تكوين موجه SD-WAN cEdge لتقييد وصول SSH

المحتويات

المقدمة

يصف هذا المستند عملية تقييد اتصال طبقة الأمان (SSH) بموجه Cisco IOS-XE® SD-WAN.

المتطلبات الأساسية

المتطلبات

يلزم توفر اتصال التحكم بين vManage و cEdge لإجراء الاختبارات المناسبة.

المكونات المستخدمة

لا يقتصر هذا الإجراء على أي إصدار برنامج في أجهزة Cisco Edge أو vManage، وبالتالي يمكن استخدام جميع الإصدارات مع هذه الخطوات. ومع ذلك، فإن هذا المستند خاص بموجهات cEdge. للتكوين، يلزم ما يلي:

- موجه Cisco cEdge (ظاهري أو مادي)
- برنامج Cisco vManage

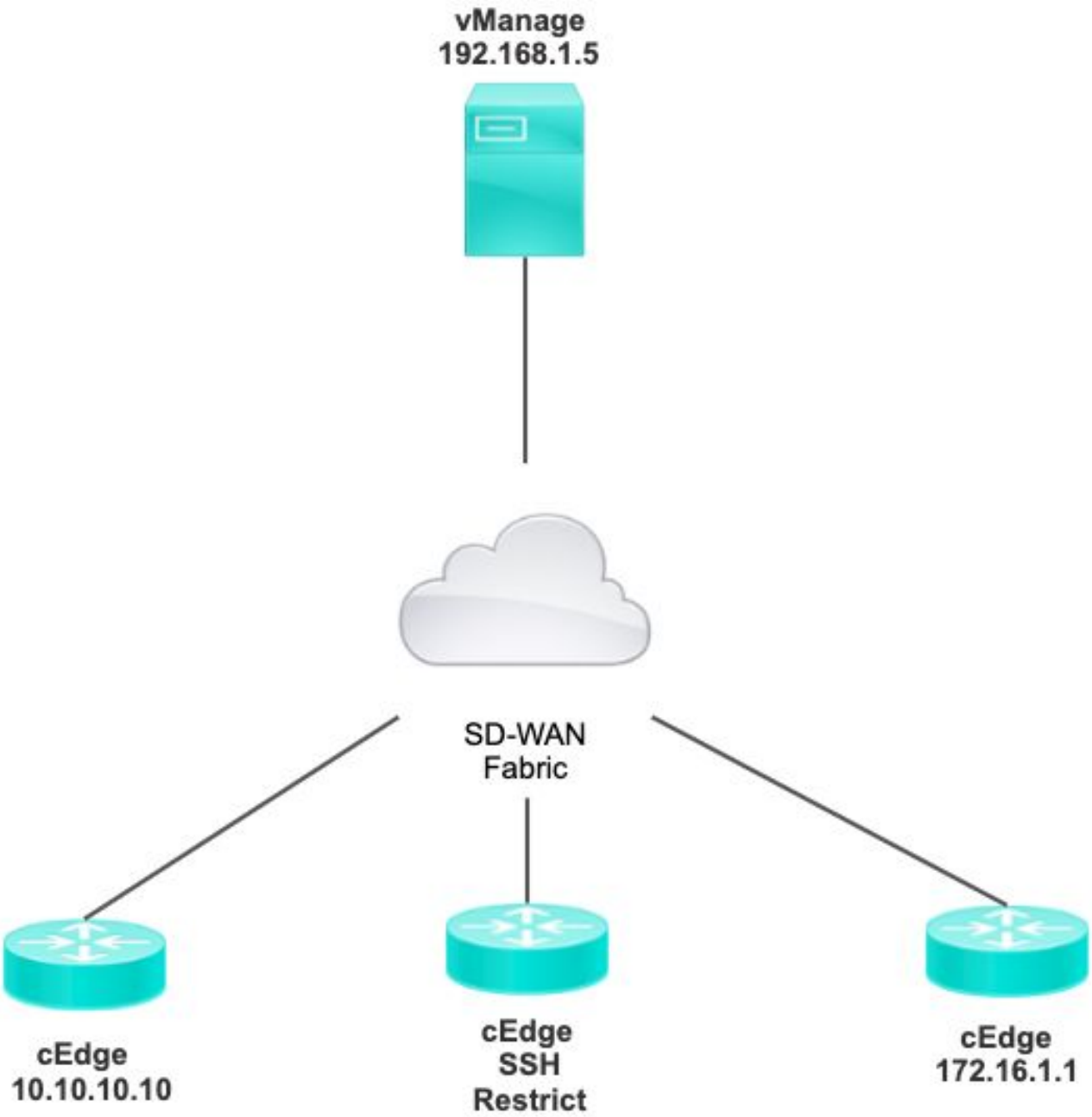
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

الغرض من هذا العرض التوضيحي هو عرض التكوين الموجود على cEdge لتقييد وصول SSH من cEdge 172.16.1.1 و لكن مع السماح ل cEdge 10.10.10.10 و vManage.

المخطط



إجراء تقييد الوصول إلى SSH

التحقق من الاتصال

يلزم التحقق من الاتصال للتحقق من صحة إمكانية وصول موجه cEdge إلى vManage. بشكل افتراضي، يستخدم vManage IP 192.168.1.5 لتسجيل الدخول إلى أجهزة cEdge.

من واجهة المستخدم الرسومية vManage، افتح SSH إلى cEdge وتأكد من أن بروتوكول الإنترنت الذي تم توصيله يحتوي على الإخراج التالي:

```
<#root>

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
```

تأكد من أن vManage ال يستخدم النفق أو النظام أو عنوان IP العام لتسجيل الدخول إلى cEdge.

لتأكيد IP الذي يتم إستخدامه لتسجيل الدخول إلى cEdge، يمكنك إستخدام قائمة الوصول التالية.

```
<#root>

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
```

التحقق من صحة قائمة التحكم بالوصول

قائمة الوصول المطبقة على خط vty

```
<#root>

cEdge#

show sdwan running-config | section vty


line vty 0 4
```

```
 access-class VTY_FILTER_SSH in vrf-also
 transport input ssh
```

بعد تطبيق قائمة التحكم في الوصول (ACL)، يمكنك فتح SSH مرة أخرى من vManage إلى cEdge ورؤية الرسالة التالية التي تم إنشاؤها على السجلات.

يمكن رؤية هذه الرسالة باستخدام الأمر: show logging.

```
*Jul 13 15:05:47.781: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Tadmin] [Source: 192.168.1.5] [l
```

على السجل السابق، أنت يستطيع رأيت محلي ميناء 22. وهذا يعني أن الإصدار 192.168.1.5 حاول فتح SSH على cEdge.

الآن بعد أن أكدت أن مصدر IP وه 192.168.1.5، يمكنك تكوين قائمة التحكم في الوصول باستخدام IP الصحيح للسماح لـ vManage بالقدرة على فتح جلسة SSH.

تكوين قائمة التحكم في الوصول

إذا كان لـ cEdge تسلسلات متعددة، فتأكد من إضافة التسلسل الجديد في أعلى قائمة التحكم في الوصول (ACL).

قبل:

<#root>

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
```

مثال التكوين:

<#root>

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.
```

تسلسل جديد:

<#root>

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
```

تطبيق قائمة التحكم في الوصول (ACL) على خط vty.

<#root>

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
```

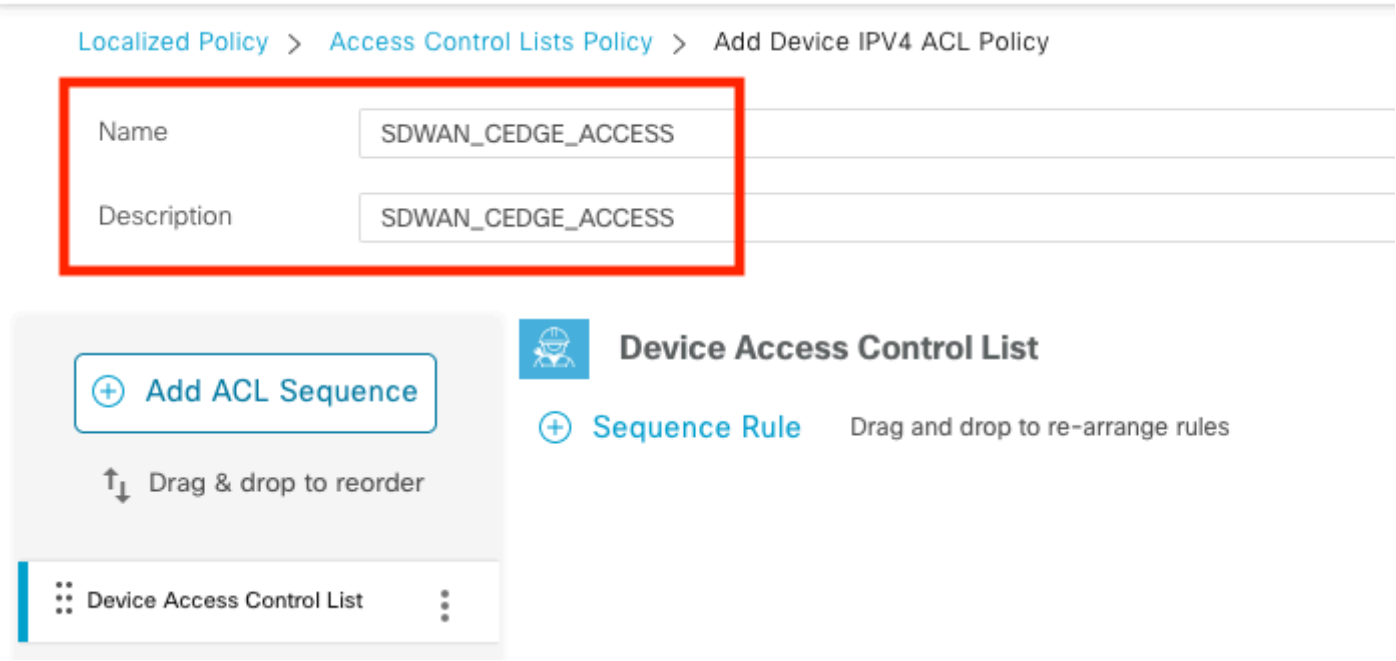
التكوين على واجهة المستخدم الرسومية vManage

إذا كان لدى جهاز cEdge قالب مرفق، يمكنك إستخدام الإجراء التالي.

الخطوة 1. إنشاء قائمة تحكم في الوصول (ACL)

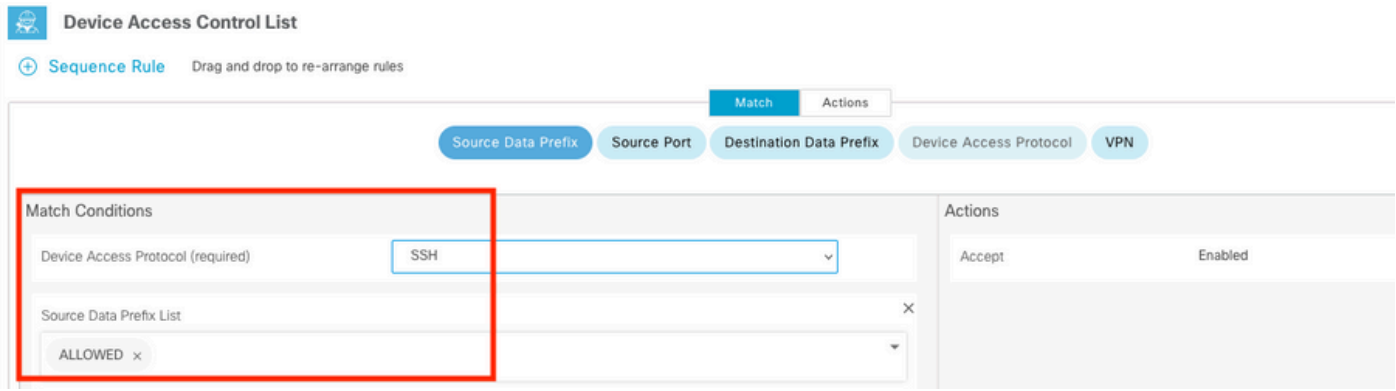
انتقل إلى التكوين > خيارات مخصصة > قائمة التحكم في الوصول > إضافة سياسة الوصول إلى الأجهزة > إضافة سياسة الوصول إلى أجهزة IPv4

قم بإضافة اسم قائمة التحكم في الوصول (ACL) ووصفه وانقر فوق إضافة تسلسل قائمة التحكم في الوصول (ACL) ثم حدد قاعدة التسلسل



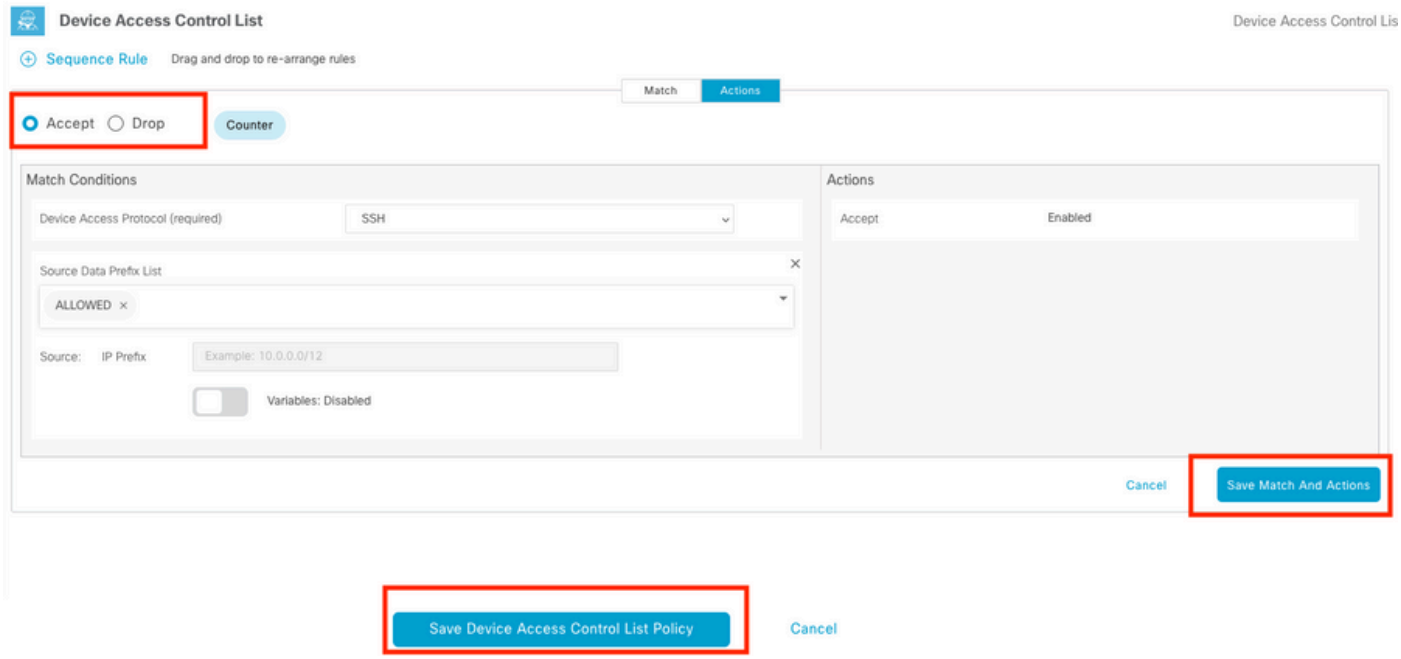
حدد بروتوكول الوصول إلى الجهاز >SSH

ثم حدد قائمة بادئات البيانات المصدر.



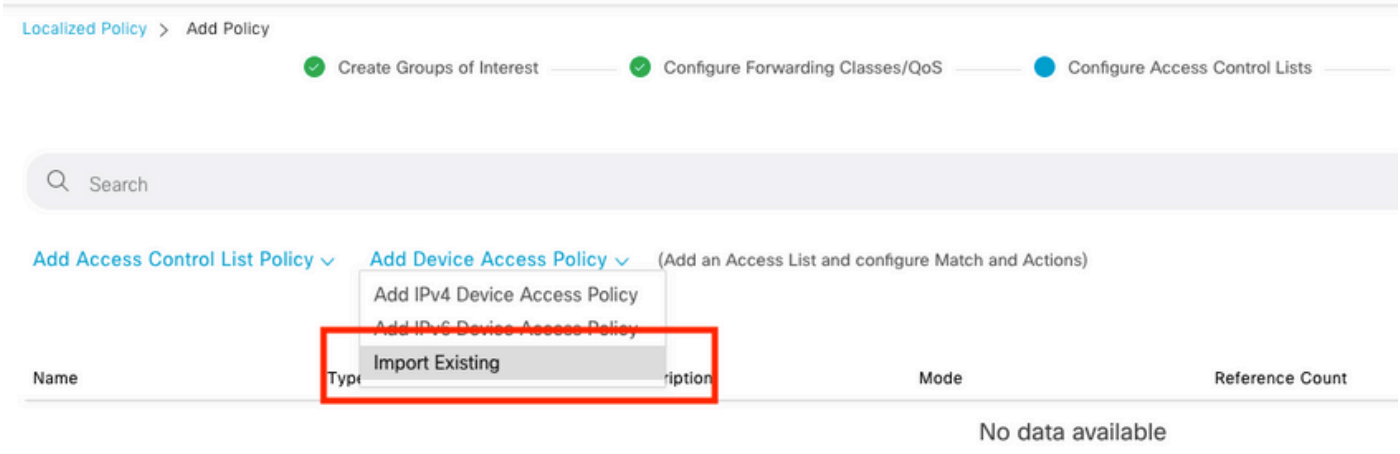
انقر عملیات، حدد قبول، ثم انقر Save Match And Actions.

أخيرا، يمكنك أن تختار Save Device Access Control List Policy.

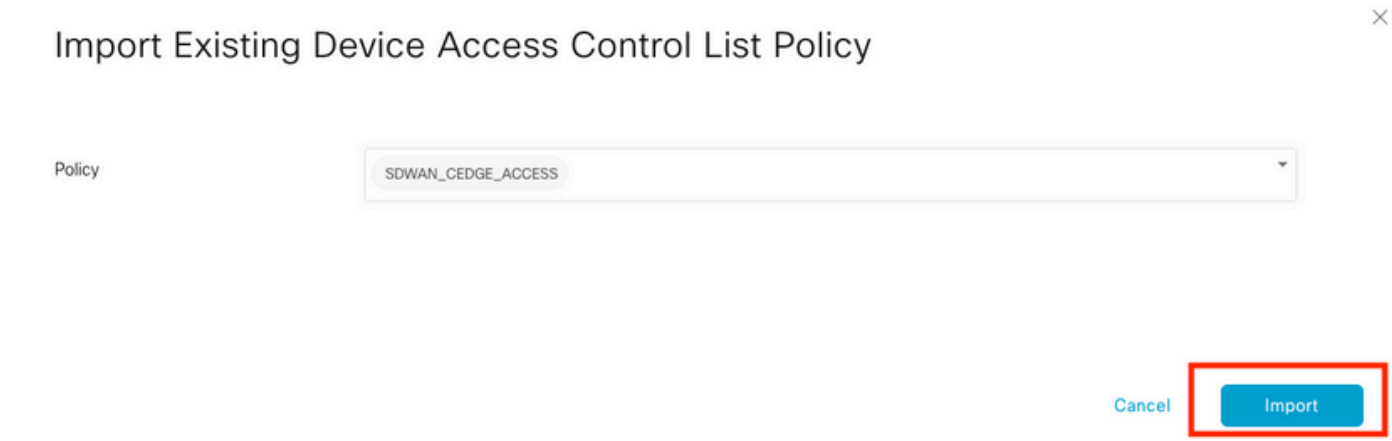


الخطوة 2. إنشاء نهج مترجم

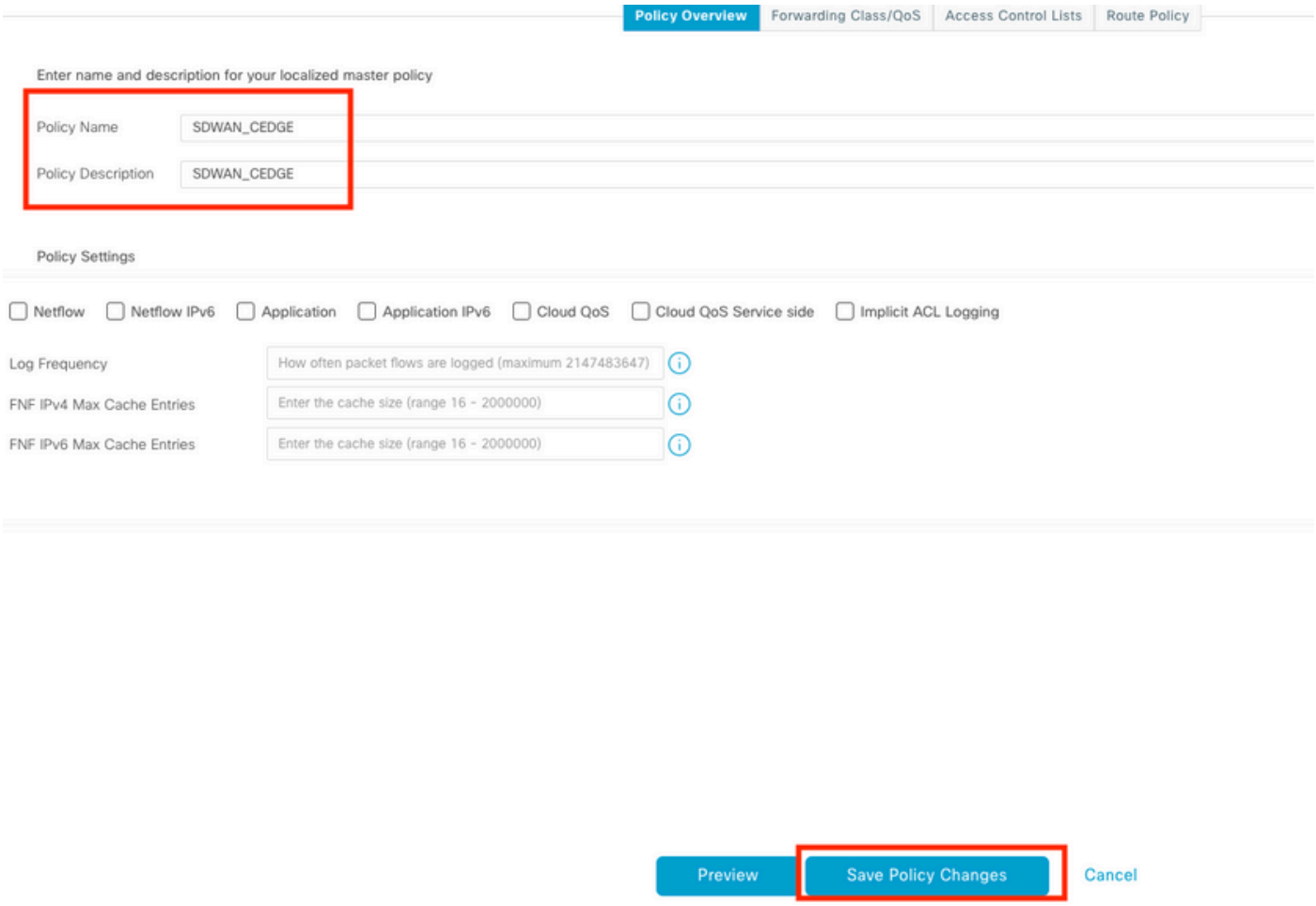
انتقل إلى التكوين > نهج مترجم > إضافة سياسة > تكوين قائمة التحكم في الوصول > إضافة سياسة الوصول إلى الجهاز > إستيراد الموجود.



حدد قائمة التحكم في الوصول (ACL) السابقة وانقر فوق إستيراد.

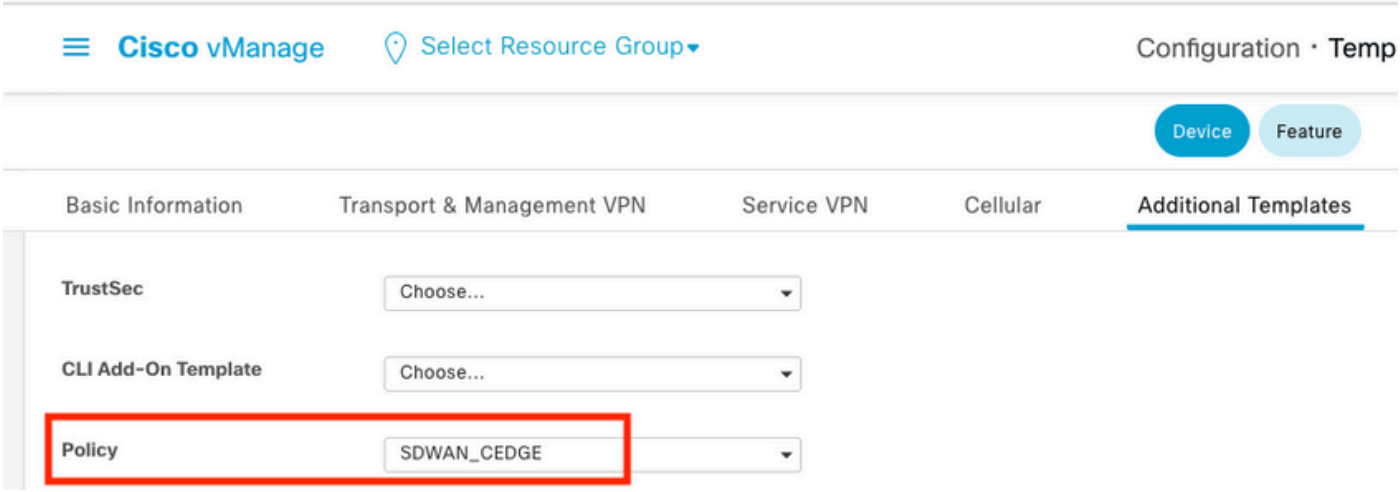


قم بإضافة اسم النهج ووصف النهج ثم انقر فوق Save Policy Changes.



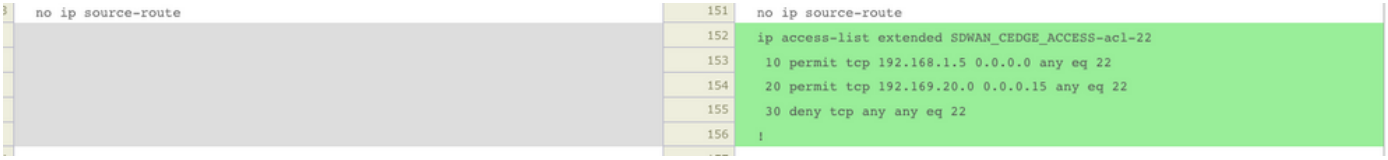
الخطوة 3. إرفاق النهج المترجم بقالب الجهاز

انتقل إلى تكوين > قالب > جهاز > تحديد الجهاز وانقر فوق > ... > تحرير > قوالب إضافية > سياسة > SDWAN_CEDGE > تحديث.

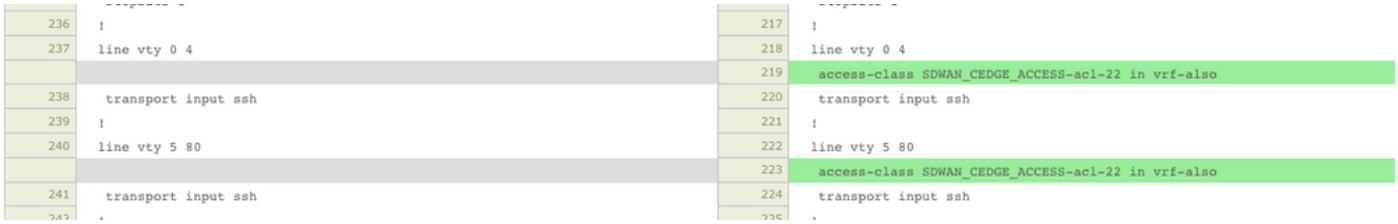


قبل أن تقوم بالضغط على القالب، يمكنك التحقق من أختلاف التكوين.

تكوين قائمة التحكم في الوصول (ACL) الجديدة



ACL مطبقة على خط vty



التحقق

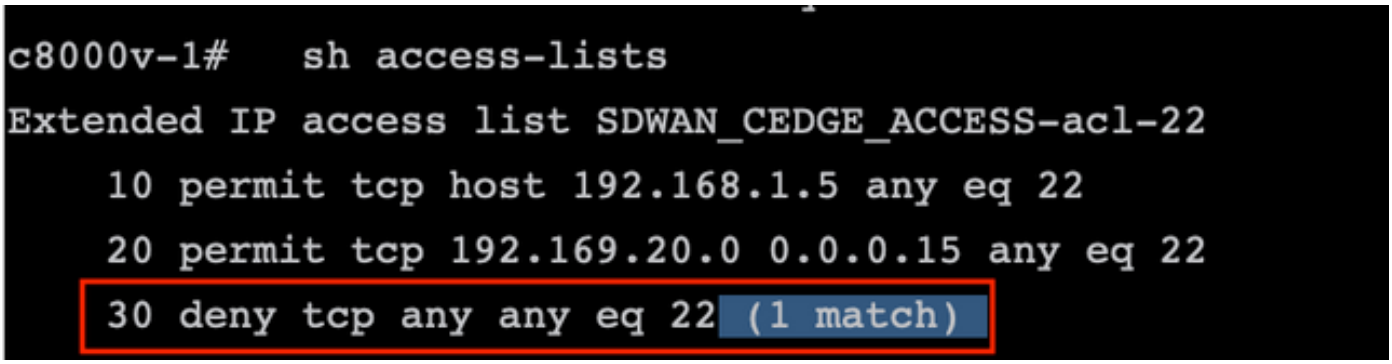
الآن يمكنك مرة أخرى إختبار وصول SSH إلى cEdge باستخدام عوامل التصفية السابقة من vManage باستخدام هذا المسار: القائمة > أدوات > الوحدة الطرفية SSH.

تمت محاولة الموجه مع SSH إلى 192.168.10.114m

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

Router#
```

إذا قمت بالتحقق من عدادات قائمة التحكم في الوصول، فيمكنك تأكيد أن Seq 30 يحتوي على تطابق واحد وتم رفض اتصال SSH.



معلومات ذات صلة

[دليل تكوين سياسات Cisco SD-WAN، Cisco IOS XE، الإصدار 17.x]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).