

ACL (لوصول) في مكحتل ةمئاق نيوكت فاوخل اىلع رورملا ةكرح ةقباطم/رظحل vManage جهن مادختساب

تايوتحمل

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيفلخل](#)

[نيوكتلا](#)

[ةكبش لىل طيطلختلا مسرلا](#)

[تانويوكتلا](#)

[ةحصل نم ققحتلا](#)

[اهخالص او عااخال فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةمئاقو ةيلحم ةسايس مادختساب cEdge في ةقباطملا/رظحلا ةيلمع دننتملا اذه فصبي
(ACL) لوصول في مكحت

ةيساسأل تابلطتملا

تابلطتملا

ةيلالاتل تا عوضوملا ةفرعمب Cisco ي صوت

- Cisco (SD-WAN) جم انرب نم ةفرعملا ةساولا ةقطنملا ةكبش
- Cisco vManage جم انرب
- cEdge (CLI) رم اوأل رطس ةهجاو

ةمدختسملا تانوكملا

ةيلالاتل ةيداملا تانوكملا او جم انربلا تارادصلا لىل دننتملا اذه دننتملا

- 17.3.3 رادصلا c8000v
- 20.6.3 رادصلا، vManage

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجال نم دننتملا اذه في ةدراولل تامولعمل عاشنإ مت
تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتملا اذه في ةمدختسملا ةزهجال عيمج تادب
رما يال لم تحملا ريثاتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش

ةيفلخلا

وأاهب حامسلا وأرورملا ةكرح رظحل ايلحم ابولسأ بلطتت ةفلتخم تاهويرانيس كانه زاهجلا ىلا مزحلا لوصو نمضت وأ هجوملا ىلا لوصولا يف ةقيرط لك مكحتت. اهتقباطم اهتجالعمو.

ةقباطم ل vManage وأ CLI لالخم نم ةيلحم ةسايس نيوكت ىلع ةردقلا cEdge تاهجوم رفوت ءارجا ديحتت و رورملا ةكرح طورش.

ةيلحملا جهنلا صئاصخل ةلثمألا ضعب هذه:

ةقباطملا طورش:

- (DSCP) ةزيمملا تامدخلا دوك ةطقن
- ةمزحلا لوط
- لوكوت و رربلا
- ردصملا تانايبلا ةئداب
- ردصملا ذفنم
- ةهجولا تانايب ةئداب
- ءانيم ةياغ

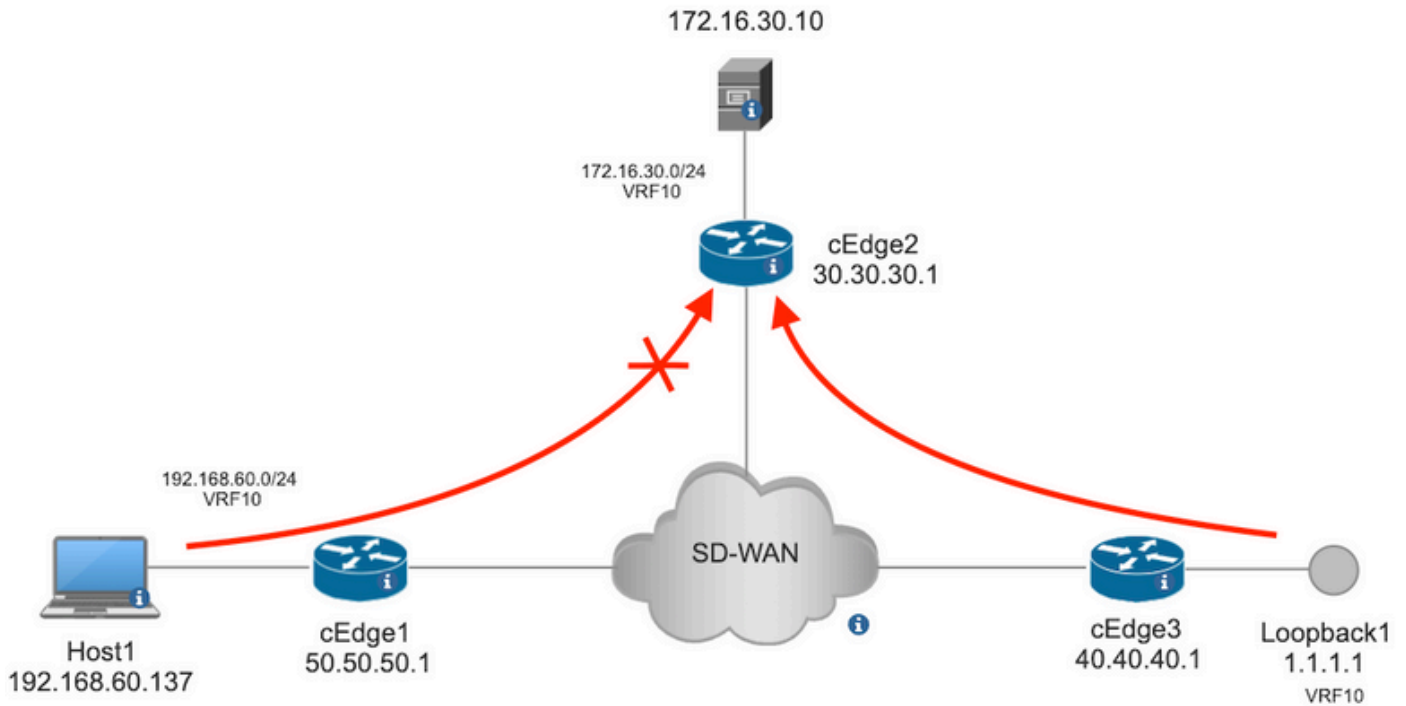
تاءارجالا:

- مظنم، ةئف، قباطم خسن ةمئاق، nexthop، تالجس، DSCP، دادع: يفافضا لوبق
- لجس، دادع: يفافضا ةرطق

نيوكتلا

ةكبشلا ليطي طختلا مسرلا

ىلع cEdge2 يف 192.168.20.0/24 ةكبشلا نم رورملا ةكرح رظح وه فدهلا، لاثملا لىبس ىلع cEdge3. ءاجرتسا ةهجاو نم ICMP لوكوت و رربلا حامسلا او جرخلا ساسا.



cEdge2 في مداخل اللى 1 فيضم اللى نم لاصلت اللى رابتخ نم ققحت اللى

```
[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
```

cEdge2 في مداخل اللى 3 في cEdge3 نم لاصلت اللى رابتخ نم ققحت اللى

```
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
```

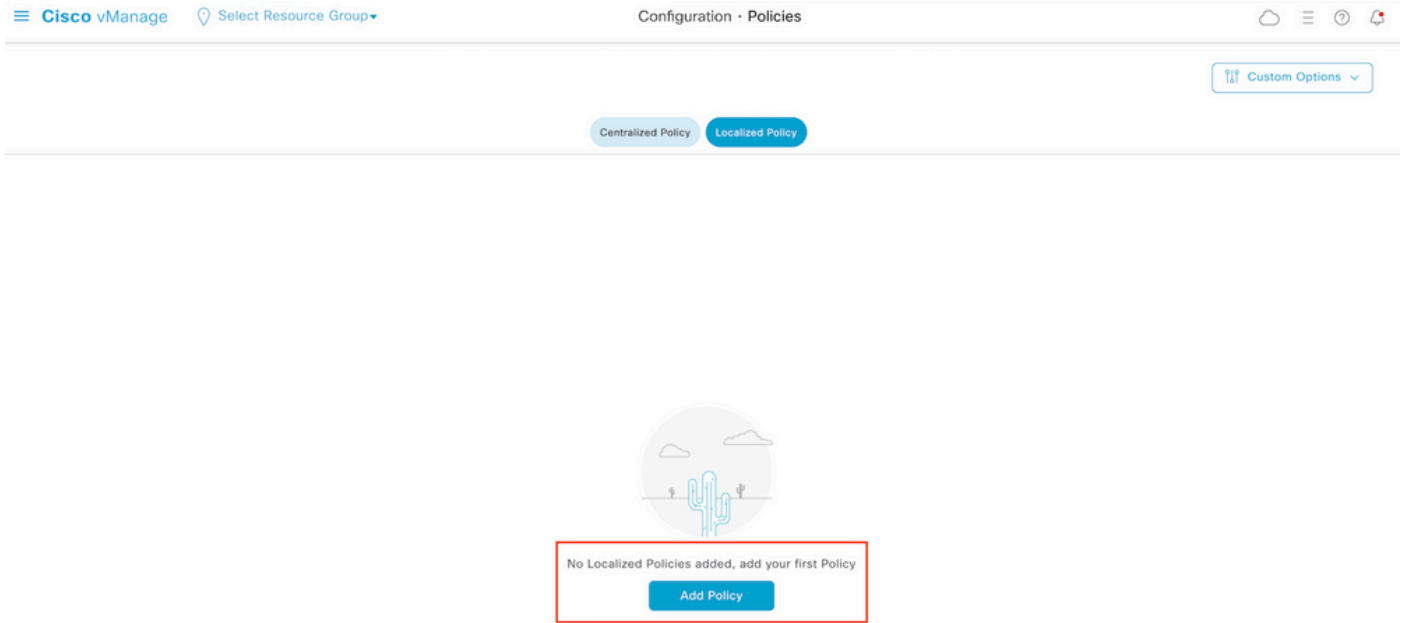
ةقبس اللى طورش اللى

- ققفرم زاهج بللق اللى ع cEdge2 يوتحي نأ بجي.
- ةطشن مكحت تالاصلت اللى CEdges ةفاك اللى نوكي نأ بجي.
- طشن ةسلج (BFD) فشك forwarding هاجت اللى ئانث اللى ققتي فيغبني cEdges لك.
- لوصول اللى (OMP) ةعرفتم اللى ةراد اللى لوكوتورب تاراسم اللى ع تادحولا عيجم يوتحت نأ بجي.
- اللى VPN10 ةمدخل اللى ةبناج اللى تاكبش اللى اللى

تاني وك اللى

مجرتم اللى جهن اللى فضا 1. ةوطخل اللى

إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة



إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة

إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة

إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة

إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة



إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة

إضافة سياسة Cisco vManage، إضافة سياسة Configuration > Policies > Localized Policy. إضافة سياسة

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

طلخال مدع بچي و لوصول في مكحتلا ةمئاق ةسايس لى دنتمس ل اذ دن تسي : ةظالم مكحتلا ةطخ في زاهج لى لوصول اهن لمعي . زاهج لى لوصول اهن نيب و هني ب ذخام ةرشقو (SNMP) طيس بل ةكبش ل ةراد لوكوتورب لثم ةيلحمل تامدخل ةنرم لوصول في مكحتلا ةمئاق ةسايس نأ نيح في ، طقف ، (SSH) ةنمآ ل لوصول ل ةقباطم ل طورش و ةفلتخمل تامدخل .

4. ةوطخل (ACL) لوصول في مكحتلا ةمئاق لس لس ت ديحت .

في مكحتلا ةمئاق ةيمستب مق ، (ACL) لوصول في مكحتلا ةمئاق نيوكت ةشاش في Sequence Rule م م نمو Add ACL Sequence رقا . فصو مي دقتو (ACL) لوصول

Source Data Prefix نم تانايب ل تائداب ةمئاق رتخ م م Source Data Prefix دح ، ةقباطم ل طورش ةمئاق في ةل دسنم ل ةمئاق ل Prefix List .

Add IPv4 ACL Policy

Name ICMP_Block

Description ICMP block from cEdge 1

Add ACL Sequence

Access Control List

Sequence Rule

Drag and drop to re-arrange rules

Drag & drop to reorder

Default Action

Match Conditions

Source Data Prefix List

Prefix_192_168_60_0

Source: IP Prefix

Example: 10.0.0.0/12

Variables: Disabled

Actions

Accept

Enabled

5. ةوطخل هتيمستب مق و لس لس تلاب صاخ ل ارجال في رعتب مق .

Save Match و Actions قوف رقا ، Drop ديحت Action لى لقتنا

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

ةساي سلاب سيلو، هسفن لسلسلاب يرضح لكشب طبترم ارجإل اذه: ةظالم
ةمجرتملا ةلماكل.

Access Control List

Sequence Rule: Drag and drop to re-arrange rules

Match Conditions

Source Data Prefix List: Prefix_192_168_60_0

Source: IP

Actions

Drop: Enabled

Counter: ICMP_block_counter

Accept راتختو، Edit ةق طوط، Default Action دح، ىرسىلا ةمئاقلا يف 6 ةوطخلا

Cisco vManage Configuration · Policies

Add IPv4 ACL Policy

Name: ICMP_Block
Description: ICMP block from cEdge 1

Default Action

Accept: Enabled

الو، drop مدختست ال. برعملا جهنلا ةيانهن يف يضارتف ال ارجإل اذه عقي: ةظالم
ةكبشلا عاطقنا يف ببستتو لماكلاب تانايبلا رورم ةكرح رثاتت نا نكمي.

رقنا 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

جهنلا ةيمستب مق 7 ةوطخلا

Save Policy رقنا. ةغراف ىرخألا ميقللا كرتأ. اهومس و Policy Overview ىتح Next رقنا

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](#)

Preview. قوف رقنا، جهنلا ةحص نم دكأتلل

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](#)

جهنلا يف رصان عل او لس لس لتلا ةحص نم ققحت

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

يُرخأ ةوطخ ي ف بولطم اذهو (ACL) لوصول ي ف مكحتل ةمئاق مسا خسنا

زاهجل بلق ب مجرتم لاهنل نارقا 8 ةوطخل

Edit قوف رقناو، ثالثل طاقنل رقناو، هجوملاب قفرم لاهجل بلق عقوم دح

Name	Description	Type ...	Device Mode...	Device Role ...	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template ID	
c1000v-Base-Template	c1000v-Base-T...	Feature	CSR1000v	SDWAN Edge	global	14	Disabled	1	ericgar	21 Aug 2022 4:5...	In Sync	...

Update > Next > Configure قوف رقناو جهنل ل قح لى مجرتم لاهنل فضاو **Additional Templates** دي دحت
cEdge لى نيوكتل عفدل **Devices**

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.
```

(ACL) لوصولو ي ف مكحتلا ةمئاق عاشناب vManage موقى ، ةطقنلا هذه دن ع : ةطخالما ريغ اهنأ مغر ، CEdge لىل تاريغتلا ع ف دو اءاشناب مت يتلا ةسايسلا لىل اءانتسا رورملا ةكرح ق فدت ي ف ريثأت ي اهل سىل ، كلذل . ةءءاو ي ءب ةطبترم

رورملا ةكرح لىل عءارءال قىببطل طىطختلا متى شىء ةءءاولل تازىملا بللق دءء . 9 ةوطخالما فءاءءال بللق ي ف

رورملا ةكرح رظح مزلي شيح ةزيملا بلواق عقوم ديدحت مهملام

ةداعا ةكبش) 3 ةيرهاطلا ةصاخلا ةكبشلا لىل GigabitEthernet3 ةهجاو يمتنت ،لاثملا اذه يف (3 ةيرهاطلا هيجوتلا

ةصاخلا ةكبشلا بلواق لىل لوصول Edit رقناو ةمدخل VPN ةكبش مسق لىل لقتنا (VPN) ةيرهاطلا

c1000v-Base-VP10-IntGi3 ةزيم بلواق لىل GigabitEthernet3 ةهجاو يوتحت ،لاثملا اذه يف قفرملا

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

ةهجاو اب (ACL) لوصولا يف مكحتلا ةمئاق مسا طبرأ 10 ةوطخلا

Edit رقناو بلواقلا ةيفصت Configuration > Templates > Feature لىل لقتنا

Cisco vManage Select Resource Group Configuration · Templates

Device Feature

1000v Search

Add Template

Template Type Non-Default

Total Rows: 7 of 32

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. ...

(ACL) لوصولا يف مكحتلا ةمئاق مسا بتكا .بجحلل رورملا ةكرح هاجتا نيكمت و ACL/QoS رقنا تاريغتلا عفو Update رقنا 7 ةوطخلا يف خوسنملا

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

 On Off

Shaping Rate (Kbps)

QoS Map

VPN QoS Map

Rewrite Rule

Ingress ACL - IPv4

 On Off

Egress ACL - IPv4

 On Off

IPv4 Egress Access List

 ICMP_Block

Ingress ACL - IPv6

 On Off

Egress ACL - IPv6

 On Off

Cancel

Update

سياسية نونب نأل vEdges ل هذه ةي لحملا ةساي سلا ءاشنإ ةي لمع اضيأ لمعت : ةظالم بلاق ةطساوب فل تخملا ءزجال ريفوت متي . نينيتي نونب ل نم لكل اهسفن يه vManage و cEdge أو vEdge عم ةقفاوتم نيوكت ةي نونب ءاشنإ ب موق ي ذل زاهال

ةحصلا نم ققحتلا

ءوملا يف ءحص لكشب تانويوكتلا نم ققحتلا 1. ةوطخل

```
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

```

رابطه | لئاسر 5 لاسرا، cEdge1، بصاخلا مداخله كيش في دوجومال Host1 نم 2. ةوطخلا
 cEdge2 في مداخله الى لاصتاله

```

[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

```

يتل تاهاولا "-ا" لثمي. سكونيل زاهج وه 1 فيضمال، لالم لابس يلع: ةطخال
 لاصتاله رابطه | لئاسر ددع "-c" لثمي وهجومال لاصتاله رابطه | اه في رداغي.

(ACL) لوصول في مكحتاله عمئاق تادادع نم ققحتاله، cEdge2 نم 3. ةوطخال

```

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

```

ةسايسلال في ددحم وه امك، 192.168.60.0/24 ةكبشلال نم تءاج مزح (5) سمخ دادعاله قباط

172.16.30.10 مداخله الى لاصتاله رابطه | لئاسر 4 لاسراب مق، cEdge3 نم 4. ةوطخال

```

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

```

دجوت الو (1.1.1.1/32) هه لاله هذه في) ةفلتخم ةكبشلال نأل مداخله الى هجومال ربع مزحل ترم
 ةسايسلال في اهله قباطم ةلاه.

ىرخأ ةرم cEdge2 في لوصول في مكحتاله عمئاق تادادع نم ققحتاله 5. ةوطخال

```

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

```

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

داز cEdge3 ةطساوب ةلسرم مزح 5 عم default_action_count دادع

clear sdwan policy access-list eraseat4000_flash: لىغش تب مق ، تادادع لى حسم ل

vEdge في ققحت لى رماو

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

اهحالص او ءاطخال فاش كتسا

ةهجاو لى في (ACL) لوصولاب م كحتلا ةمئاق م سالى نوناق ريغ عجرم :أطخ

دعب .زاهجلا بلقبا الو (ACL) لوصولا في م كحتلا ةمئاق لىع يوتحي يذلا جهنلا قافرا بجي
ةهجاو لى ةزيملا زاهج بلقبا في (ACL) لوصولا في م كحتلا ةمئاق مسا ديدحت نكمي ، كلذ

Push Feature Template Configuration | Validation Success Initiated By: ericgar From: 72.163.2.247

Total Task: 1 | Failure: 1

Search Total Rows: 1

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-BD61-ASFFEDC7B1FB)/vpn/vpn-instance(10)/interface(gigabitEthernet3)/access-list(out)/acl-name
```

ةلص تاذا تامولعم

- [Cisco SD-WAN، Cisco IOS XE، رادصلال 17.x تاسايس نيوكت لى لى](#)
- [Cisco Systems - تادنت سمل او ينقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوءو تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل