

Configurer une liste de contrôle d'accès pour bloquer/faire correspondre le trafic sur les périphéries avec la stratégie vManage

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Fond](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus de blocage/correspondance dans un serveur cEdge avec une stratégie localisée et une liste de contrôle d'accès (ACL) .

Conditions préalables

Conditions requises

Cisco recommande de connaître ces sujets :

- Réseau étendu défini par logiciel (SD-WAN) Cisco
- Cisco vManage
- Interface de ligne de commande (CLI) cEdge

Components Used

Ce document est basé sur les versions logicielles et matérielles suivantes :

- c8000v version 17.3.3
- vManage version 20.6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

Il existe différents scénarios qui nécessitent une méthode locale pour bloquer, autoriser ou faire correspondre le trafic. Chaque méthode contrôle l'accès au routeur ou garantit que les paquets arrivent au périphérique et sont traités.

Les routeurs cEdge permettent de configurer une stratégie localisée via l'interface de ligne de commande ou vManage pour faire correspondre les conditions de trafic et définir une action.

Voici quelques exemples de caractéristiques des politiques localisées :

Conditions de correspondance :

- DSCP (Differentiated Services Code Point)
- Longueur du paquet
- Protocol
- Préfixe de données source
- Port source
- Préfixe des données de destination
- Destination Port (port de destination)

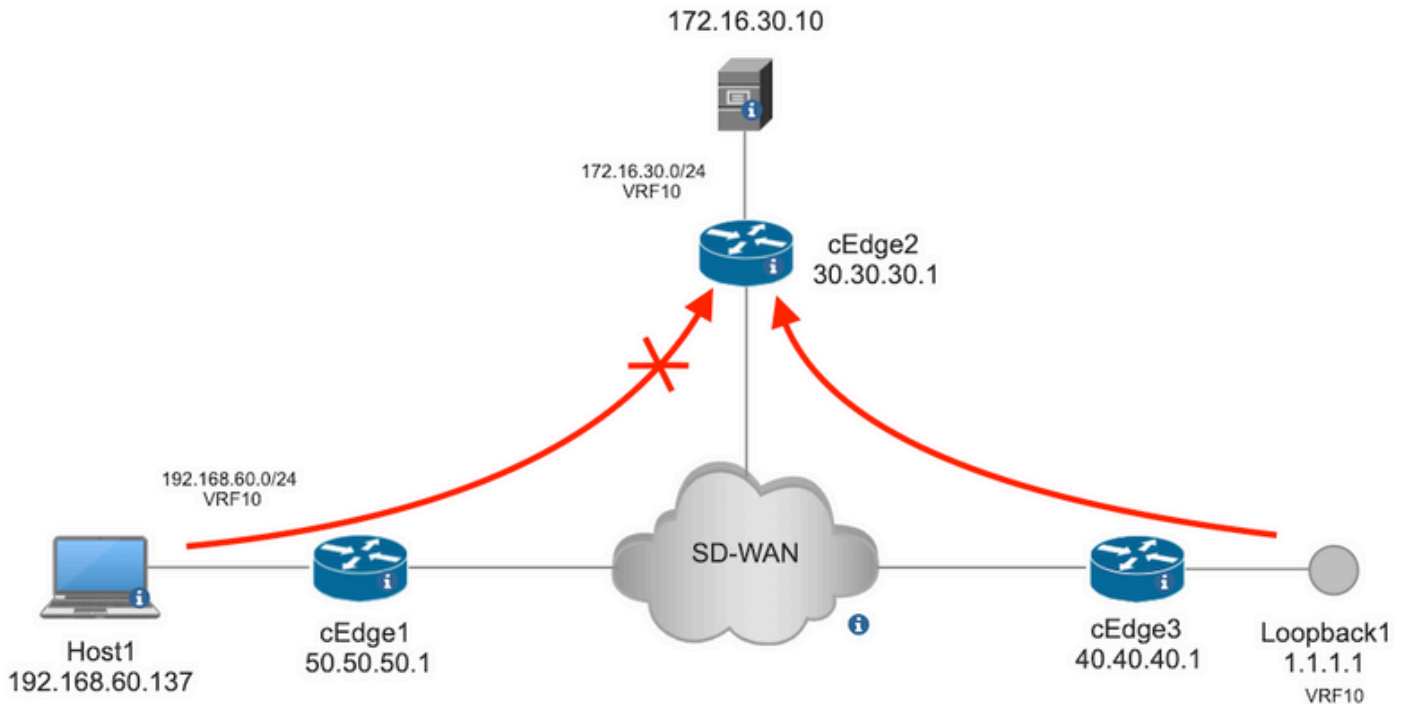
Actions:

- Accept (accepter) Supplémentaire : compteur, DSCP, journaux, tronçon suivant, liste miroir, classe, régulateur
- Chute Supplémentaire : compteur, journal

Configuration

Diagramme du réseau

Pour cet exemple, l'intention est de bloquer le trafic en provenance du réseau 192.168.20.0/24 dans cEdge2 sur la base de la sortie et d'autoriser le protocole ICMP à partir de l'interface de bouclage cEdge3.



Vérification de la requête ping de l'hôte 1 vers le serveur dans 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
```

Vérification ping de cEdge3 vers Server dans 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
```

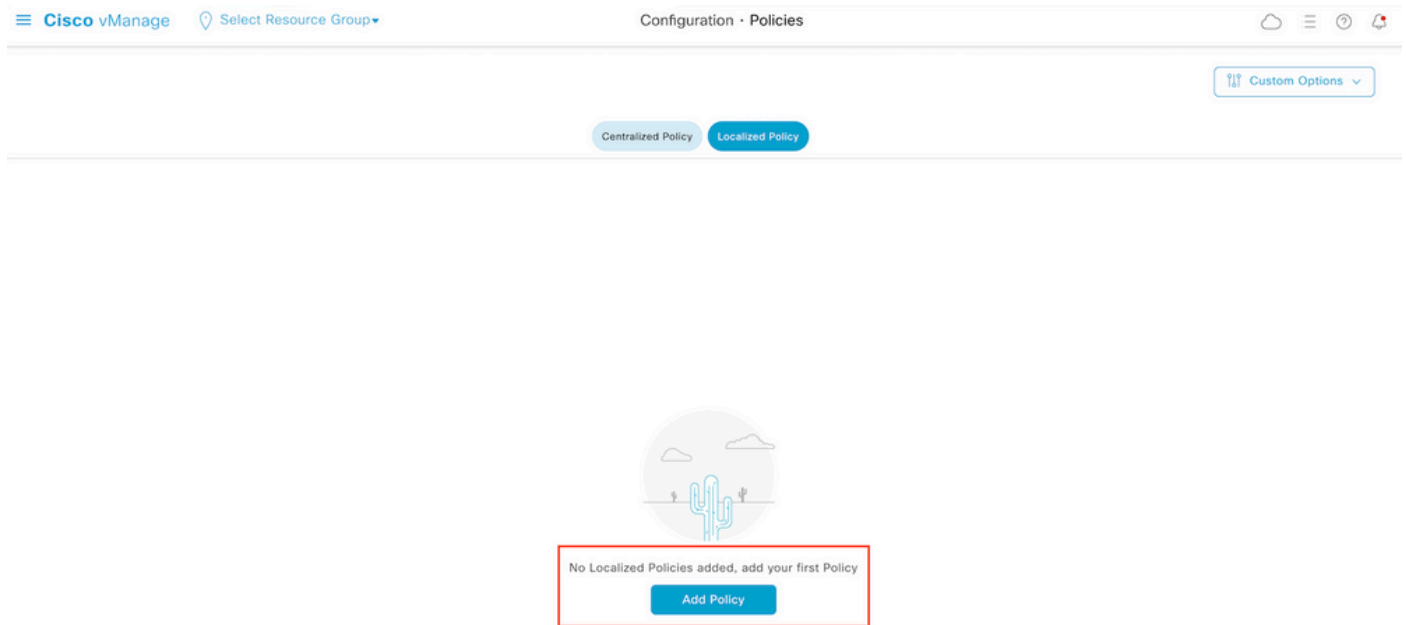
Conditions préalables :

- Un modèle de périphérique doit être attaché à cEdge2.
- Toutes les arêtes doivent avoir des connexions de contrôle actives.
- Toutes les arêtes doivent avoir des sessions BFD (Bidirectional Forwarding Detection) actives.
- Tous les Ecedes doivent disposer de routes OMP (Overlay Management Protocol) pour atteindre les réseaux côté VPN10 de service.

Configurations

Étape 1. Ajout de la stratégie localisée

Dans Cisco vManage, accédez à **Configuration > Politiques > Localized Policy**. Cliquez **Add Policy**

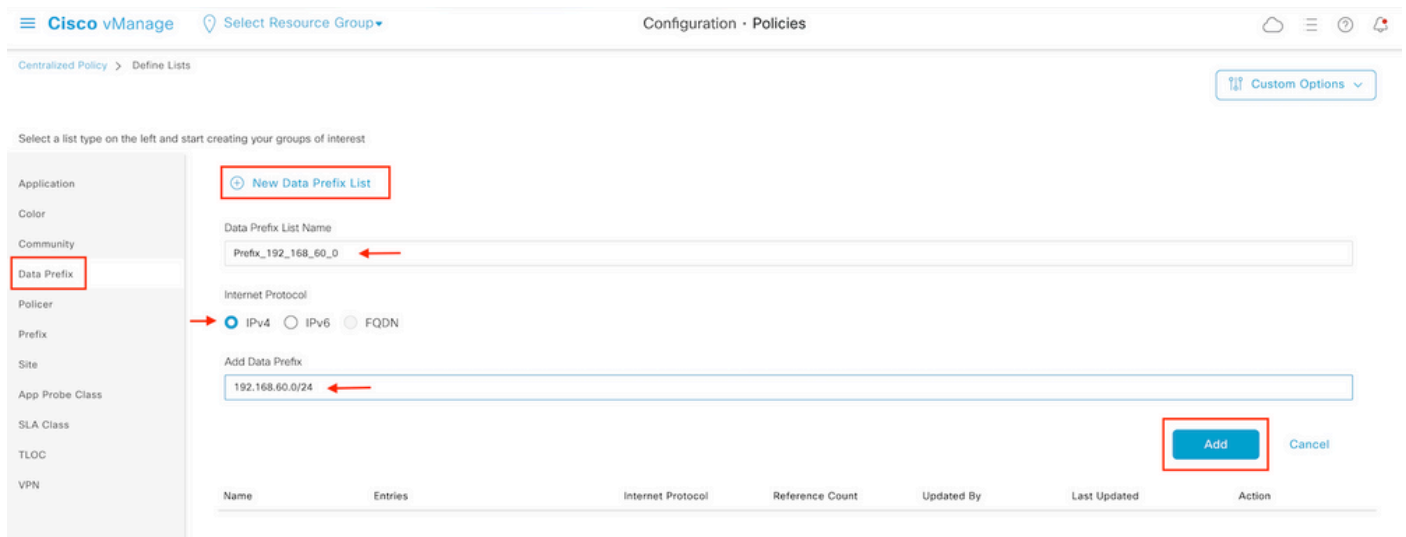


Étape 2 : création de groupes d'intérêt pour la correspondance souhaitée

Cliquez **Data Prefix** dans le menu de gauche et sélectionnez **New Data Prefix List**.

Attribuez un nom à la condition de correspondance, définissez le protocole Internet et ajoutez un préfixe de données.

Cliquez **Add** et ensuite **Next** jusqu'à **Configure Access Control List** s'affiche.



Étape 3 : création de la liste d'accès pour appliquer la condition de correspondance

Sélectionner **Add IPv4 ACL Policy** à partir des versions **Add Access Control List Policy** menu déroulant.

Localized Policy > Add Policy

✔ Create Groups of Interest ✔ Configure Forwarding Classes/QoS ● Configure Access Control Lists

Search

Add Access Control List Policy

Add Device Access Policy

(Add an Access List and configure Match and Actions)

Add IPv4 ACL Policy

Add IPv6 ACL Policy

Import Existing

Description

Mode

Reference Count

No data available

Note: Ce document est basé sur une politique de liste de contrôle d'accès et ne doit pas être confondu avec une politique d'accès aux périphériques. La stratégie d'accès aux périphériques agit uniquement dans le plan de contrôle pour les services locaux tels que SNMP (Simple Network Management Protocol) et SSH (Secure Socket Shell), alors que la stratégie de liste de contrôle d'accès est flexible pour différents services et conditions de correspondance.

Étape 4 : définition de la séquence ACL

Dans l'écran de configuration de la liste de contrôle d'accès, nommez la liste et fournissez une description. Cliquez **Add ACL Sequence** et ensuite **Sequence Rule**.

Dans le menu Conditions de correspondance, sélectionnez **Source Data Prefix** puis sélectionnez la liste de préfixes de données dans la liste **Source Data Prefix List** menu déroulant.

The screenshot shows the configuration page for an IPv4 ACL Policy. The name is 'ICMP_Block' and the description is 'ICMP block from cEdge 1'. On the left, the 'Add ACL Sequence' button is highlighted with a red box. Below it, the 'Sequence Rule' button is also highlighted with a red box. The 'Match' tab is active, and the 'Source Data Prefix' condition is selected and highlighted with a red box. The dropdown menu for 'Source Data Prefix List' is open, showing 'Prefix_192_168_60_0' selected and highlighted with a red box. The 'Actions' section shows 'Accept' and 'Enabled'.

Étape 5. Définissez l'action de la séquence et nommez-la

Naviguez jusqu'à **Action select Drop**, et cliquez sur **Save Match et Actions**.

Add IPv4 ACL Policy

Name: ICMP_Block
Description: ICMP block from cEdge 1

Access Control List

Sequence Rule: Drag and drop to re-arrange rules

Match: **Actions**

Accept **Drop** Counter Log

Match Conditions

Source Data Prefix List: Prefix_192_168_60_0

Source: IP Prefix Example: 10.0.0.0/12

Variables: Disabled

Actions

Drop Enabled

Counter Name: **ICMP_block_counter**

Cancel Save Match And Actions

Note: Cette action est associée exclusivement à la séquence elle-même, et non à la stratégie localisée complète.

Access Control List

Sequence Rule: Drag and drop to re-arrange rules

1 Match Conditions

Source Data Prefix List: Prefix_192_168_60_0

Source: IP

Actions

Drop Enabled

Counter ICMP_block_counter

Étape 6. Dans le menu de gauche, sélectionnez **Default Action**, cliquez **Edit**, et choisissez **Accept**.

Cisco vManage Configuration · Policies

Add IPv4 ACL Policy

Name: ICMP_Block
Description: ICMP block from cEdge 1

Default Action

Accept Enabled

Default Action

Note: Cette action par défaut se situe à la fin de la stratégie localisée. N'utilisez pas **drop**, sinon tout le trafic peut être impacté et provoquer une panne du réseau.

Cliquer **Save Access Control List Policy**.

Add Access Control List Policy Add Device Access Policy (Add an Access List and configure Match and Actions)

Total Rows: 1

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
ICMP_Block	Access Control List (IPv4)	ICMP block from cEdge 1	created	0	ericgar	21 Aug 2022 5:55:54 PM CDT

Étape 7. Nommer la stratégie

Cliquer **Next** jusqu'à **Policy Overview** et nommez-le. Laissez les autres valeurs vides. Cliquer **Save Policy**

Enter name and description for your localized master policy

Policy Name	Policy_ICMP
Policy Description	Policy_ICMP

Policy Settings

 Netflow Netflow IPv6 Application Application IPv6 Cloud QoS Cloud QoS Service side Implicit ACL LoggingLog Frequency ⓘFNF IPv4 Max Cache Entries ⓘFNF IPv6 Max Cache Entries ⓘ[Back](#)[Preview](#)[Save Policy](#)[Cancel](#)

Pour vous assurer que la stratégie est correcte, cliquez sur **Preview**.

Name	Description	Devices Attached	Device Templates	Updated By	Last Updated	
Policy_ICMP	Policy_ICMP	0	0	ericgar	21 Aug 2022 6:05:06 PM CDT	...

[View](#)
[Preview](#)
[Copy](#)
[Edit](#)
[Delete](#)

Vérifiez que la séquence et les éléments sont corrects dans la stratégie.

Policy Configuration Preview

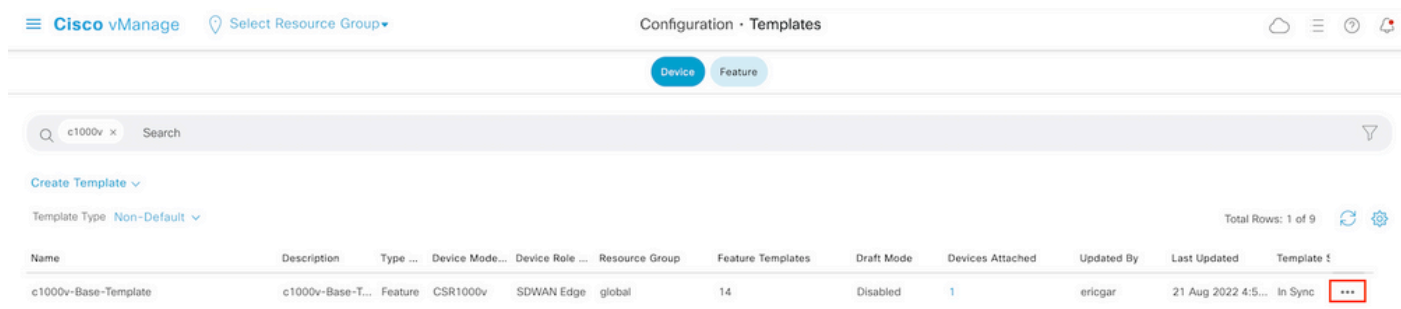
```
policy
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 ←
!
action drop ←
count ICMP_block_counter ←
!
!
default-action accept ←
!
lists
data-prefix-list Prefix_192_168_60_0
ip-prefix 192.168.60.0/24 ←
!
!
!
```

OK

Copiez le nom de la liste. Elle est requise dans une étape ultérieure.

Étape 8. Associez la stratégie localisée au modèle de périphérique.

Localisez le modèle de périphérique connecté au routeur, cliquez sur les trois points, puis sur **Edit**.



Sélectionner **Additional Templates** et ajoutez la stratégie localisée au champ de stratégie, puis cliquez sur **Update > Next > Configure Devices** pour pousser la configuration vers le cEdge.

Additional Templates

AppQoE

Choose...

Global Template *

Factory_Default_Global_CISCO_Templ...



Cisco Banner

Choose...

Cisco SNMP

Choose...

TrustSec

Choose...

CLI Add-On Template

Choose...

Policy

Policy_ICMP

Probes

Choose...

Security Policy

Choose...

Push Feature Template Configuration ● Validation Success

Initiated By: ericgar From: 72.163.2.247

Total Task: 1 | Success : 1

Search

Total Rows: 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
● Success	Done - Push Feature Templat...	CSR-E4716CEE-A536-A79C...	CSR1000v	cEdge2	30.30.30.1	30	1.1.1.5

```
[21-Aug-2022 23:31:47 UTC] Configuring device with feature template: c1000v-Base-Template
[21-Aug-2022 23:31:47 UTC] Checking and creating device in vManage
[21-Aug-2022 23:31:48 UTC] Generating configuration from template
[21-Aug-2022 23:31:49 UTC] Device is online
[21-Aug-2022 23:31:49 UTC] Updating device configuration in vManage
[21-Aug-2022 23:31:50 UTC] Sending configuration to device
[21-Aug-2022 23:31:50 UTC] Completed template push to device.
```

Note: À ce stade, vManage crée la liste de contrôle d'accès en fonction de la stratégie créée et répercute les modifications sur le serveur cEdge, bien qu'il ne soit associé à aucune interface. Par conséquent, il n'a aucun effet sur le flux de trafic.

Étape 9 : identification du modèle de fonctionnalité de l'interface sur laquelle l'action doit être appliquée au trafic du modèle de périphérique

Il est important de localiser le modèle de fonctionnalité où le trafic doit être bloqué.

Dans cet exemple, l'interface GigabitEthernet3 appartient au réseau privé virtuel 3 (Virtual Forwarding Network 3).

Accédez à la section Service VPN et cliquez sur **Edit** pour accéder aux modèles VPN.

Dans cet exemple, l'interface GigabitEthernet3 est associée au modèle de fonctionnalité c1000v-Base-VP10-IntGi3.

Edit VPN - c1000v-Base-VP10

Cisco VPN Interface Ethernet: c1000v-Base-VP10-Lo1

Cisco VPN Interface Ethernet: c1000v-Base-VP10-IntGi3

Additional Cisco VPN Templates

- Cisco IGMP
- Cisco Multicast
- Cisco PIM
- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco VPN Interface Ethernet
- Cisco VPN Interface IPsec
- EIGRP

Étape 10. Associez le nom de la liste de contrôle d'accès à l'interface.

Naviguez jusqu'à **Configuration > Templates > Feature**. Filtrez les modèles et cliquez sur **Edit**

Configuration · Templates

Device Feature

1000v x Search

Add Template

Template Type: Non-Default

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
c1000v-Base-VP0-IntGi1	c1000v-Base-VP0-IntGi1	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	29 Jul 2022 12:26:31 A. ...
c1000v-Base-VP0-IntGi2	c1000v-Base-VP0-IntGi2	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	19 Aug 2022 5:40:54 P. ...
c1000v-Base-VP10-IntGi3	c1000v-Base-VP0-IntGi3	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	21 Aug 2022 4:51:08 P. ...
c1000v-Base-VP10	c1000v-Base-VP10	Cisco VPN	CSR1000v	1	global	1	ericgar	26 Jul 2022 12:34:41 P. ...
c1000v-Base-VP10-Lo1	c1000v-Base-VP10-Lo1	Cisco VPN Interface Eth...	CSR1000v	1	global	1	ericgar	26 Jul 2022 12:06:35 A. ...
c1000v-Base-VPN0	c1000v-Base-VPN0	Cisco VPN	CSR1000v	1	global	1	ericgar	26 Jul 2022 12:48:52 A. ...

Cliquer **ACL/QoS** et activez la direction de blocage du trafic. Écrivez le nom de la liste de contrôle d'accès copié à l'étape 7. Cliquez **update** et pousser les changements.

Device

Feature

Feature Template > Cisco VPN Interface Ethernet > c1000v-Base-VP10-IntGi3

Basic Configuration

Tunnel

NAT

VRRP

ACL/QoS

ARP

TrustSec

Advanced

ACL/QoS

Adaptive QoS	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Shaping Rate (Kbps)	<input type="text"/>
QoS Map	<input type="text"/>
VPN QoS Map	<input type="text"/>
Rewrite Rule	<input type="text"/>
Ingress ACL - IPv4	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Egress ACL - IPv4	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
IPv4 Egress Access List	<input type="text" value="ICMP_Block"/>
Ingress ACL - IPv6	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Egress ACL - IPv6	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off

Cancel

Update

Remarque : ce processus de création de stratégie localisée fonctionne également pour vEdge, car la structure de stratégie vManage est la même pour les deux architectures. La partie différente est fournie par le modèle de périphérique qui crée une structure de configuration compatible avec cEdge ou vEdge.

Vérification

Étape 1 : vérification des configurations du routeur

```
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

```

Étape 2. À partir de l'hôte 1 qui se trouve sur le réseau de service de cEdge1, envoyez 5 messages ping au serveur sur 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

```

Note: Dans cet exemple, host1 est une machine Linux. "-I" représente les interfaces où la requête ping quitte le routeur et "-c" représente le nombre de messages ping.

Étape 3. À partir de cEdge2, vérifiez les compteurs de la liste de contrôle d'accès

```

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

```

Le compteur correspondait à cinq (5) paquets provenant du réseau 192.168.60.0/24, comme défini dans la stratégie.

Étape 4. À partir de cEdge3, envoyez 4 messages ping au serveur 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

```

Les paquets ont transité par le routeur vers le serveur car le réseau est différent (dans ce cas, il s'agit de 1.1.1.1/32) et il n'existe aucune condition correspondante dans la stratégie.

Étape 5. Vérifiez à nouveau les compteurs de la liste de contrôle d'accès dans 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
```

Le compteur de default_action_count a été incrémenté avec les 5 paquets envoyés par cEdge3.

Pour effacer les compteurs, exécutez `clear sdwan policy access-list erasecat4000_flash`.

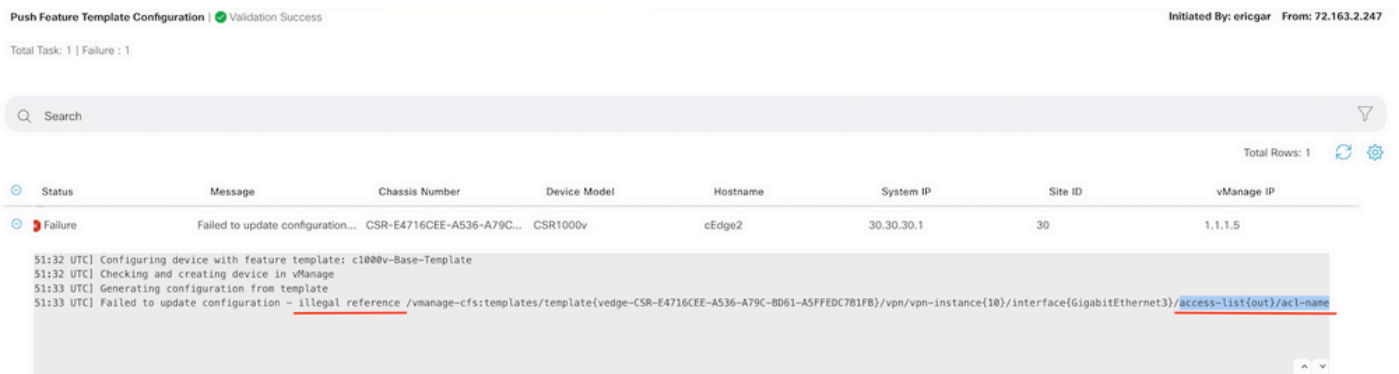
Commandes de vérification dans vEdge

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

Dépannage

Erreur : Référence illégale au nom de la liste de contrôle d'accès dans l'interface

La stratégie qui contient la liste de contrôle d'accès doit d'abord être attachée au modèle de périphérique. Ensuite, le nom de la liste de contrôle d'accès peut être spécifié dans le modèle de périphérique de fonction de l'interface.



The screenshot shows a vManage interface with a configuration push failure. The top bar indicates 'Push Feature Template Configuration' with a green 'Validation Success' status. Below, a table lists the failed task. The log details the error: 'Failed to update configuration - illegal reference /vmanage-cfs:templates/template(vedge-CSR-E4716CEE-A536-A79C-8D61-A5FFEDC7B1FB)/vpn/vpn-instance(10)/interface(GigabitEthernet3)/access-list(out)/acl-name'.

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Failure	Failed to update configuration...	CSR-E4716CEE-A536-A79C...	CSR1000v	cEdge2	30.30.30.1	30	1.1.1.5

```
51:32 UTC| Configuring device with feature template: c1000v-Base-Template  
51:32 UTC| Checking and creating device in vManage  
51:33 UTC| Generating configuration from template  
51:33 UTC| Failed to update configuration - illegal reference /vmanage-cfs:templates/template(vedge-CSR-E4716CEE-A536-A79C-8D61-A5FFEDC7B1FB)/vpn/vpn-instance(10)/interface(GigabitEthernet3)/access-list(out)/acl-name
```

Informations connexes

- [Guide de configuration des politiques Cisco SD-WAN, Cisco IOS XE version 17.x](#)
- [Support et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.