تكوين قائمة التحكم في الوصول (ACL) لحظر/مطابقة حركة المرور على الحواف باستخدام نهج vManage

المحتويات

المقدمة

يصف هذا المستند عملية الحظر/المطابقة في cEdge باستخدام سياسة محلية وقائمة تحكم في الوصول (ACL) .

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- شبكة المنطقة الواسعة المعرفة من برنامج Cisco (SD-WAN)
- برنامج Cisco vManage
- واجهة سطر الأوامر (CLI) cEdge

المكونات المستخدمة

يستند هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- c8000v الإصدار 17.3.3
- vManage، الإصدار 20.6.3

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الخلفية

هناك سيناريوهات مختلفة تتطلب أسلوبا محليا لحظر حركة المرور أو السماح بها أو مطابقتها. تتحكم كل طريقة في الوصول إلى الموجه أو تضمن وصول الحزم إلى الجهاز ومعالجتها.

توفر موجهات cEdge القدرة على تكوين سياسة محلية من خلال CLI أو vManage لمطابقة شروط حركة المرور وتحديد إجراء.

هذه بعض الأمثلة لخصائص النهج المحلية:

شروط المطابقة:

- نقطة كود الخدمات المميزة (DSCP)
- طول الحزمة
- البروتوكول
- بادئة البيانات المصدر
- منفذ المصدر
- بادئة بيانات الوجهة
- غاية ميناء

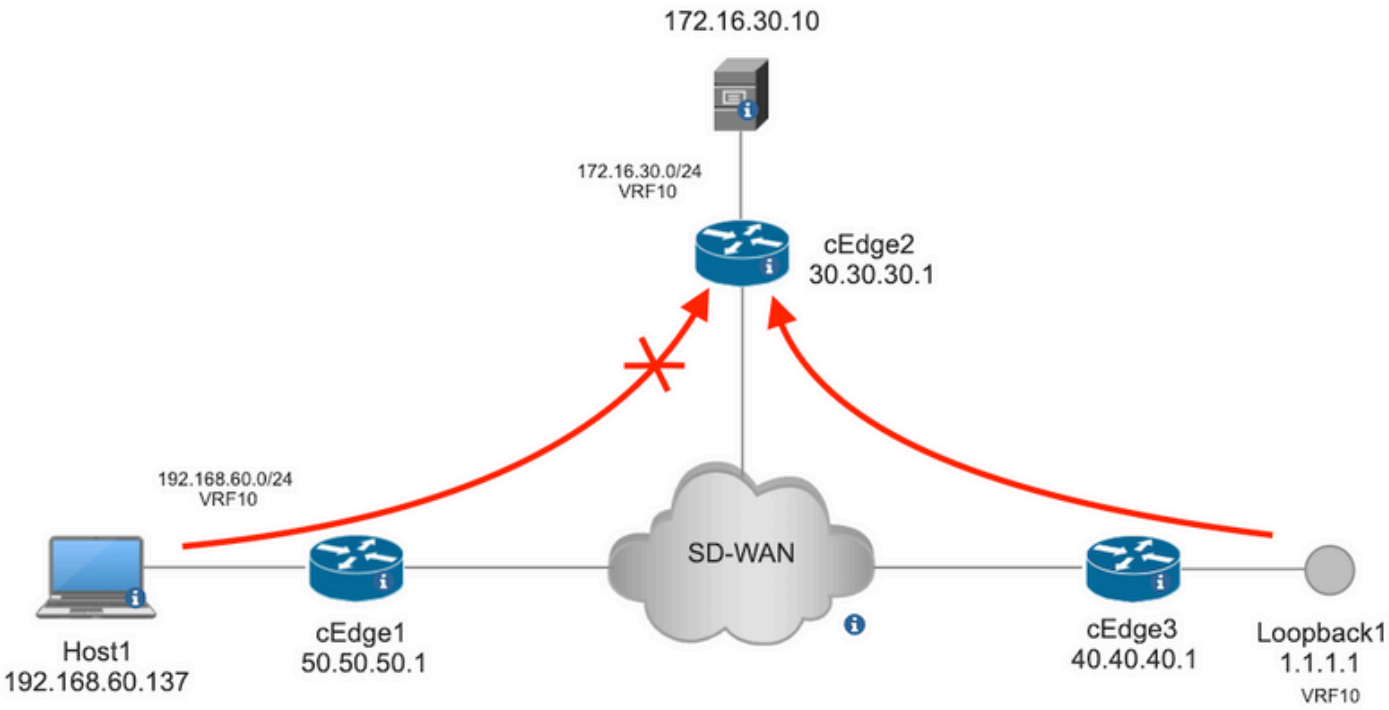
الإجراءات:

- قبول إضافي: عداد، DSCP، سجلات، nexthop، قائمة نسخ متطابق، فئة، منظم
- قطرة إضافي: عداد، سجل

التكوين

الرسم التخطيطي للشبكة

على سبيل المثال، الهدف هو حظر حركة المرور من الشبكة 192.168.20.0/24 في cEdge2 على أساس الخروج والسماح لبروتوكول ICMP من واجهة إسترجاع cEdge3.



التحقق من إختبار الاتصال من المضيف 1 إلى الخادم في cEdge2.

```
[Host2 ~]$ ping -I eth1 -c 5 172.16.30.10
PING 172.16.30.10 (172.16.30.10) from 192.168.60.137 eth1: 56(84) bytes of data.
64 bytes from 172.16.30.10: icmp_seq=1 ttl=253 time=20.6 ms
64 bytes from 172.16.30.10: icmp_seq=2 ttl=253 time=20.5 ms
64 bytes from 172.16.30.10: icmp_seq=3 ttl=253 time=20.5 ms
64 bytes from 172.16.30.10: icmp_seq=4 ttl=253 time=20.5 ms
64 bytes from 172.16.30.10: icmp_seq=5 ttl=253 time=20.5 ms

--- 172.16.30.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 20.527/20.582/20.669/0.137 ms
```

التحقق من إختبار الاتصال من cEdge3 إلى الخادم في cEdge2.

```
cEdge3# ping vrf 10 172.16.30.10 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.10, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/73/76 ms
```

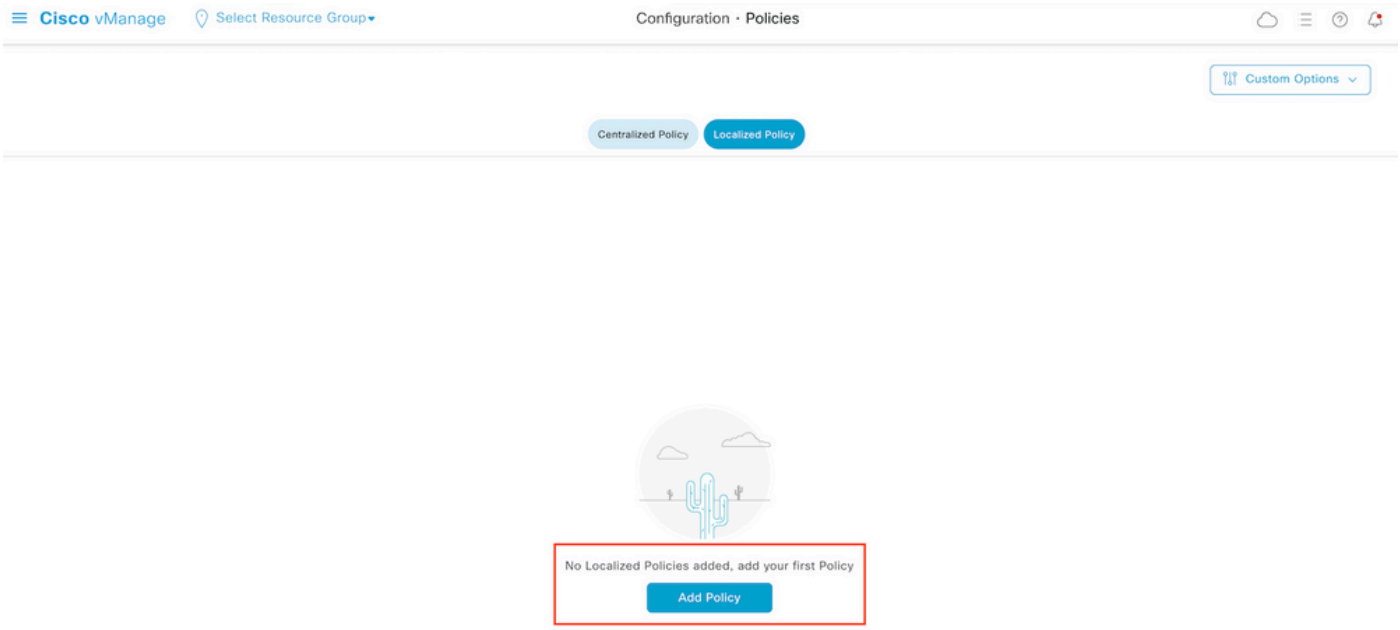
الشروط المسبقة:

- يجب أن يحتوي cEdge2 على قالب جهاز مرفق.
- يجب أن يكون لدى كافة CEdges إتصالات تحكم نشطة.
- كل cEdges ينبغي يتلقى ثنائي إتجاه forwarding كشف (BFD) جلسة نشط.
- يجب أن تحتوي جميع الوحدات على مسارات بروتوكول الإدارة المتفرعة (OMP) للوصول إلى الشبكات الجانبية للخدمة VPN10.

التكوينات

الخطوة 1. أضف النهج المترجم.

في برنامج Cisco vManage، انتقل إلى **Configuration > Policies > Localized Policy**. انقر **Add Policy**



الخطوة 2. قم بإنشاء مجموعات مصالح للمطابقة المقصودة.

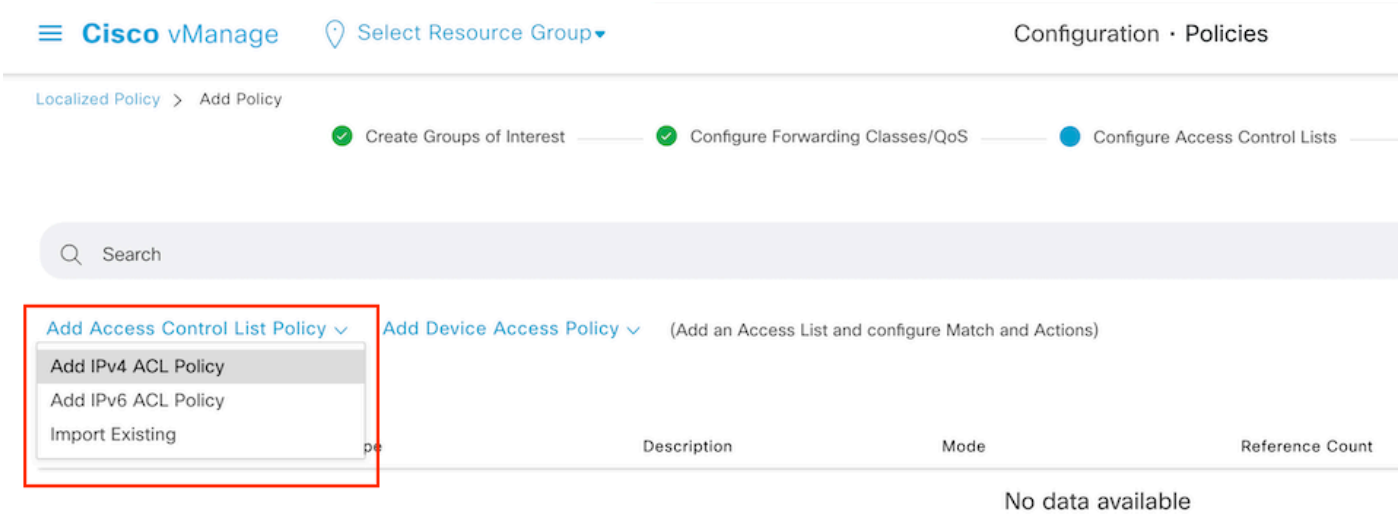
انقر **Data Prefix** في القائمة اليسرى وحدد **New Data Prefix List.**

قم بإعطاء اسم لحالة التطابق، وقم بتعريف بروتوكول الإنترنت، وإضافة بادئة بيانات.

انقر **Add** ومن ثم **Next** حتى **Configure Access Control List** معروض.

الخطوة 3. قم بإنشاء قائمة الوصول لتطبيق حالة المطابقة.

تحديد **Add IPv4 ACL Policy** من **Add Access Control List Policy** قائمة منسدلة.

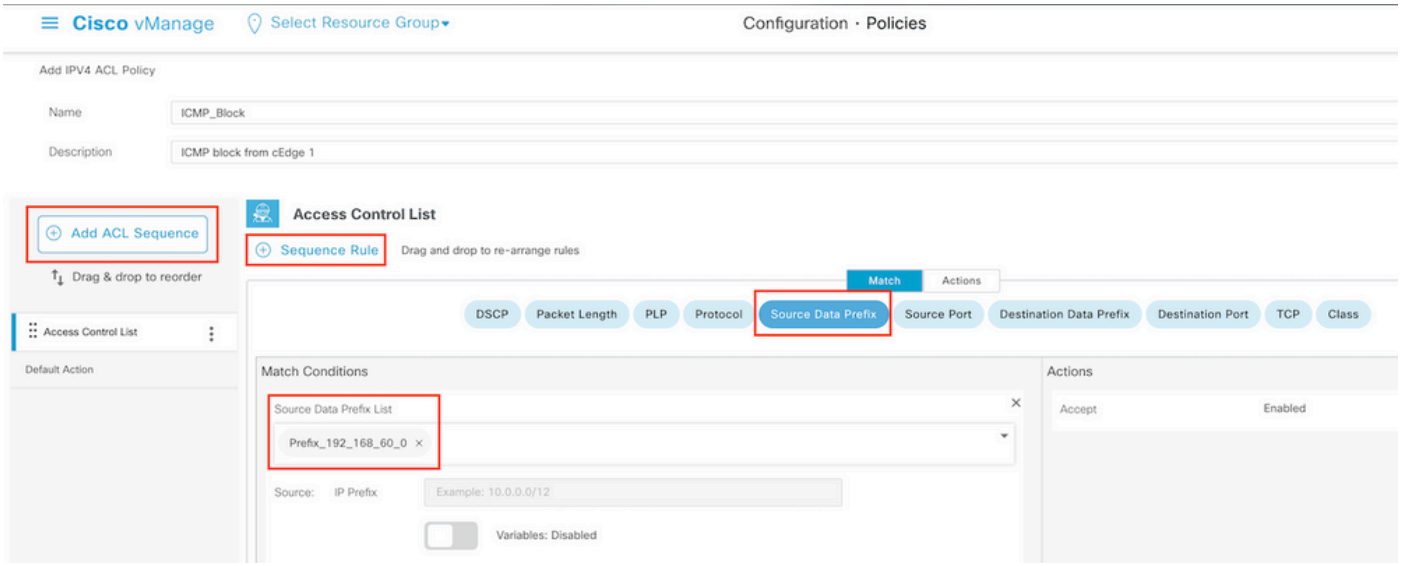


ملاحظة: يستند هذا المستند إلى سياسة قائمة التحكم في الوصول ويجب عدم الخلط بينه وبين نهج الوصول إلى الجهاز. يعمل نهج الوصول إلى الجهاز في خطة التحكم للخدمات المحلية مثل بروتوكول إدارة الشبكة البسيط (SNMP) وقشرة مأخذ التوصيل الآمنة (SSH)، فقط، في حين أن سياسة قائمة التحكم في الوصول مرنة للخدمات المختلفة وشروط المطابقة.

الخطوة 4. تحديد تسلسل قائمة التحكم في الوصول (ACL)

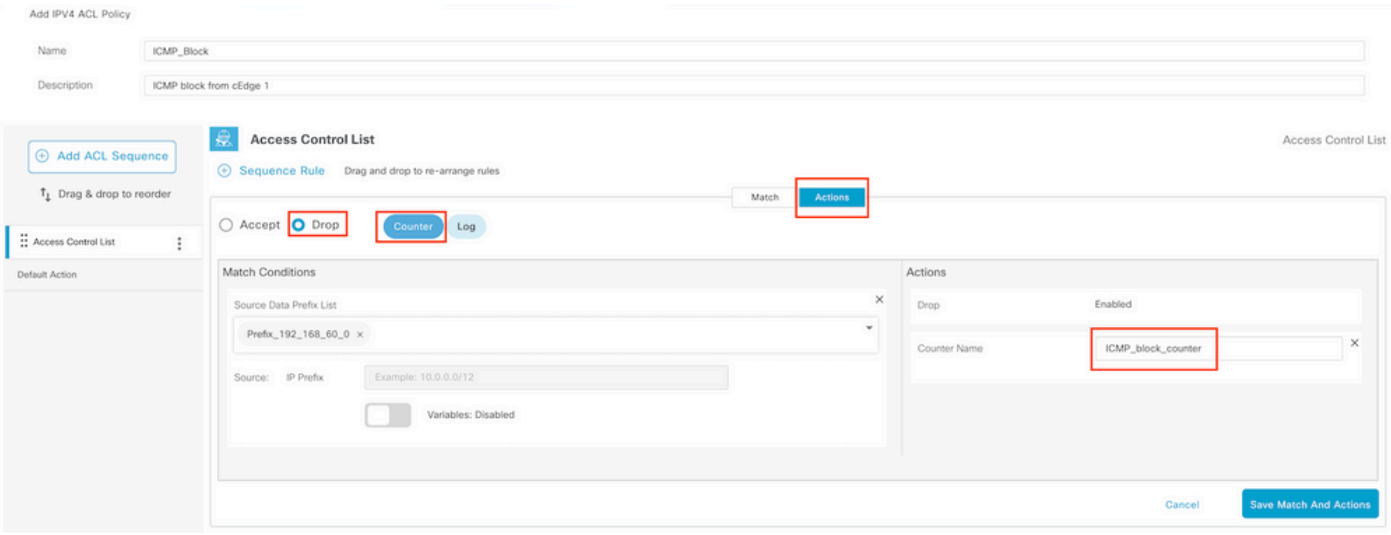
في شاشة تكوين قائمة التحكم في الوصول (ACL)، قم بتسمية قائمة التحكم في الوصول (ACL) وتقديم وصف. انقر **Add ACL Sequence** ومن ثم **Sequence Rule.**

في قائمة شروط المطابقة، حدد **Source Data Prefix** ثم أختر قائمة بادئات البيانات من **Source Data Prefix List** القائمة المنسدلة.

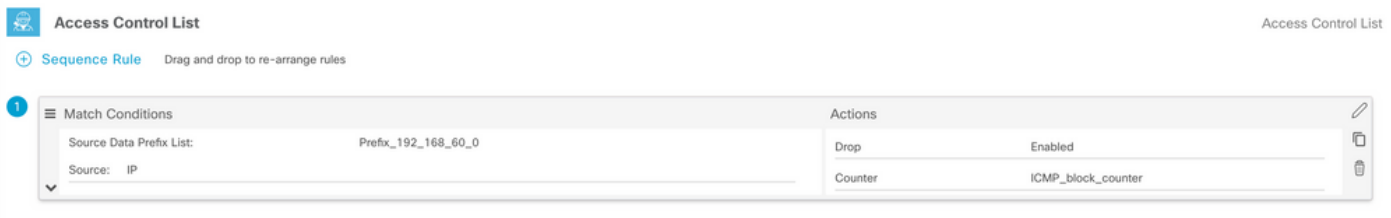


الخطوة 5. قم بتعريف الإجراء الخاص بالتسلسل وقم بتسميته

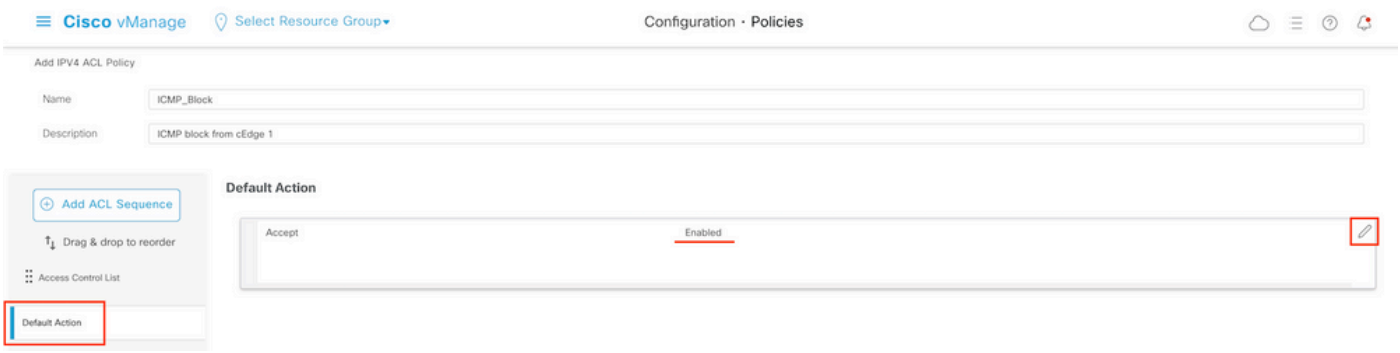
انتقل إلى **Action** تحديد **Drop**, وانقر فوق **Save Match** و **Actions**.



ملاحظة: هذا الإجراء مرتبط بشكل حصري بالتسلسل نفسه، وليس بالسياسة الكاملة المترجمة.



الخطوة 6. في القائمة اليسرى، حدد **Default Action**, طقطقة **Edit**, وتختار **Accept**.

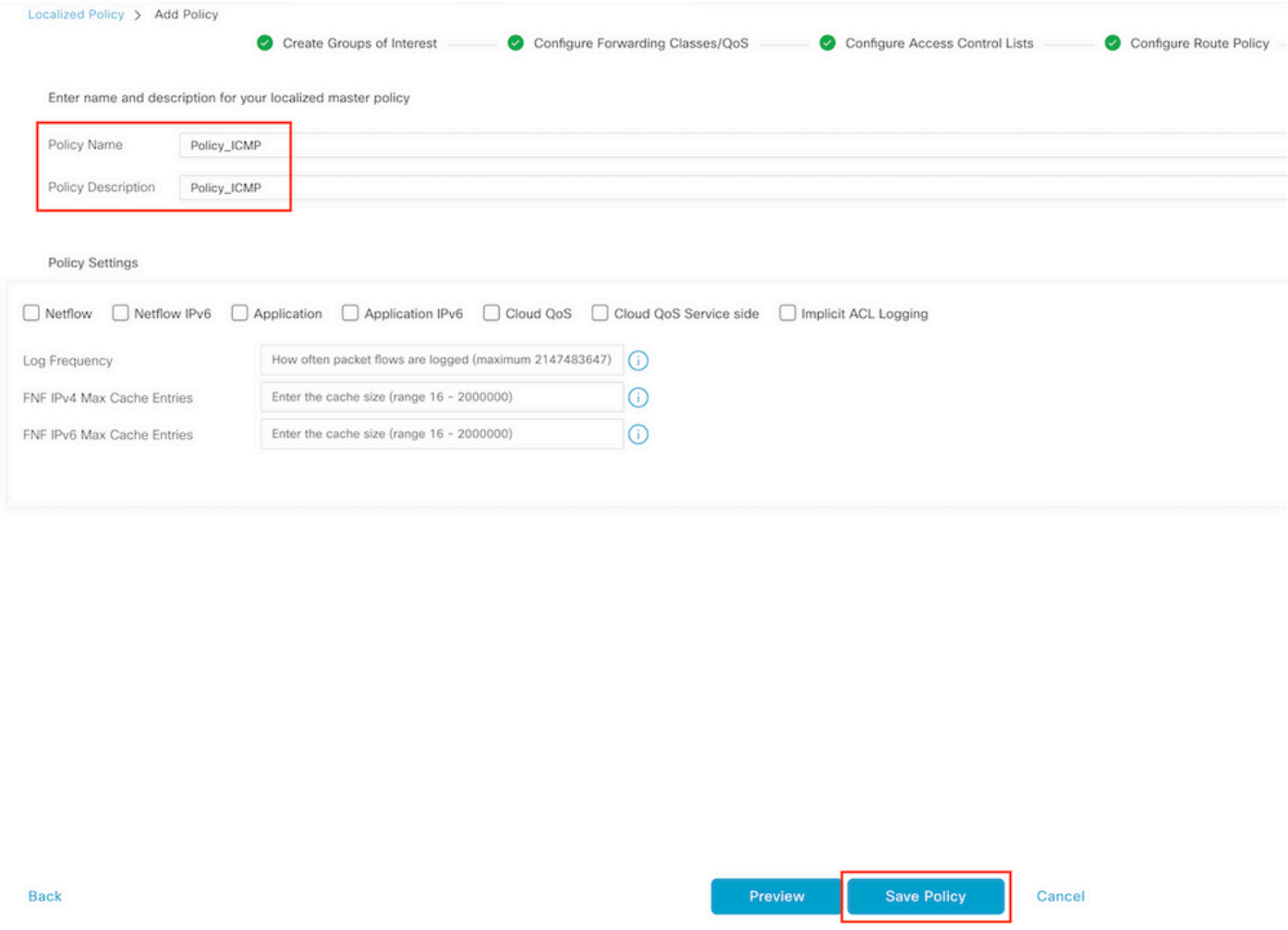


ملاحظة: يقع هذا الإجراء الافتراضي في نهاية النهج المعرب. لا تستخدم **drop**، وإلا، يمكن أن تتأثر حركة مرور البيانات بالكامل وتتسبب في انقطاع الشبكة.

انقر **Save Access Control List Policy.**

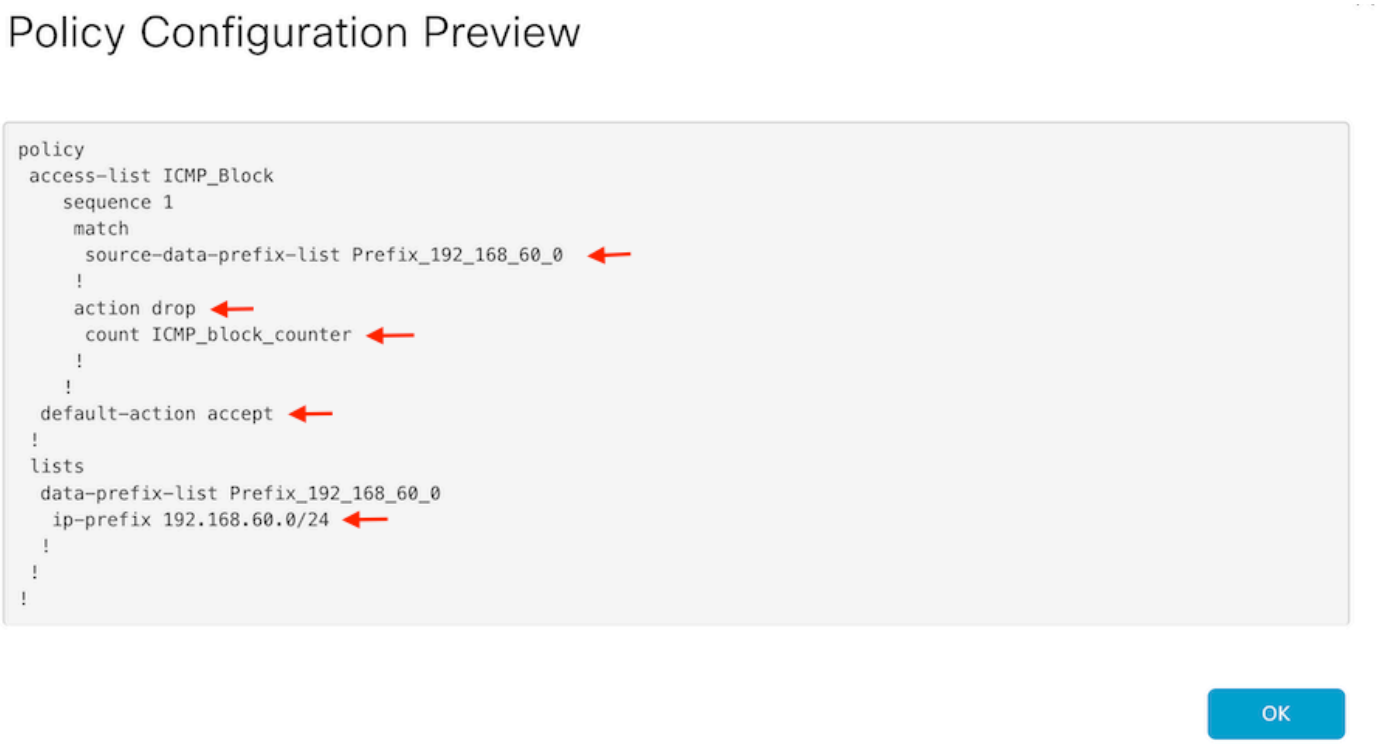
الخطوة 7. قم بتسمية النهج

انقر **Next** حتى **Policy Overview** و سموها. أترك القيم الأخرى فارغة. انقر **Save Policy**



للتأكد من صحة النهج، انقر فوق **Preview**.

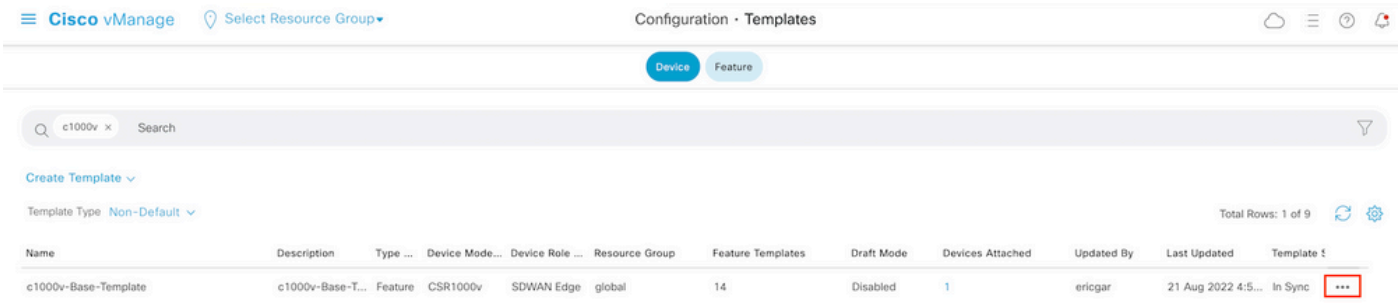
تحقق من صحة التسلسل والعناصر في النهج.



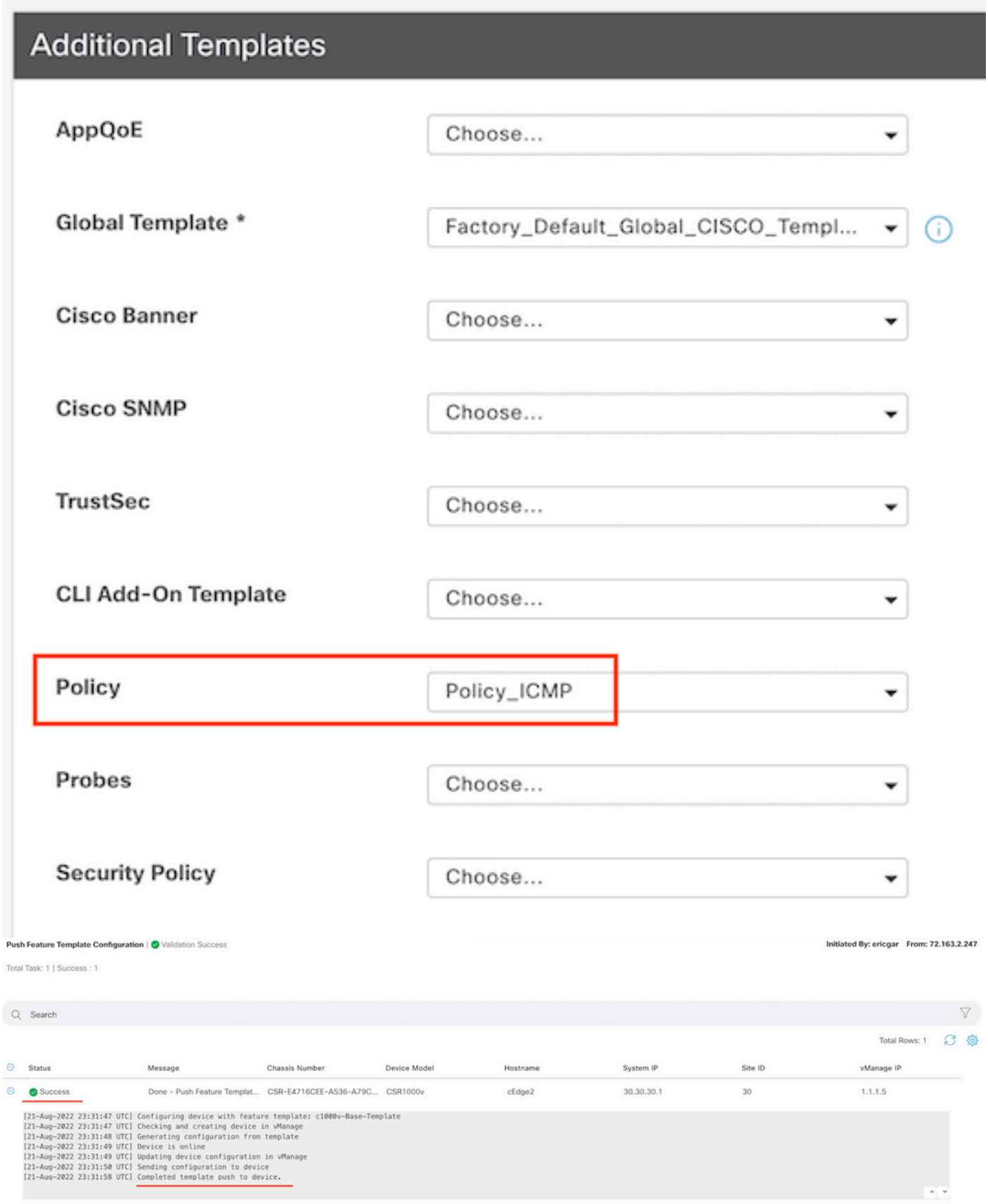
انسخ اسم قائمة التحكم في الوصول (ACL). وهذا مطلوب في خطوة أخرى.

الخطوة 8. إقران النهج المترجم بقالب الجهاز.

حدد موقع قالب الجهاز المرفق بالموجه، وانقر النقاط الثلاث، وانقر فوق **Edit**.



تحديد **Additional Templates** وأضف النهج المترجم إلى حقل النهج وانقر فوق **Update > Next > Configure Devices** لدفع التكوين إلى cEdge.



ملاحظة: عند هذه النقطة، يقوم vManage بإنشاء قائمة التحكم في الوصول (ACL) استنادا إلى السياسة التي تم إنشاؤها ودفع التغييرات إلى CEdge، رغم أنها غير مرتبطة بأي واجهة. لذلك، ليس لها أي تأثير في تدفق حركة المرور.

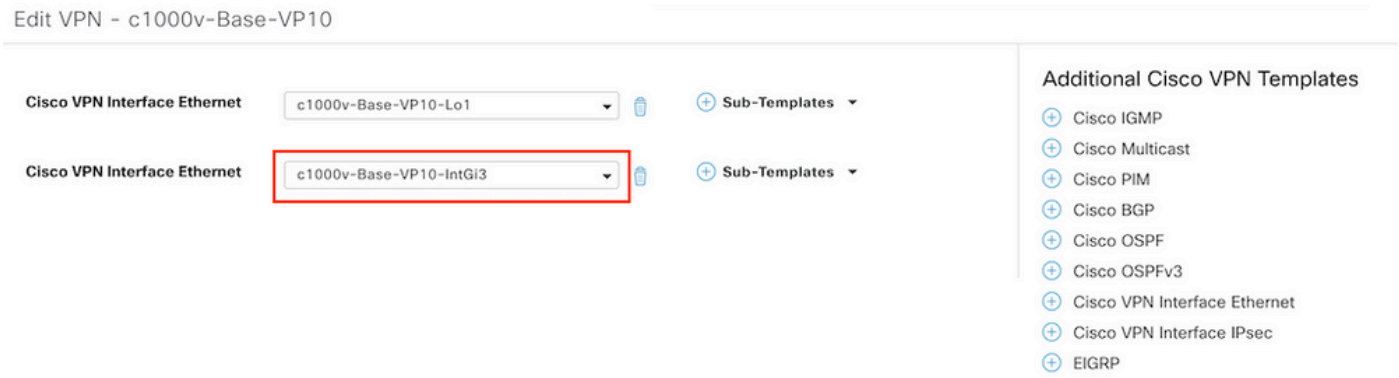
الخطوة 9. حدد قالب المميزات للواجهة حيث يتم التخطيط لتطبيق الإجراء على حركة المرور في قالب الجهاز.

من المهم تحديد موقع قالب الميزة حيث يلزم حظر حركة المرور.

في هذا المثال، تنتمي واجهة GigabitEthernet3 إلى الشبكة الخاصة الظاهرية 3 (شبكة إعادة التوجيه الظاهرية 3).

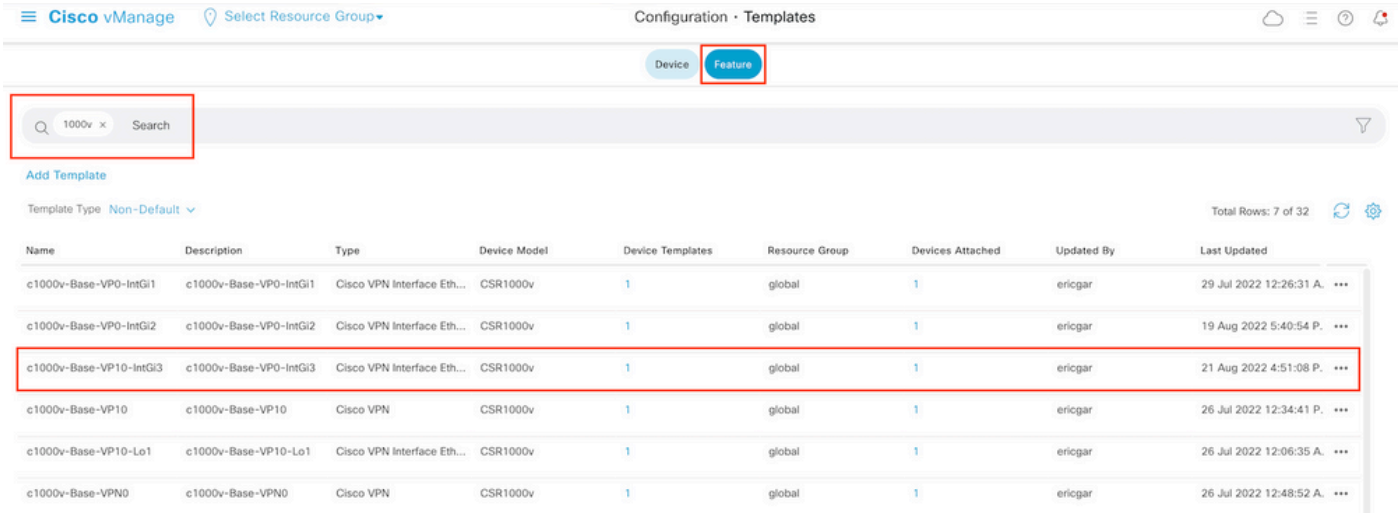
انتقل إلى قسم شبكة VPN للخدمة وانقر **Edit** للوصول إلى قوالب الشبكة الخاصة الظاهرية (VPN).

في هذا المثال، تحتوي واجهة GigabitEthernet3 على قالب ميزة c1000v-Base-VP10-IntGi3 المرفق.

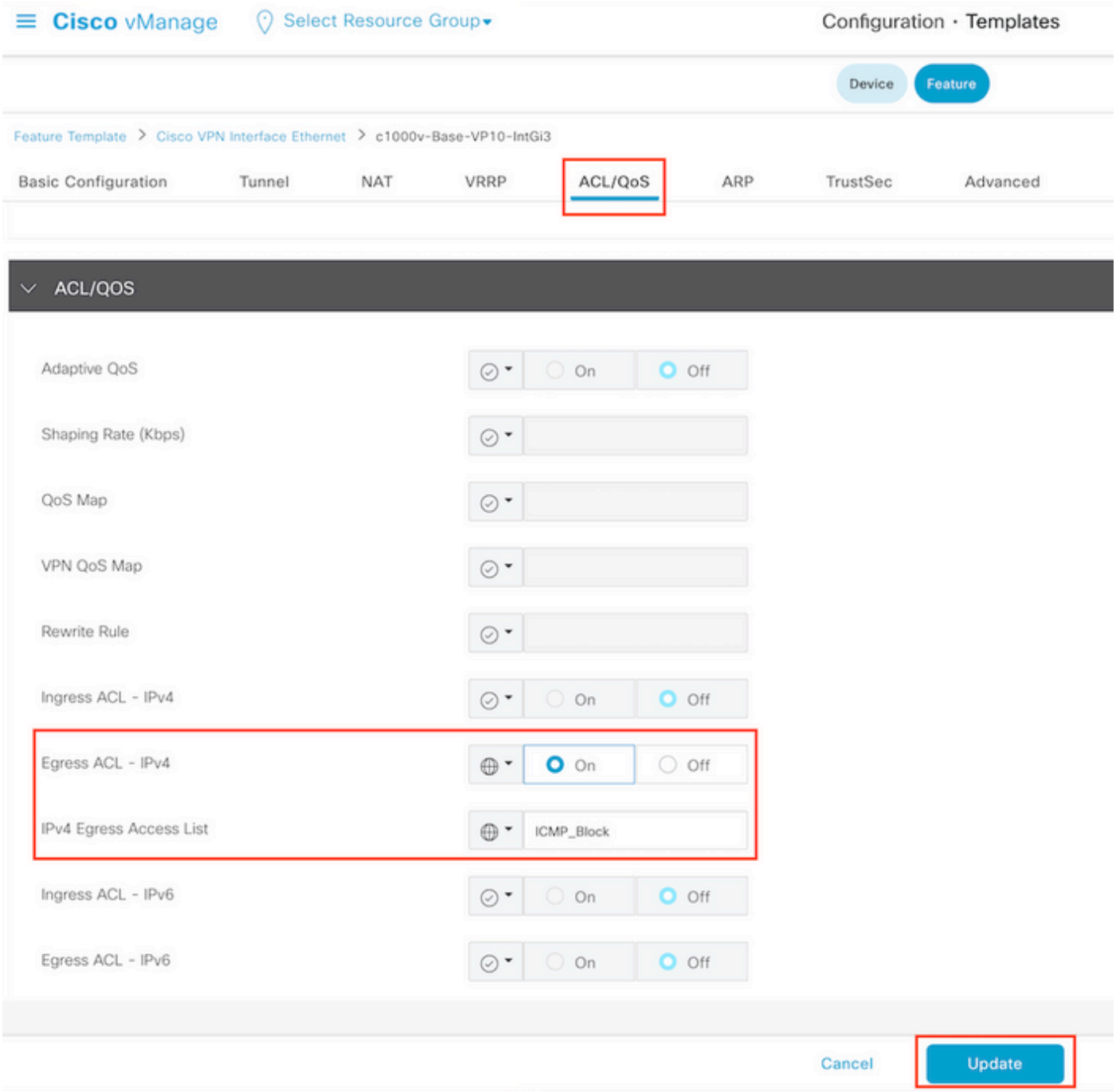


الخطوة 10. أرفق اسم قائمة التحكم في الوصول (ACL) بالواجهة.

انتقل إلى **Configuration > Templates > Feature.** تصفية القوالب وانقر **Edit**



انقر **ACL/QoS** وتمكين إتجاه حركة المرور للحجب. اكتب اسم قائمة التحكم في الوصول (ACL) المنسوخ في الخطوة 7. انقر **Update** ودفع التغييرات.



ملاحظة: تعمل أيضا عملية إنشاء السياسة المحلية هذه ل vEdges لأن بنية سياسة vManage هي نفسها لكل من البنيتين. يتم توفير الجزء المختلف بواسطة قالب الجهاز الذي يقوم بإنشاء بنية تكوين متوافقة مع cEdge أو vEdge.

التحقق من الصحة

الخطوة 1. التحقق من التكوينات بشكل صحيح في الموجه

```
cEdge2# show sdwan running-config policy
policy
lists
  data-prefix-list Prefix_192_168_60_0 <<<<<<<<<
   ip-prefix 192.168.60.0/24 <<<<<<<<<
```

```
  !
!
access-list ICMP_Block
  sequence 1
   match
    source-data-prefix-list Prefix_192_168_60_0 <<<<<<<<<
   !
   action drop <<<<<<<<<
    count ICMP_block_counter <<<<<<<<<
   !
  !
  default-action accept <<<<<<<<<
!
!

cEdge2# show sdwan running-config sdwan | section interface GigabitEthernet3
interface GigabitEthernet3
  access-list ICMP_Block out
```

الخطوة 2. من Host1 الموجود في شبكة الخدمة الخاصة ب cEdge1، إرسال 5 رسائل إختبار الاتصال إلى الخادم في cEdge2

```
[Host1 ~]$ ping -I eth1 -c 5 172.16.30.10
PING 172.16.30.10 (172.16.30.10) from 192.168.60.137 eth1: 56(84) bytes of data.
--- 172.16.30.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4088ms
```

ملاحظة: على سبيل المثال، المضيف 1 هو جهاز لينوكس. يمثل "-I" الواجهات التي يغادر فيها إختبار الاتصال الموجه ويمثل "-c" عدد رسائل إختبار الاتصال.

الخطوة 3. من cEdge2، التحقق من عدادات قائمة التحكم في الوصول (ACL)

```
cEdge2# show sdwan policy access-list-counters
NAME COUNTER NAME PACKETS BYTES
------------------------------------------------------------------------------
ICMP_Block ICMP_block_counter 5     610
default_action_count 0 0
```

طابق العداد خمس (5) حزم جاءت من الشبكة 192.168.60.0/24، كما هو محدد في السياسة.

الخطوة 4. من cEdge3، قم بإرسال 4 رسائل إختبار اتصال إلى الخادم 172.16.30.10

```
cEdge3# ping vrf 10 172.16.30.10 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.10, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/76/88 ms
```

مرت الحزم عبر الموجه إلى الخادم لأن الشبكة مختلفة (في هذه الحالة هي 1.1.1.1/32) والوجود في حالة مطابقة لها في السياسة.

الخطوة 5. تحقق من عدادات قائمة التحكم في الوصول في cEdge2 مرة أخرى.

```
cEdge2# show sdwan policy access-list-counters
NAME COUNTER NAME PACKETS BYTES
------------------------------------------------------------------------------
```

```
ICMP_Block ICMP_block_counter 5     610
default_action_count  5     690
```

زاد عداد default_action_count مع 5 حزم مرسلة بواسطة cEdge3.

لمسح العدادات، قم بتشغيل **clear sdwan policy access-list** erasecat4000_flash:.

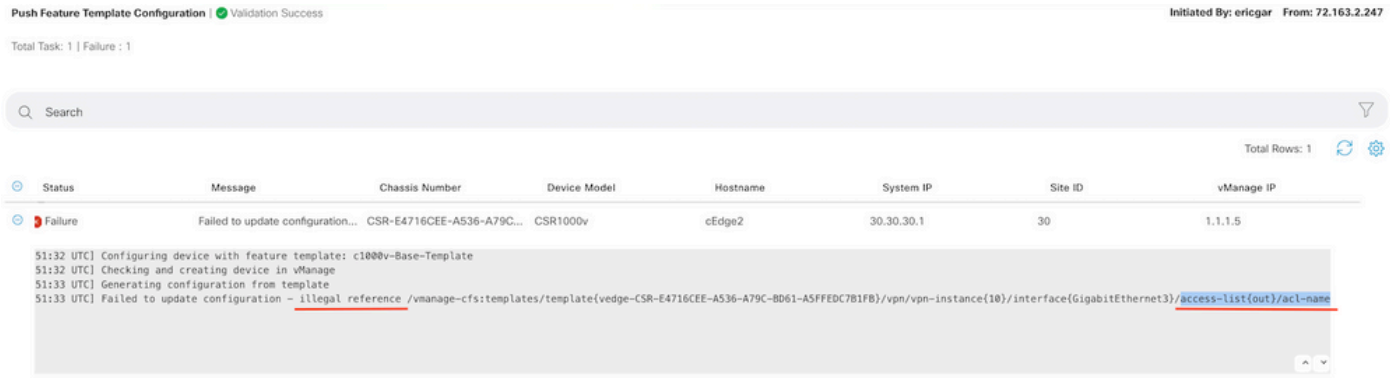
أوامر للتحقق في vEdge

```
show running-config policy
show running-config
show policy access-list-counters
clear policy access-list
```

استكشاف الأخطاء وإصلاحها

خطأ: مرجع غير قانوني لاسم قائمة التحكم بالوصول (ACL) في الواجهة

يجب إرفاق النهج الذي يحتوي على قائمة التحكم في الوصول (ACL) أولا بقالب الجهاز. بعد ذلك، يمكن تحديد اسم قائمة التحكم في الوصول (ACL) في قالب جهاز المميزة للواجهة.



معلومات ذات صلة

- دليل تكوين سياسات Cisco SD-WAN، Cisco IOS XE، الإصدار 17.x
- الدعم التقني والمستندات - Cisco Systems

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).