Configurazione dell'ACL per bloccare/associare il traffico sui bordi con criteri vManage

Sommario

Introduzione

In questo documento viene descritto il processo di blocco/corrispondenza in un cEdge con un criterio localizzato e un Access Control List (ACL).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- Cisco vManage
- CLI (Command Line Interface) cEdge

Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

- c800v versione 17.3.3
- vManage versione 20.6.3

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.

Sfondo

Esistono diversi scenari che richiedono un metodo locale per bloccare, autorizzare o associare il traffico. Ogni metodo controlla l'accesso al router o assicura che i pacchetti arrivino al dispositivo e vengano elaborati.

I router cEdge consentono di configurare un criterio localizzato tramite CLI o vManage per soddisfare le condizioni del traffico e definire un'azione.

Di seguito sono riportati alcuni esempi di caratteristiche localizzate dei criteri:

Condizioni di corrispondenza:

- DSCP (Differentiated Services Code Point)
- Lunghezza pacchetto
- Protocollo
- Prefisso dati di origine
- Porta di origine
- Prefisso dati di destinazione
- Porta di destinazione

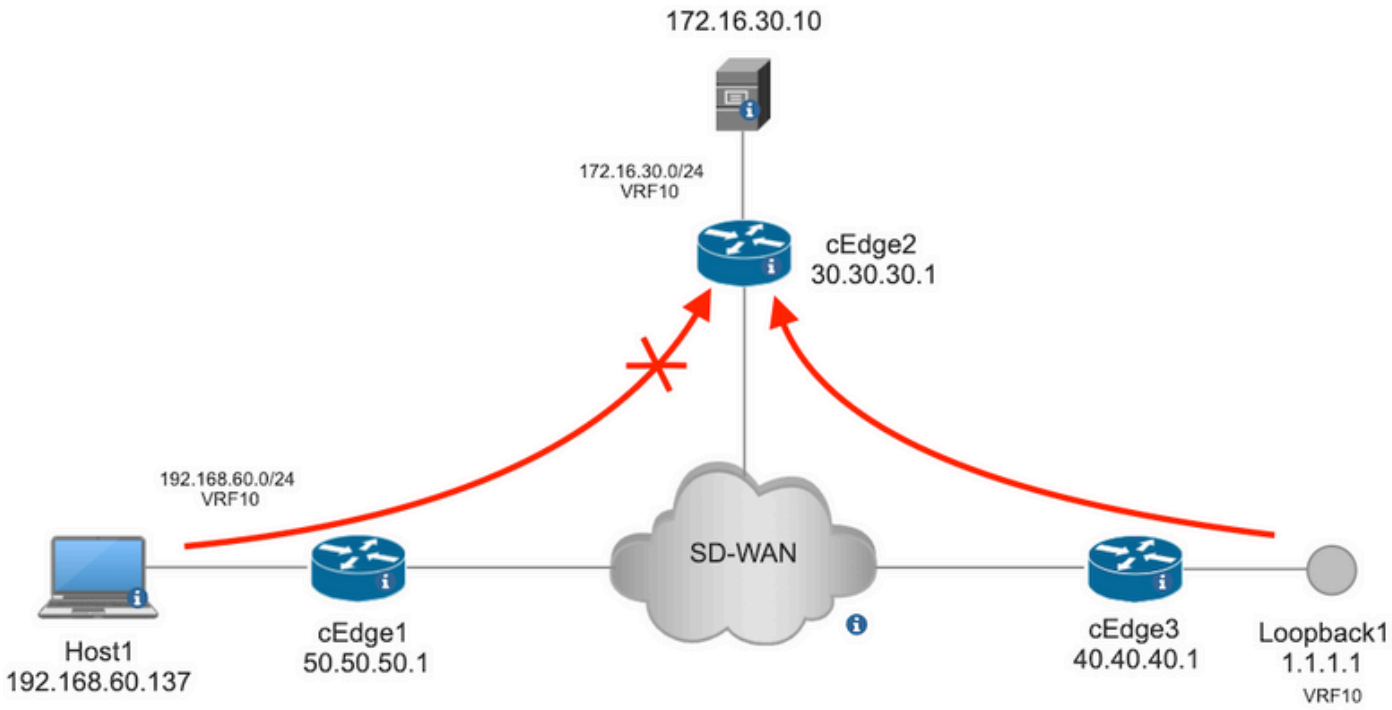
Azioni:

- Accetta Altro: contatore, DSCP, registri, nexthop, elenco mirror, classe, policer
- Drop Altro: contatore, registro

Configurazione

Esempio di rete

Per questo esempio, l'intenzione è bloccare il traffico proveniente dalla rete 192.168.20.0/24 in cEdge2 in uscita e autorizzare l'ICMP dall'interfaccia di loopback cEdge3.



Eseguire il ping della verifica da Host1 a Server in 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
```

Eseguire il ping della verifica da cEdge3 al server in 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
```

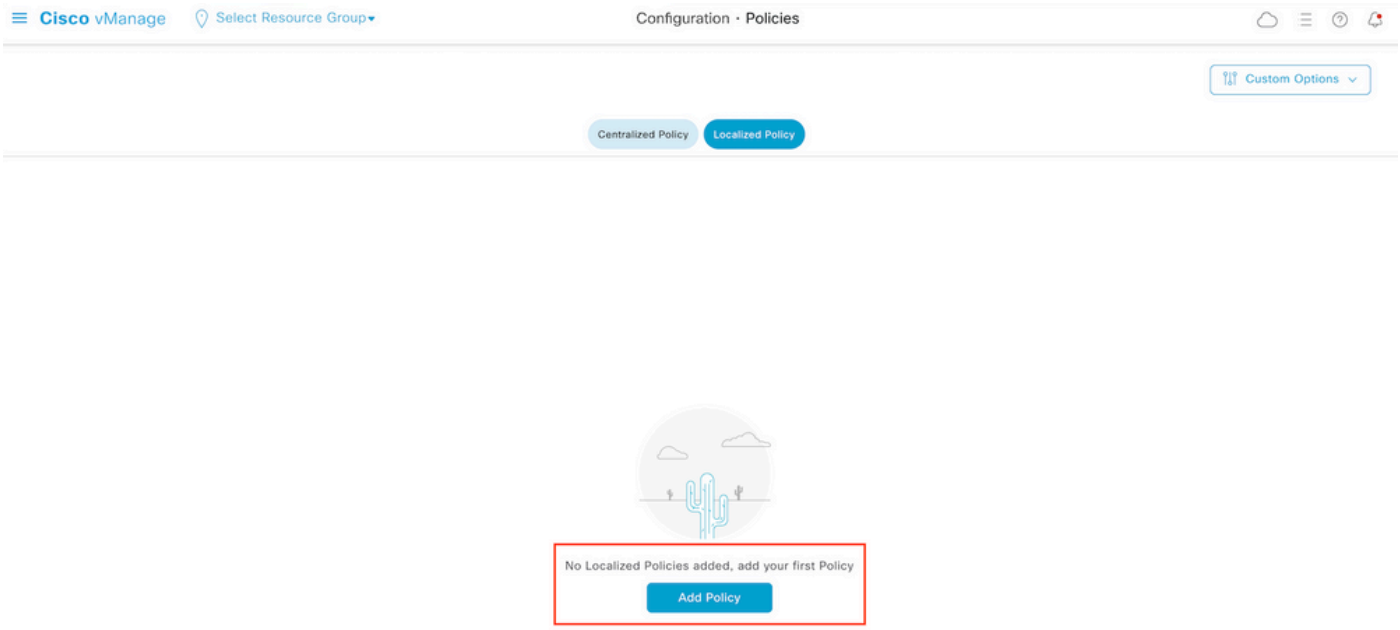
Condizioni preliminari:

- a cEdge2 deve essere associato un modello di dispositivo.
- Tutti gli spigoli devono avere connessioni di controllo attive.
- Tutti i bordi devono avere sessioni BFD (Bidirectional Forwarding Detection) attive.
- Tutti i nodi devono avere route OMP (Overlay Management Protocol) per raggiungere le reti lato VPN10 del servizio.

Configurazioni

Passaggio 1. Aggiungere il criterio localizzato.

In Cisco vManage, passare a **Configuration > Policies > Localized Policy**. Clic **Add Policy**

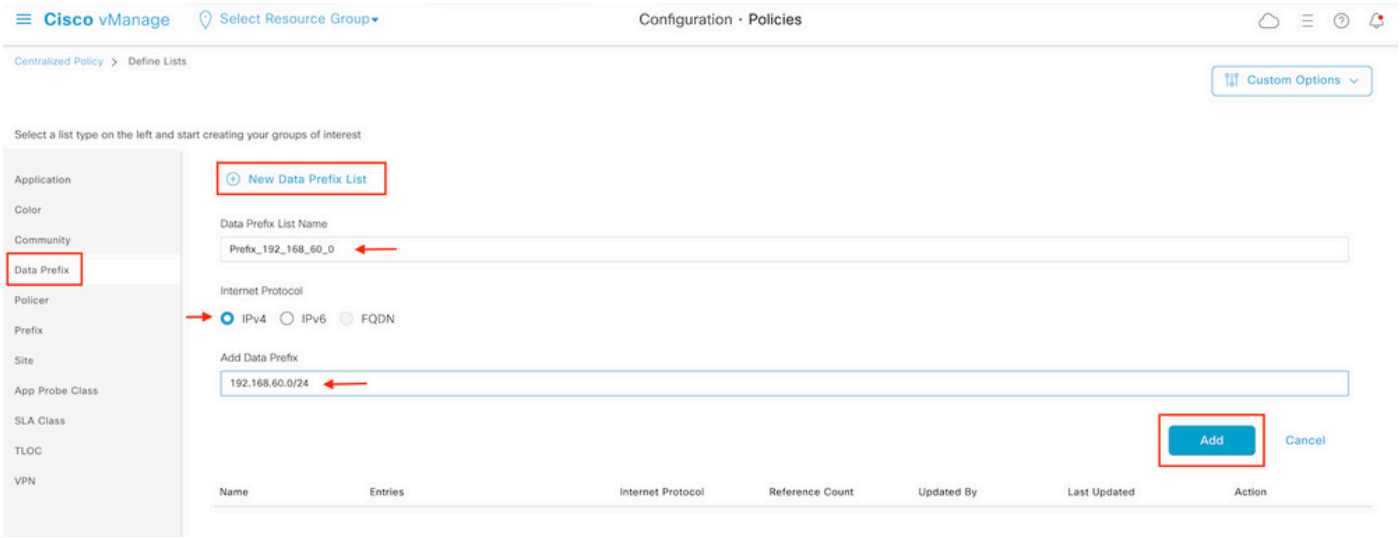


Passaggio 2. Creare i gruppi di interesse per la corrispondenza desiderata.

Clic **Data Prefix** nel menu a sinistra e selezionare **New Data Prefix List.**

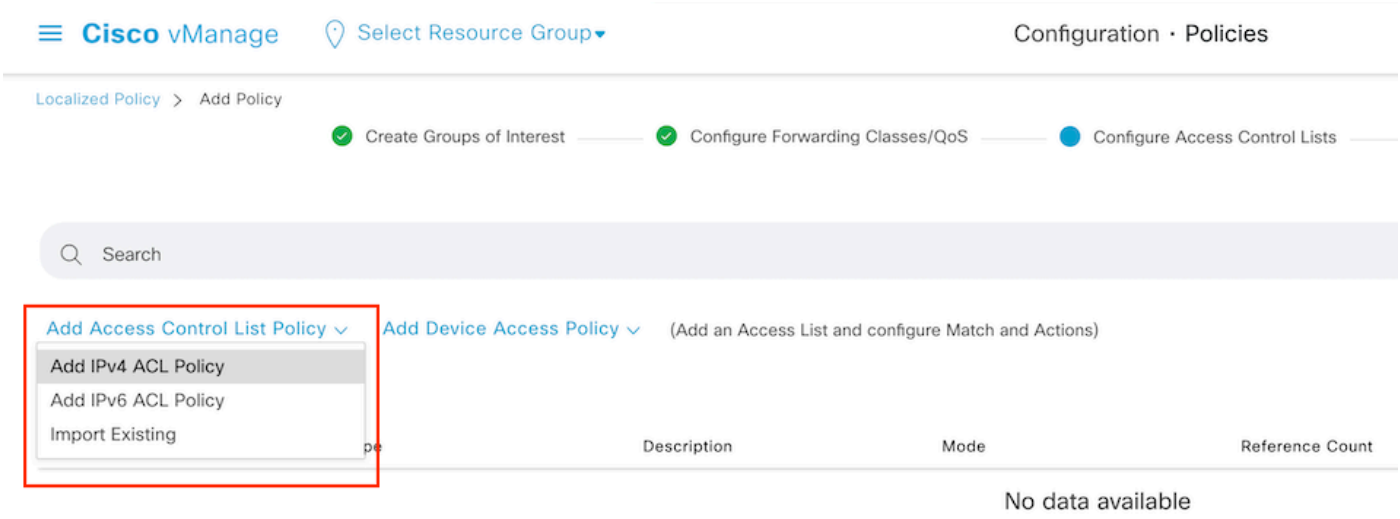
Assegnare un nome alla condizione di corrispondenza, definire il protocollo Internet e aggiungere un prefisso dati.

Clic **Add** e poi **Next** fino al **Configure Access Control List** viene visualizzato.



Passaggio 3. Creare l'elenco degli accessi per applicare la condizione di corrispondenza.

Seleziona **Add IPv4 ACL Policy** dal **Add Access Control List Policy** menu a discesa.

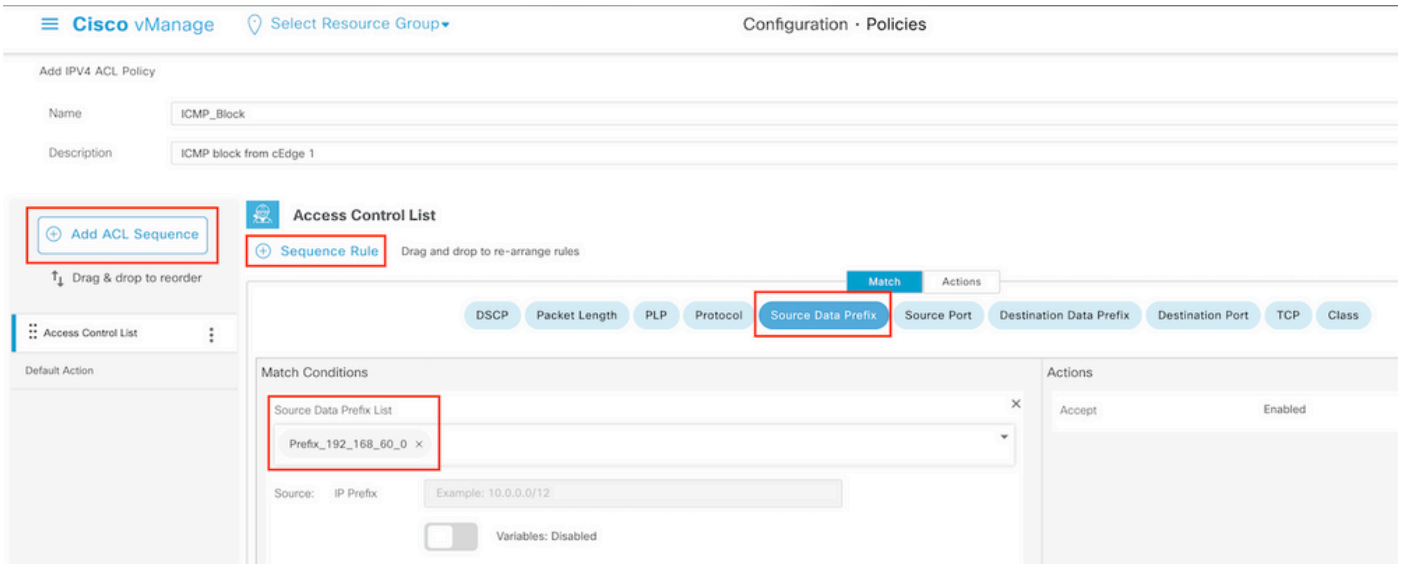


Nota: Questo documento è basato sui criteri dell'elenco di controllo di accesso e non deve essere confuso con i criteri di accesso alle periferiche. I criteri di accesso ai dispositivi agiscono solo nel piano di controllo per i servizi locali, ad esempio SNMP (Simple Network Management Protocol) e SSH (Secure Socket Shell), mentre i criteri degli elenchi di controllo di accesso sono flessibili per servizi diversi e soddisfano le condizioni.

Passaggio 4. Definizione della sequenza ACL

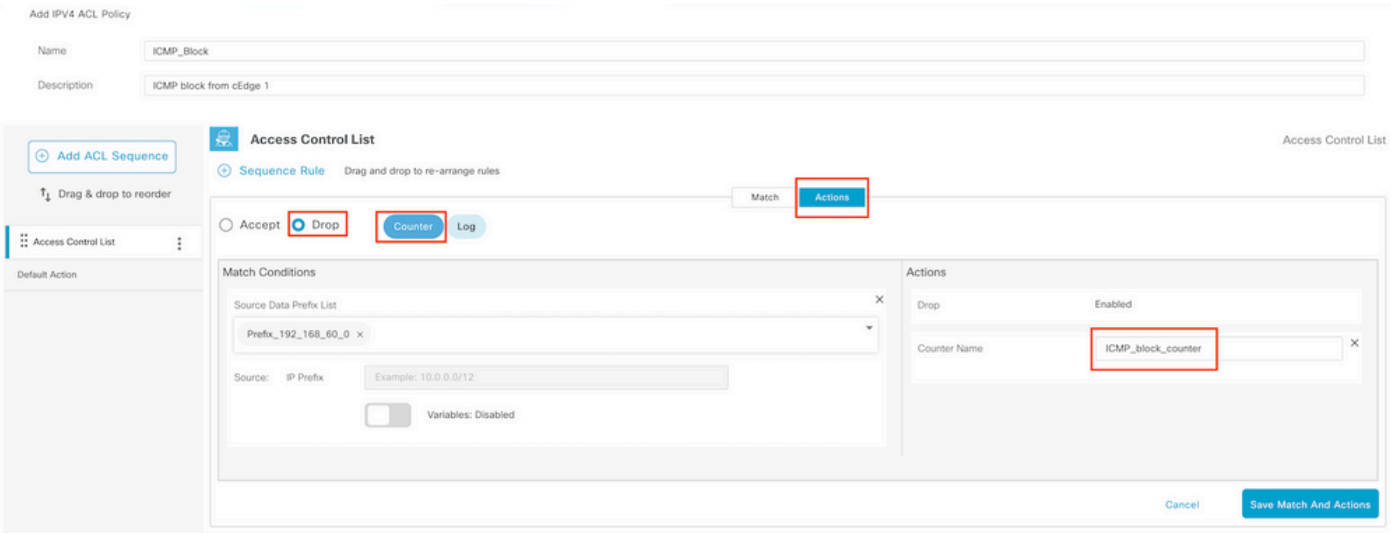
Nella schermata di configurazione dell'ACL, assegnare un nome all'ACL e fornire una descrizione. Clic **Add ACL Sequence** e poi **Sequence Rule.**

Nel menu Condizioni di corrispondenza, selezionare **Source Data Prefix** e quindi scegliere l'elenco di prefissi dei dati dal **Source Data Prefix List** menu a discesa.

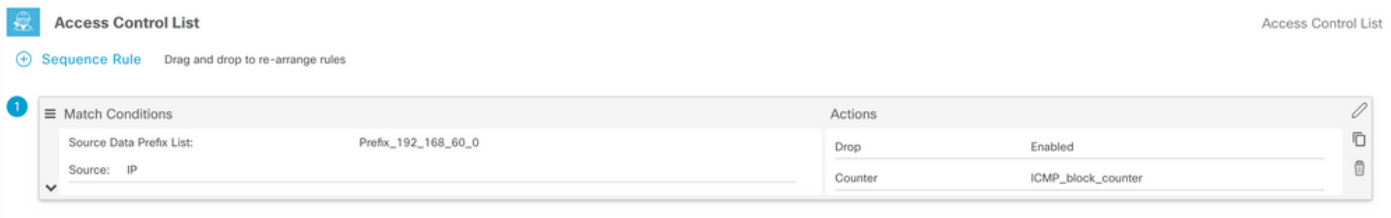


Passaggio 5. Definire l'azione per la sequenza e denominarla

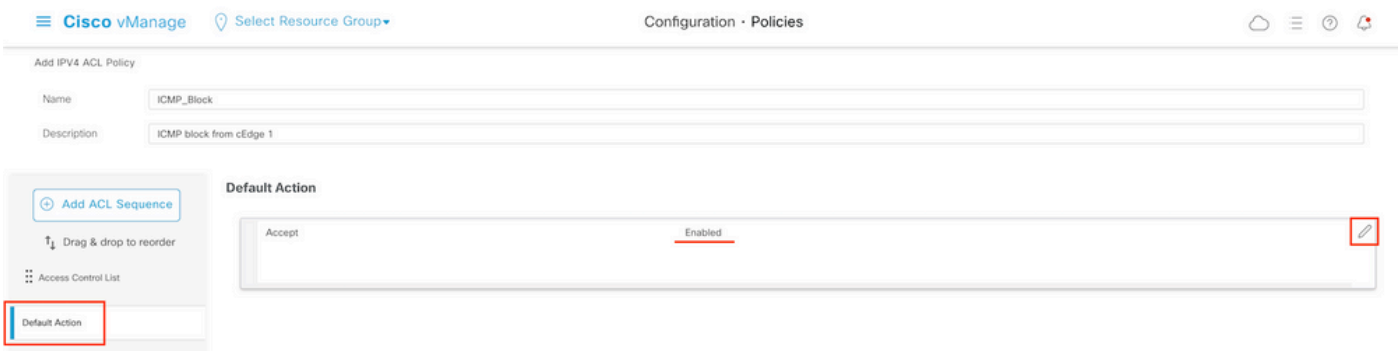
Passa a **Action** selezionare **Drop**, e fare clic su **Save Match** e **Actions**.



Nota: Questa azione è associata in modo esclusivo alla sequenza stessa, non al criterio localizzato completo.



Passaggio 6. Nel menu a sinistra, selezionare **Default Action** ,fare clic **Edit**, e scegliere **Accept**.

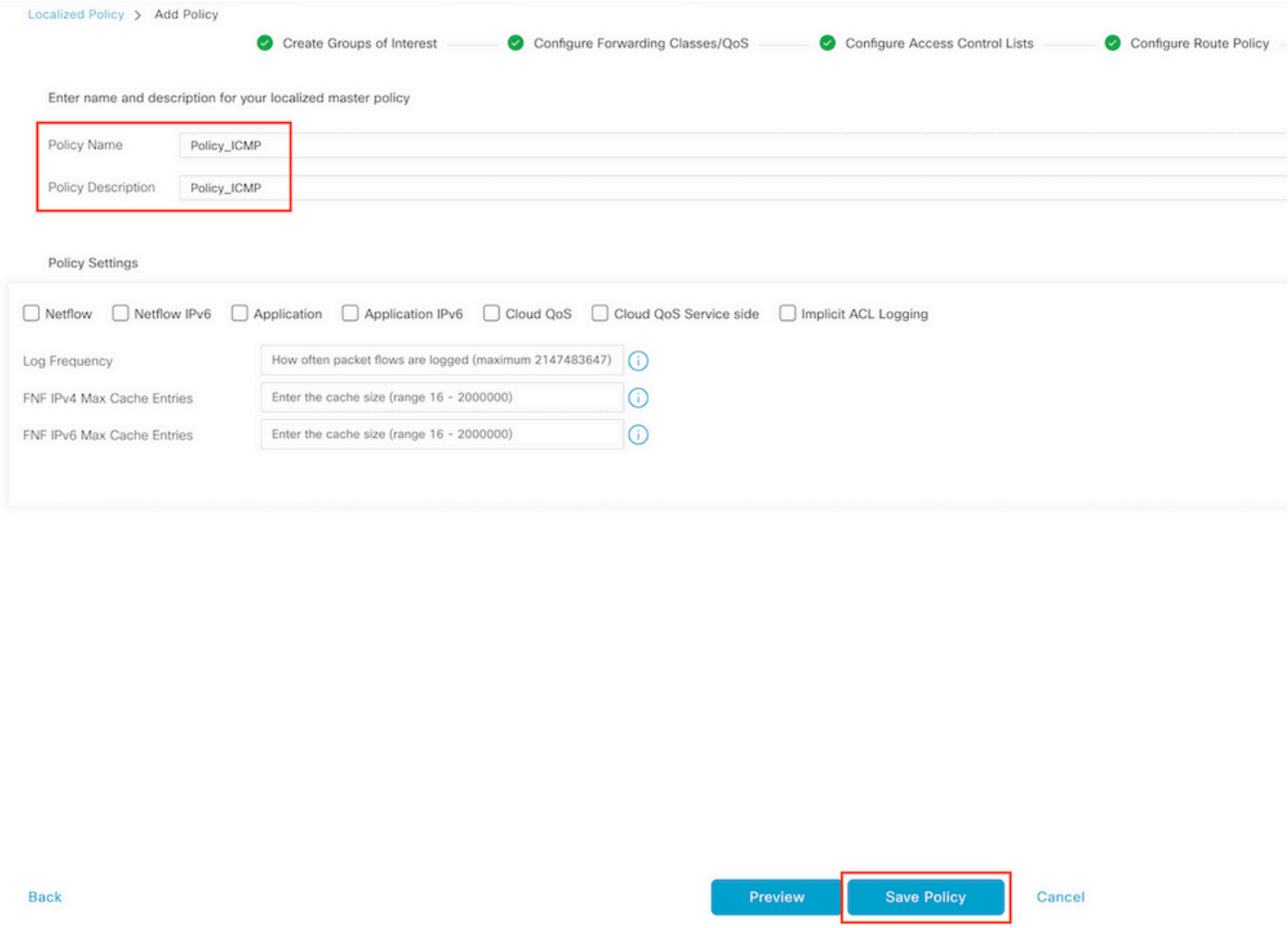


Nota: Questa azione predefinita è alla fine del criterio localizzato. Non utilizzare il comando **drop**, altrimenti tutto il traffico potrebbe risentirne e causare un'interruzione della rete.

Clic **Save Access Control List Policy.**

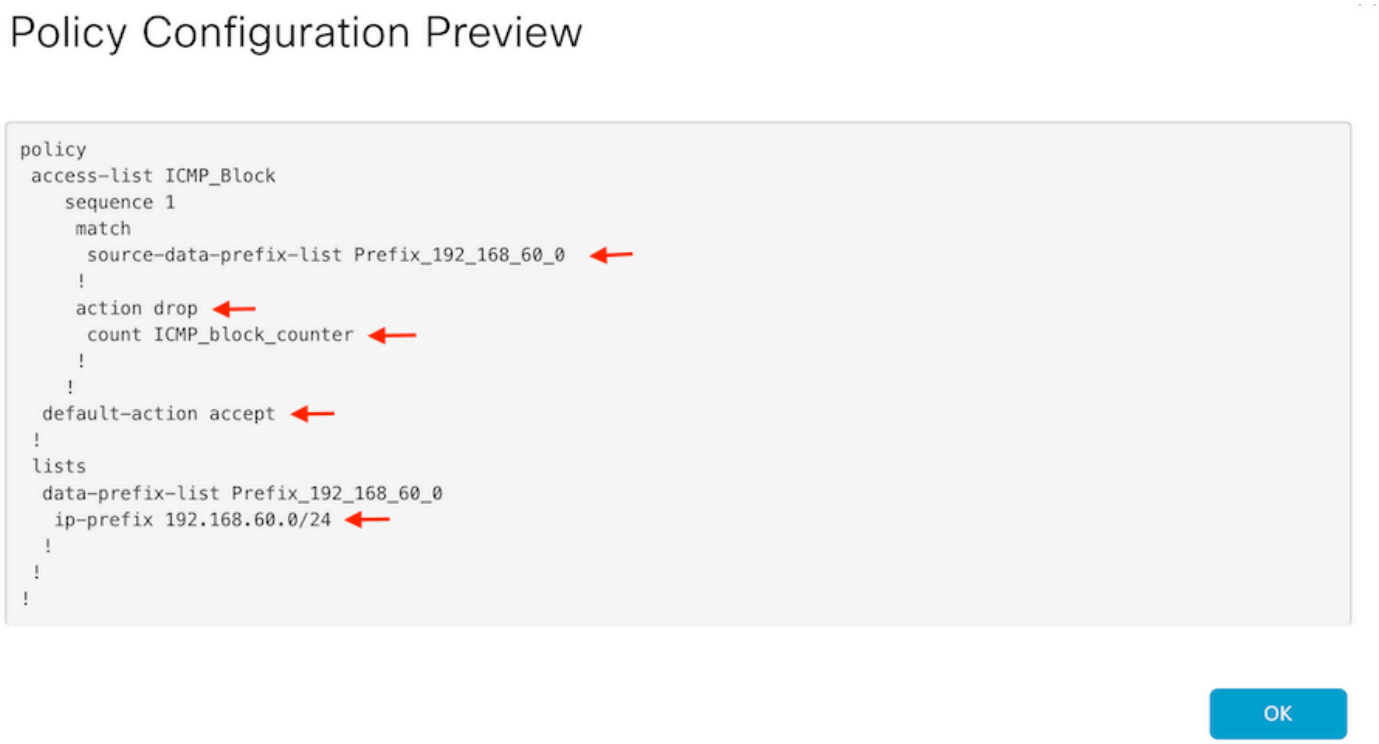
Passaggio 7. Assegnare un nome al criterio

Clic **Next** fino al **Policy Overview** e lo chiami. Lasciare vuoti gli altri valori. Clic **Save Policy**



Per verificare la correttezza del criterio, fare clic su **Preview**.

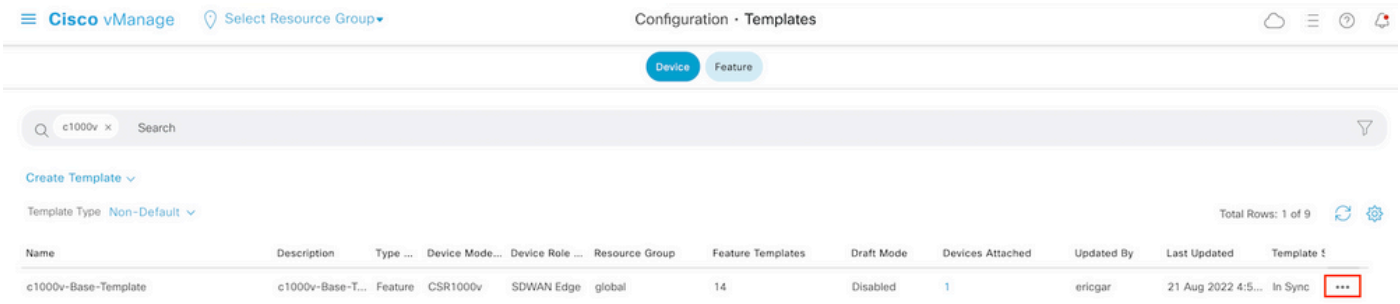
Verificare che la sequenza e gli elementi siano corretti nel criterio.



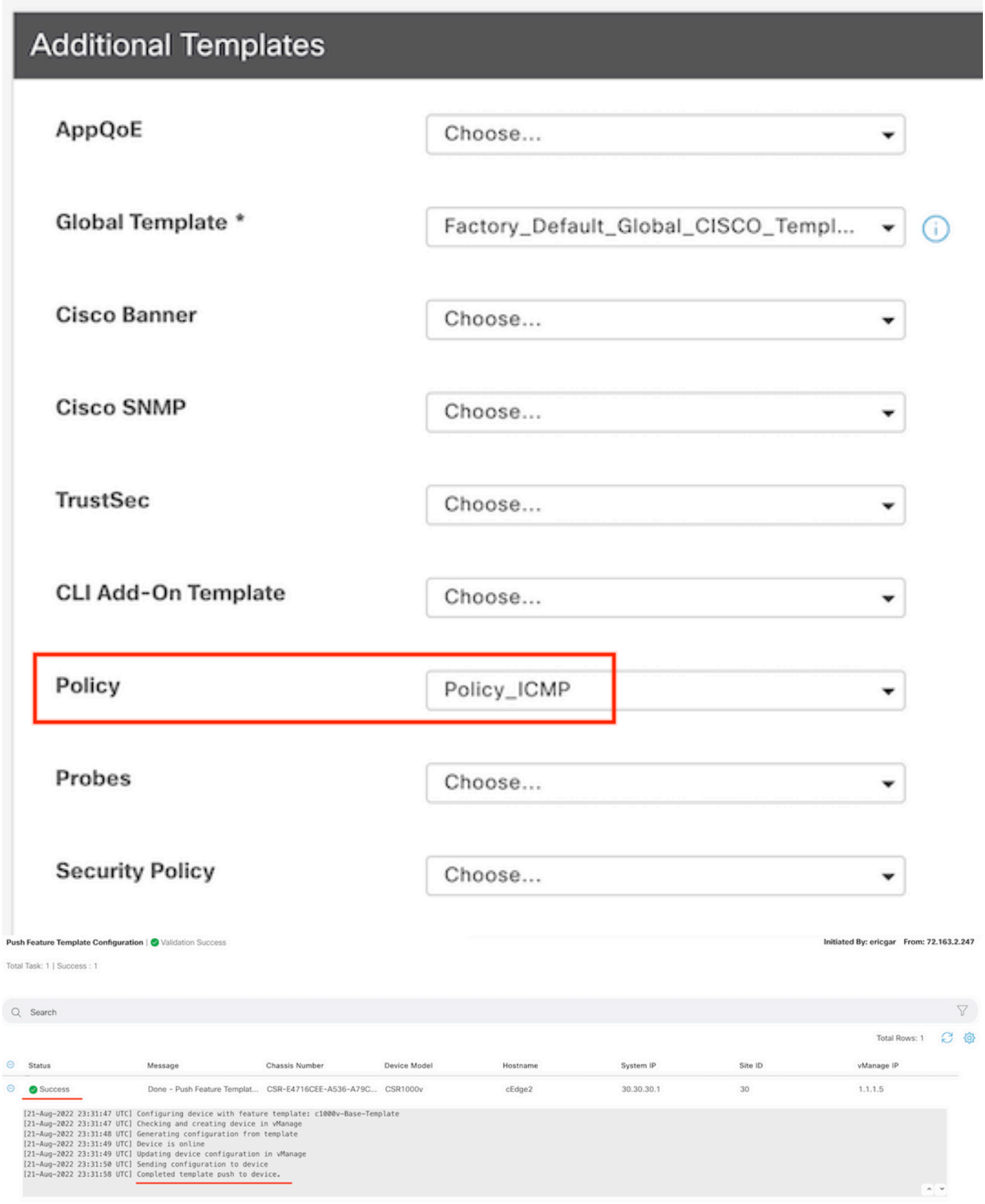
Copiare il nome dell'ACL. È richiesto in una fase successiva.

Passaggio 8. Associare il criterio localizzato al modello di dispositivo.

Individuare il modello di dispositivo collegato al router, fare clic sui tre punti, quindi fare clic su **Edit**.



Seleziona **Additional Templates** e aggiungere il criterio localizzato al campo criterio e fare clic su **Update > Next > Configure Devices** per eseguire il push della configurazione su cEdge.



Nota: A questo punto, vManage crea l'ACL in base al criterio creato e invia le modifiche a cEdge, anche se non è associato ad alcuna interfaccia. Pertanto, non ha alcun effetto sul flusso del traffico.

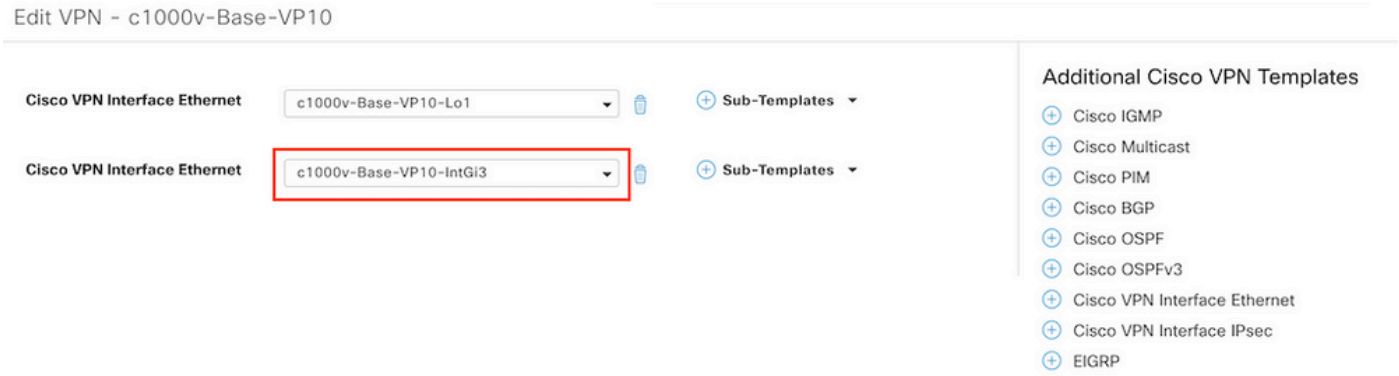
Passaggio 9. Identificare il modello di funzionalità dell'interfaccia a cui deve essere applicata l'azione al traffico nel modello di dispositivo.

Èimportante individuare il modello di funzionalità in cui il traffico deve essere bloccato.

Nell'esempio, l'interfaccia Gigabit Ethernet3 appartiene a Virtual Private Network 3 (Virtual Forwarding Network 3).

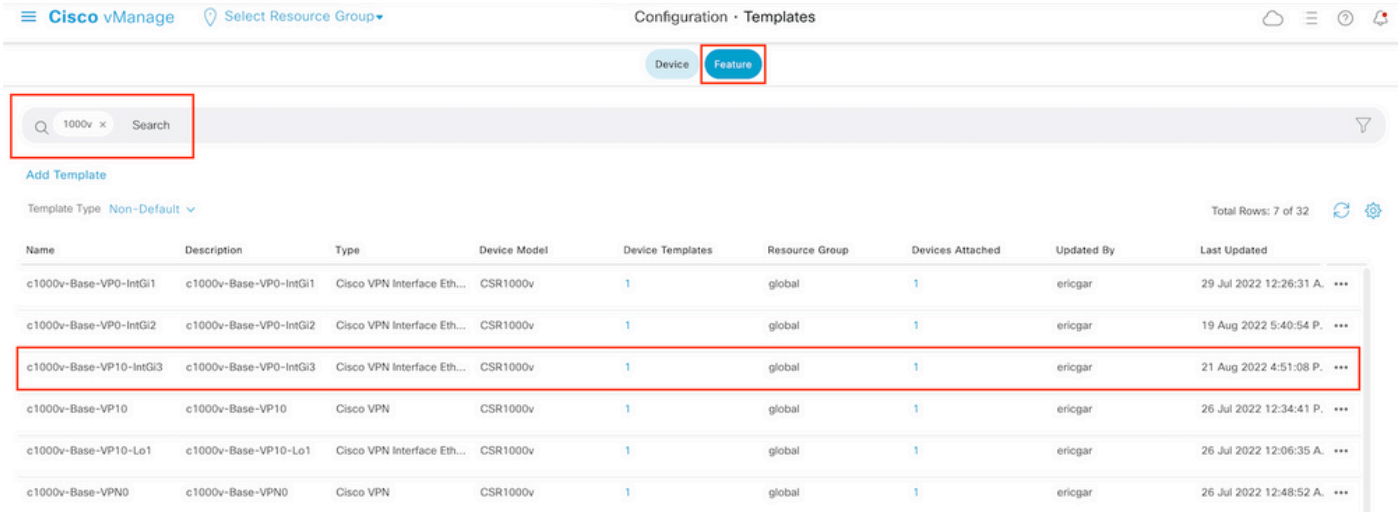
Passare alla sezione Service VPN e fare clic su **Edit** per accedere ai modelli VPN.

Nell'esempio, all'interfaccia Gigabit Ethernet3 è associato un modello di funzionalità c1000v-Base-VP10-IntGi3.

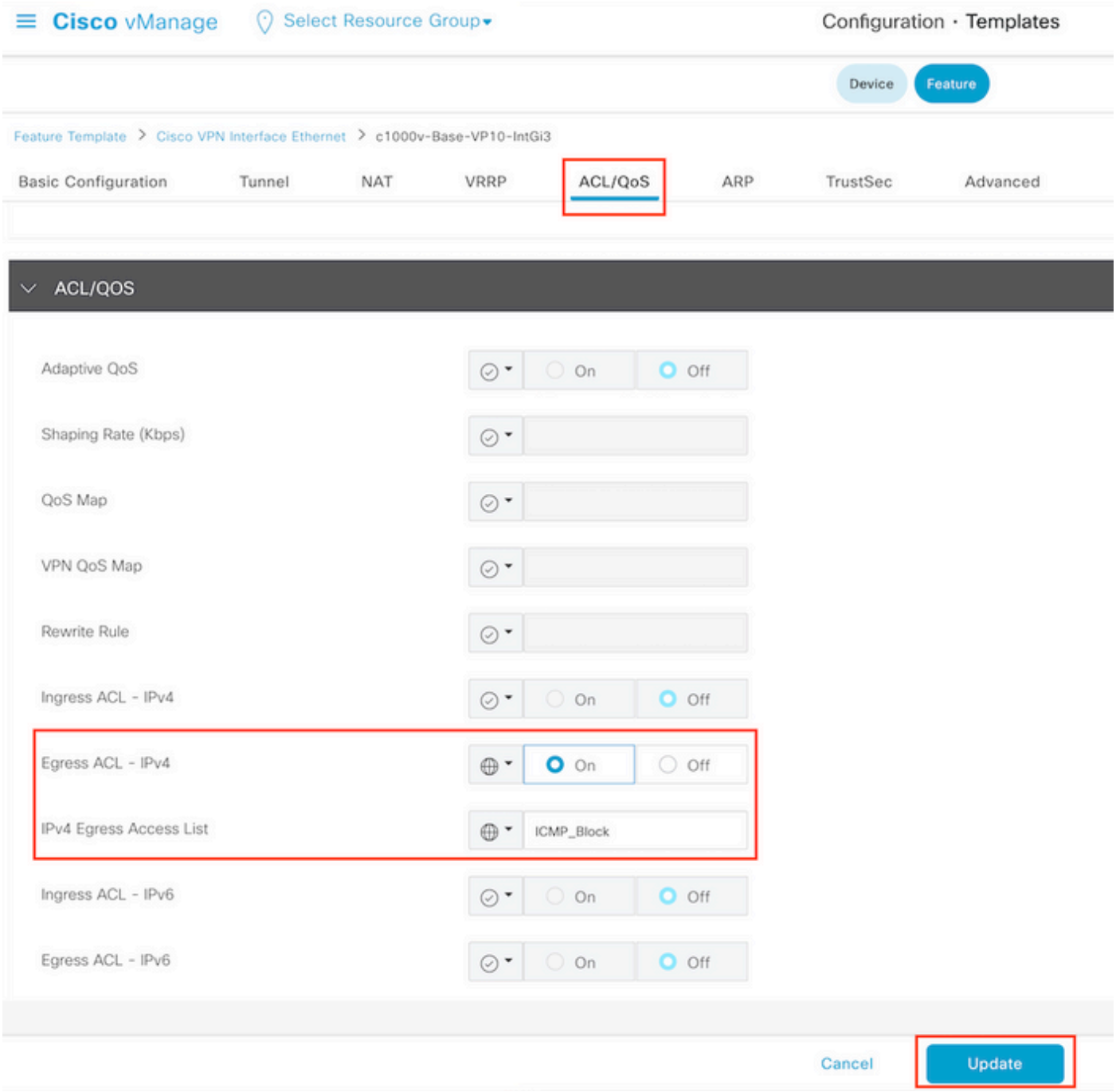


Passaggio 10. Associare il nome ACL all'interfaccia.

Passa a **Configuration > Templates > Feature.** Filtrare i modelli e fare clic su **Edit**



Clic **ACL/QoS** e abilitare la direzione di blocco del traffico. Scrivere il nome ACL copiato nel passaggio 7. Fare clic su **Update** e premere i cambiamenti.



Nota: questo processo di creazione localizzato dei criteri funziona anche per vEdges, in quanto la struttura dei criteri di vManage è la stessa per entrambe le architetture. L'altra parte viene fornita dal modello di dispositivo che crea una struttura di configurazione compatibile con cEdge o vEdge.

Verifica

Passaggio 1. Verificare la corretta configurazione nel router

```
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
```

Passaggio 2. Dall'host 1 nella rete di servizio di cEdge1, inviare 5 messaggi ping al server in 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
```

> **Nota:** Per questo esempio, host1 è un computer Linux. "-I" rappresenta le interfacce su cui il ping esce dal router e "-c" rappresenta il numero di messaggi ping.

Passaggio 3. Da cEdge2, verificare i contatori 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
```

Il contatore corrisponde a cinque (5) pacchetti provenienti dalla rete 192.168.60.0/24, come definito nel criterio.

Passaggio 4. Da cEdge3, inviare 4 messaggi ping al server 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
```

I pacchetti passati attraverso il router al server perché la rete è diversa (in questo caso è 1.1.1.1/32) e non esiste alcuna condizione corrispondente nel criterio.

Passaggio 5. Verificare di nuovo i contatori ACL in cEdge2.

```
cEdge2# show sdwan policy access-list-counters
```

```
NAME COUNTER NAME PACKETS BYTES
------------------------------------------------------------------------------
ICMP_Block ICMP_block_counter 5     610
default_action_count  5     690
```

Il contatore di default_action_count è stato incrementato con i 5 pacchetti inviati da cEdge3.

Per cancellare i contatori, eseguire **clear sdwan policy access-list**

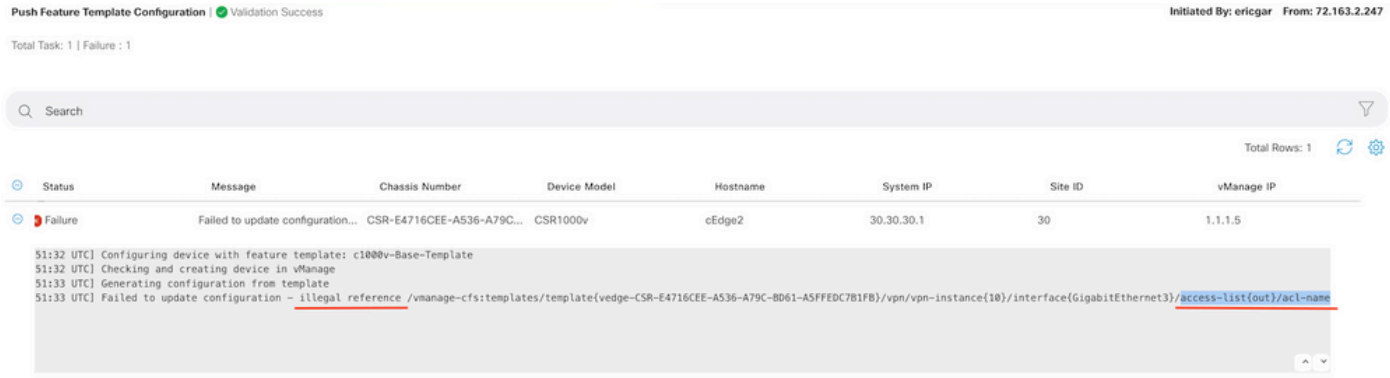
Comandi per la verifica in vEdge

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

Risoluzione dei problemi

Errore: Riferimento non valido al nome ACL nell'interfaccia

Il criterio che contiene l'ACL deve essere prima associato al modello di dispositivo. Quindi, il nome ACL può essere specificato nel modello di dispositivo della funzione dell'interfaccia.



Informazioni correlate

- Guida alla configurazione delle policy Cisco SD-WAN, Cisco IOS XE release 17.x
- Documentazione e supporto tecnico – Cisco Systems

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).