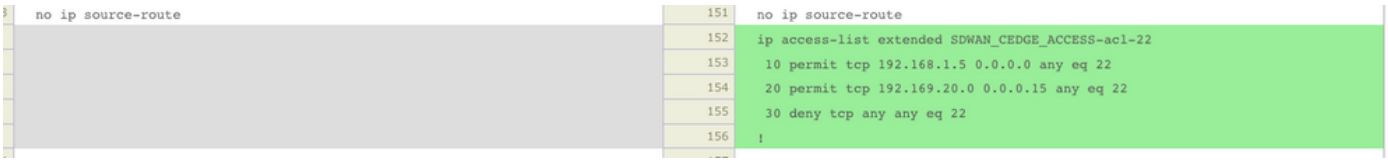
Stap 3. Hang het gelokaliseerde beleid aan de apparaatsjabloon

Navigeer naar **Configuratie > Sjabloon > Apparaat > Selecteer het apparaat en klik op > ... > Bewerken > Aanvullende sjablonen > Beleid > SDWAN_CEDGE > Bijwerken**.

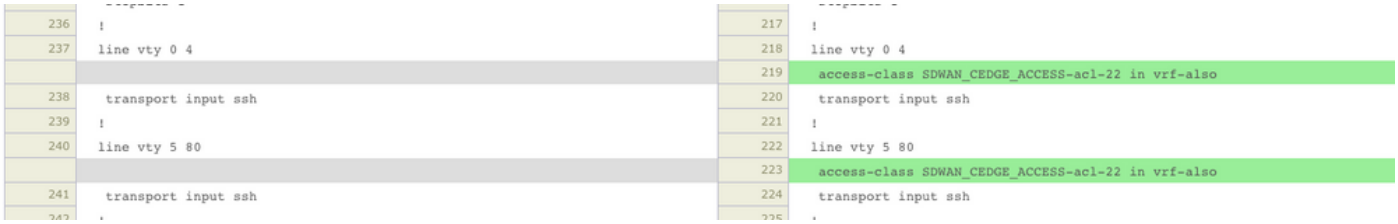


Alvorens u het malplaatje duwt, kunt u het Verschil van de Configuratie verifiëren.

Nieuwe ACL-configuratie



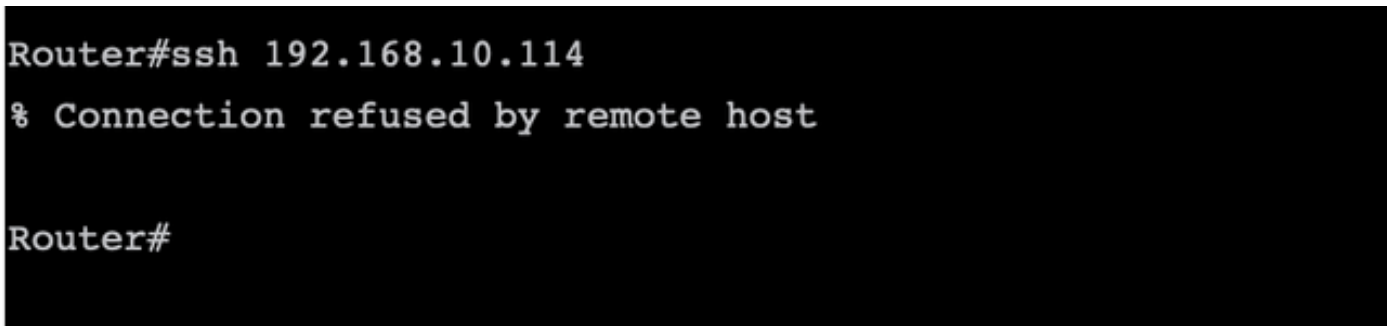
ACL toegepast op regel vty



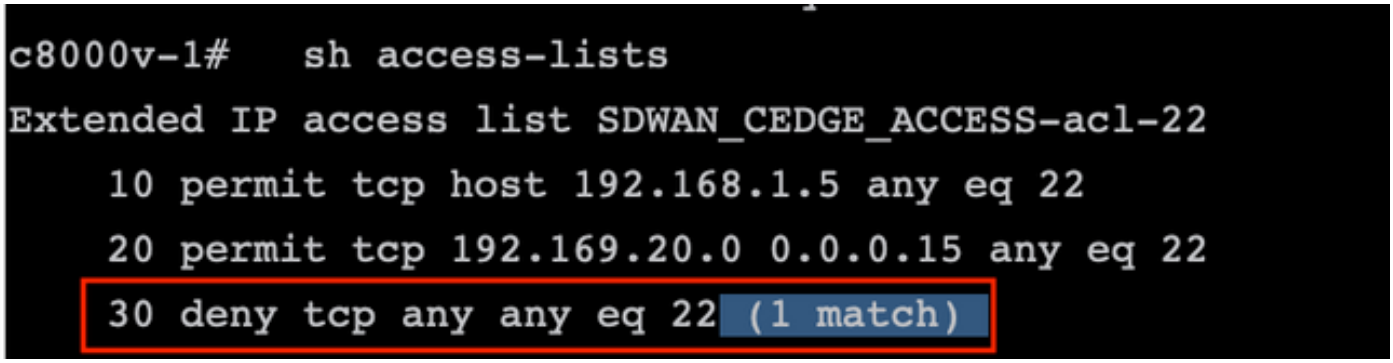
Verificatie

Nu kunt u de SSH-toegang tot cEdge opnieuw testen met eerdere filters van vManager via dit pad: **Menu > Tools > SSH Terminal**.

Router geprobeerd naar SSH naar 192.168.10.14m



Als u de ACL-tellers controleert, kunt u bevestigen dat Seq 30 1 match heeft en dat de SSH-verbinding is geweigerd.



Gerelateerde informatie

[Cisco SD-WAN Policy Configuration Guide, Cisco IOS XE release 17.x]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.