

vManage 정책을 사용하여 cEdge에서 트래픽을 차단/매칭하도록 ACL 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 현지화된 정책 및 ACL(Access Control List)을 사용하여 cEdge에서 차단/일치시키는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)
- Cisco vManage
- cEdge CLI(Command Line Interface)

사용되는 구성 요소

이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- c8000v 버전 17.3.3
- vManage 버전 20.6.3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

트래픽을 차단, 허용 또는 매칭하려면 로컬 방법이 필요한 다양한 시나리오가 있습니다. 각 방법은 라우터에 대한 액세스를 제어하거나 패킷이 디바이스에 도착하고 처리되도록 합니다.

cEdge 라우터는 CLI 또는 vManage를 통해 현지화된 정책을 구성하여 트래픽 조건과 일치시키고 작업을 정의할 수 있는 기능을 제공합니다.

다음은 현지화된 정책 특성의 몇 가지 예입니다.

일치 조건:

- 차등 서비스 코드 포인트(DSCP)
- 패킷 길이
- 프로토콜
- 소스 데이터 접두사
- 소스 포트
- 대상 데이터 접두사
- 대상 포트

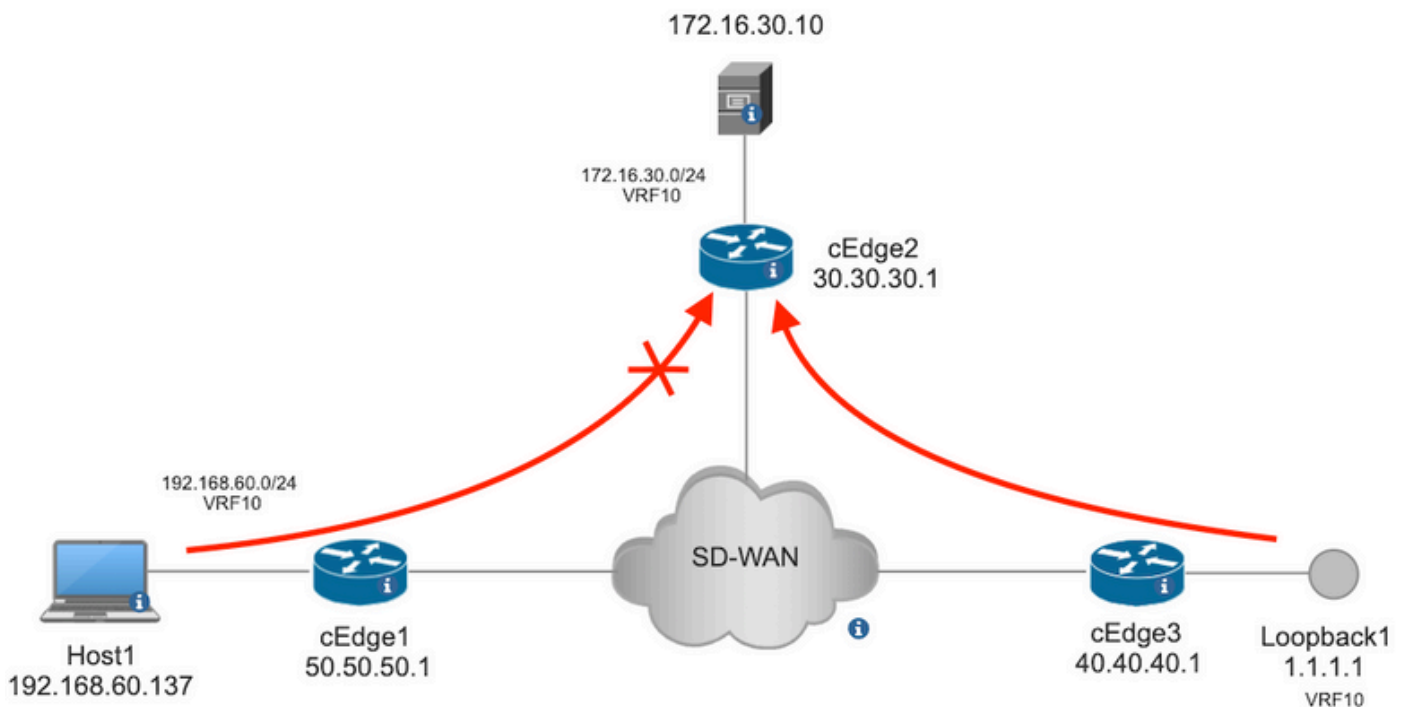
작업:

- 수락 추가: 카운터, DSCP, 로그, nexthop, 미러 목록, 클래스, 폴리서
- 삭제 추가: counter, log

구성

네트워크 다이어그램

이 예에서 의도는 이그레스 기반으로 cEdge2의 네트워크 192.168.20.0/24에서 트래픽을 차단하고 cEdge3 루프백 인터페이스에서 ICMP를 허용하는 것입니다.



cEdge2의 Host1에서 서버로 ping 확인

```
[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
```

cEdge3에서 cEdge2의 서버로 ping 확인

```
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
```

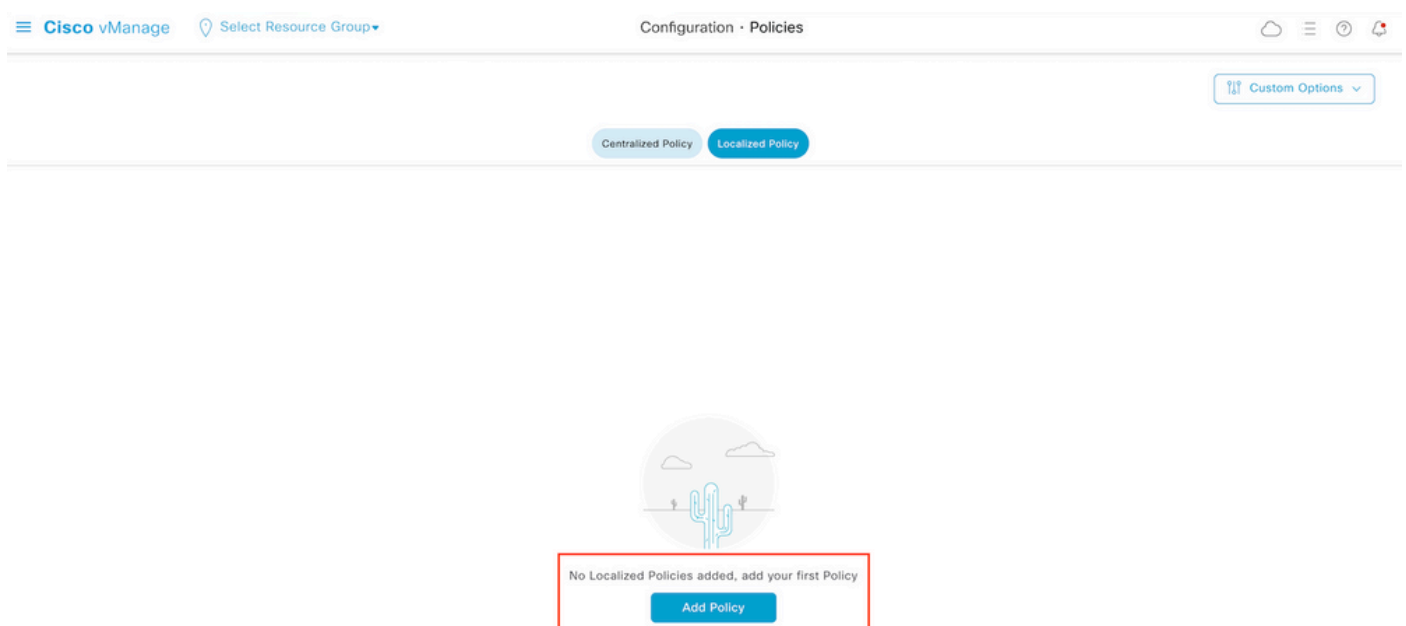
전제 조건:

- cEdge2에는 연결된 장치 템플릿이 있어야 합니다.
- 모든 cEdge에는 제어 연결이 활성화되어 있어야 합니다.
- 모든 cEdge에는 BFD(Bidirectional Forwarding Detection) 세션이 활성화되어 있어야 합니다.
- 서비스 VPN10측 네트워크에 연결하려면 모든 헤더에 OMP(Overlay Management Protocol) 경로가 있어야 합니다.

설정

1단계. 현지화된 정책을 추가합니다.

Cisco vManage에서 **Configuration > Policies > Localized Policy**. 클릭 **Add Policy**

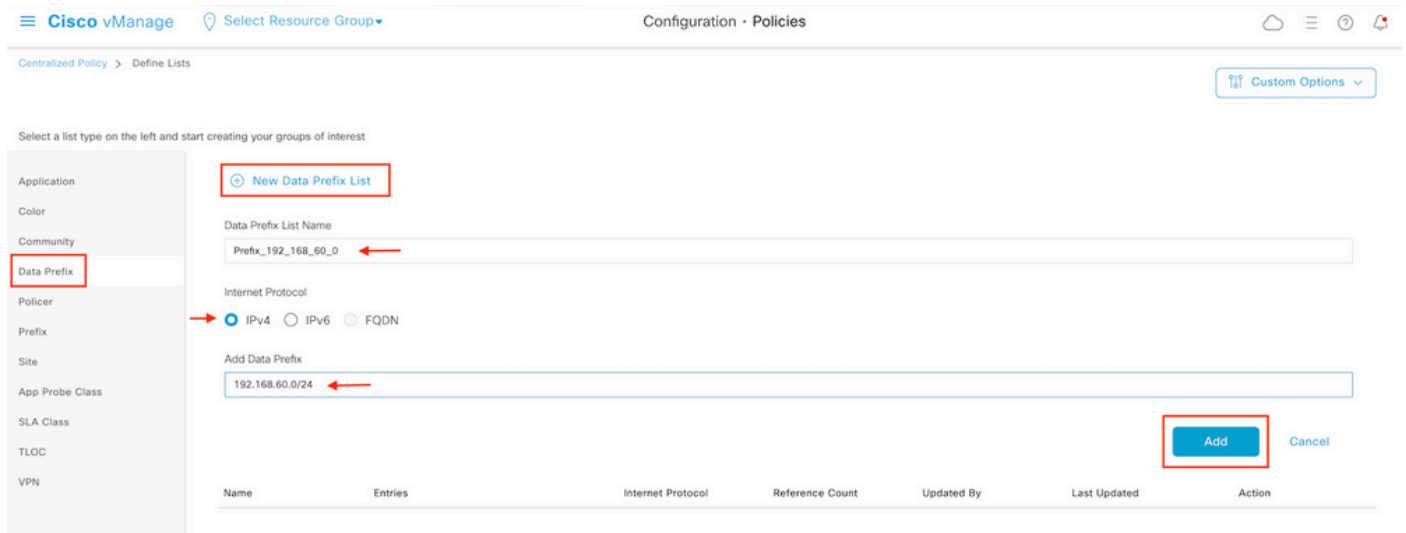


2단계. 원하는 일치에 대한 관심 그룹을 생성합니다.

클릭 **Data Prefix** 왼쪽 메뉴에서 **New Data Prefix List**.

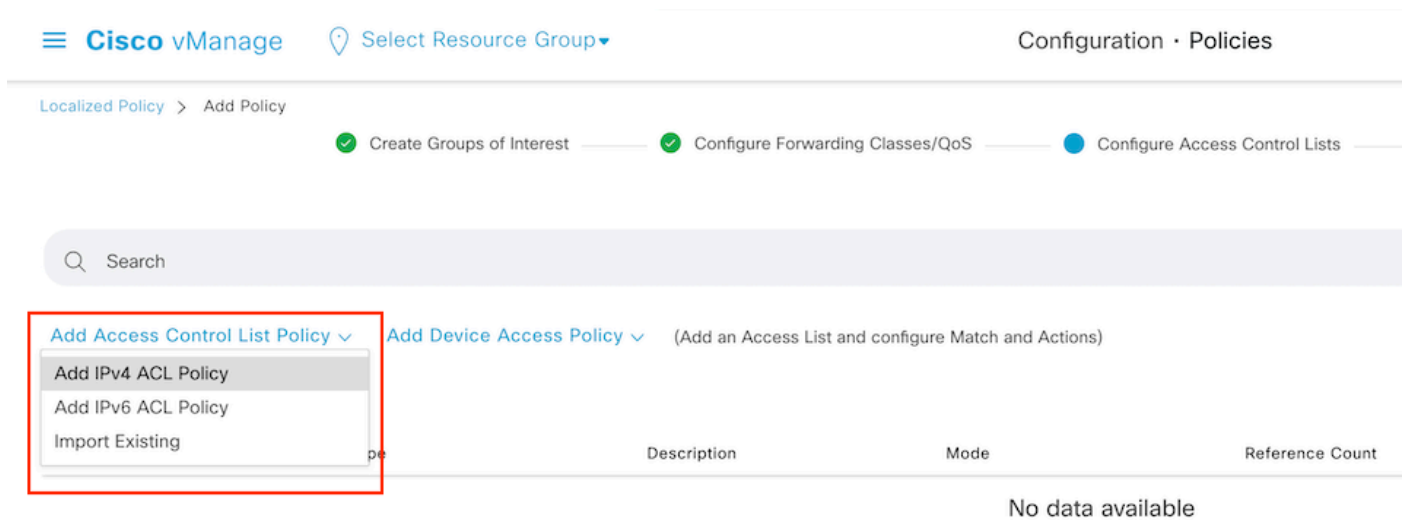
일치 조건에 이름을 지정하고, 인터넷 프로토콜을 정의하고, 데이터 접두사를 추가합니다.

클릭 **Add** 그리고 **Next** 까지 **Configure Access Control List** 표시됩니다.



3단계. 일치 조건을 적용할 액세스 목록을 생성합니다.

선택 **Add IPv4 ACL Policy** 에서 **Add Access Control List Policy** 드롭다운 메뉴.

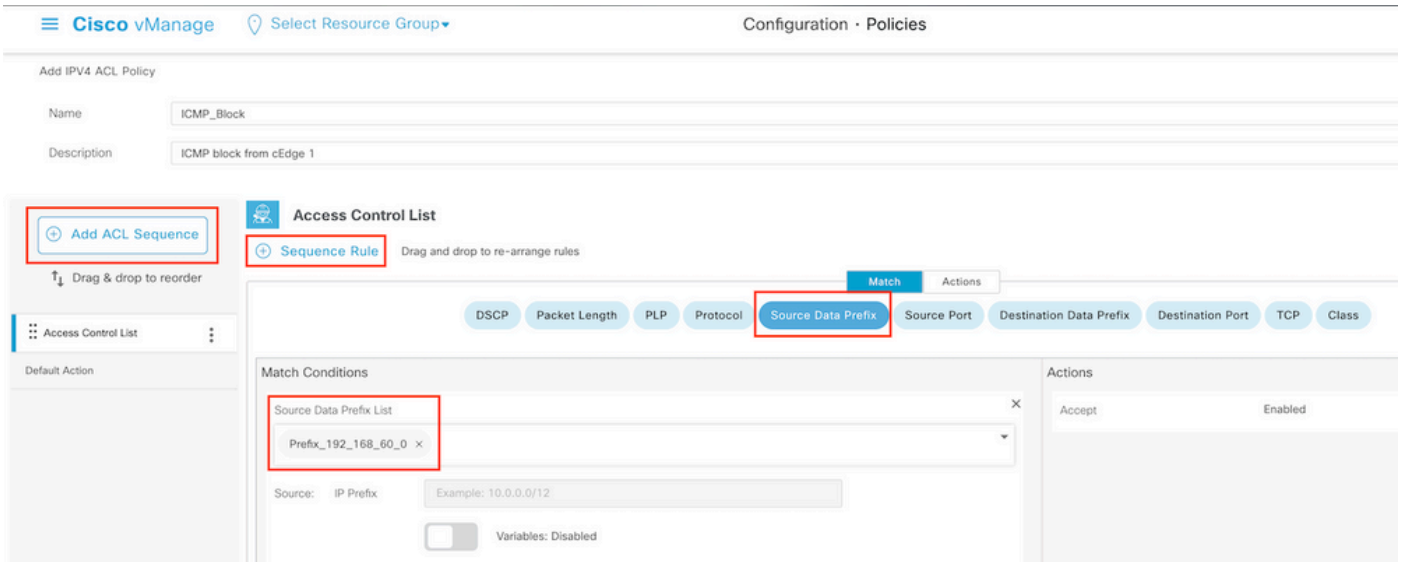


참고: 이 문서는 액세스 제어 목록 정책을 기반으로 하며 디바이스 액세스 정책과 혼동해서는 안 됩니다. 디바이스 액세스 정책은 SNMP(Simple Network Management Protocol) 및 SSH(Secure Socket Shell)와 같은 로컬 서비스에 대한 제어 계획에서만 작동하는 반면, 액세스 제어 목록 정책은 다양한 서비스 및 일치 조건에 대해 유동적입니다.

4단계. ACL 시퀀스 정의

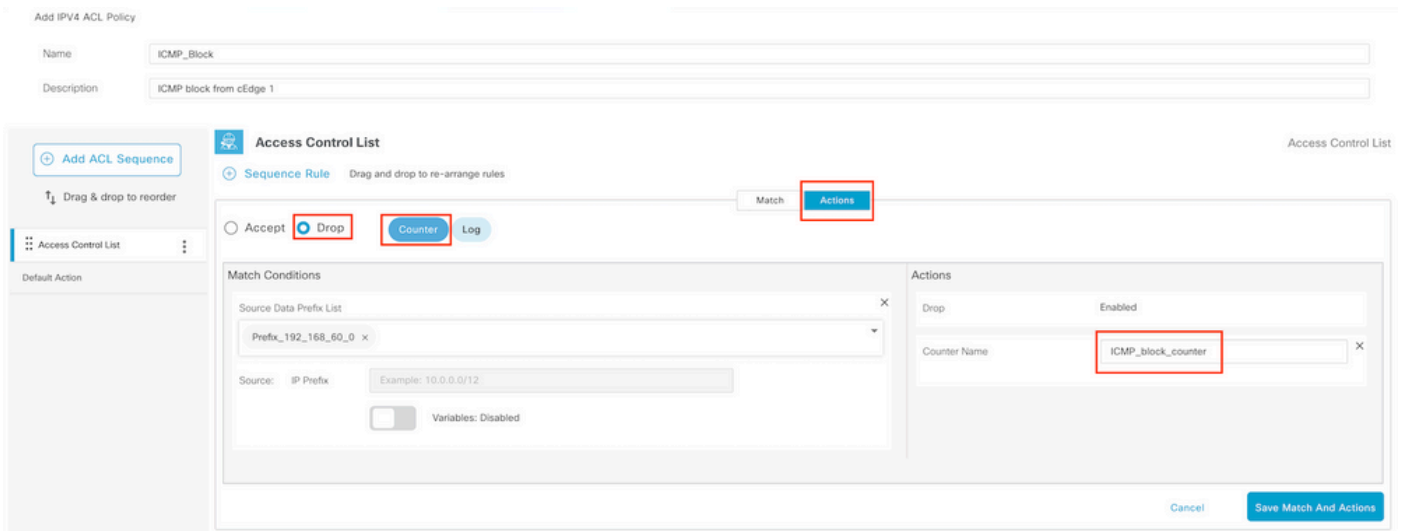
ACL 컨피그레이션 화면에서 ACL의 이름을 지정하고 설명을 제공합니다. 클릭 **Add ACL Sequence** 그리고 **Sequence Rule**.

일치 조건 메뉴에서 **Source Data Prefix** 데이터 접두사 목록을 **Source Data Prefix List** 드롭다운 메뉴.

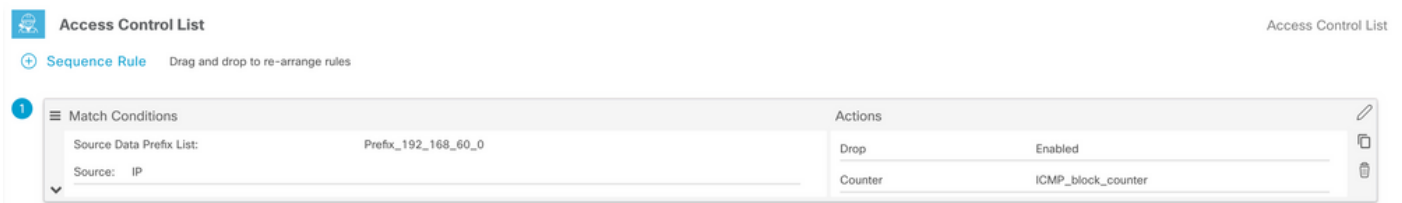


5단계. 시퀀스에 대한 조치를 정의하고 이름을 지정합니다

탐색 **Action** 선택 **Drop**, 및 **Save Match** 및 **Actions**.



참고: 이 작업은 지역화된 전체 정책이 아니라 시퀀스 자체와 배타적으로 연결됩니다.



6단계. 왼쪽 메뉴에서 **Default Action** ,클릭 **Edit**, 선택 **Accept**.

Add IPv4 ACL Policy

Name

Description


[Add ACL Sequence](#)

⬇️ Drag & drop to reorder

☰ Access Control List

Default Action

Default Action

Accept Enabled 

참고: 이 기본 작업은 현지화된 정책의 끝에 있습니다. **drop**을 사용하지 마십시오. 그렇지 않으면 모든 트래픽이 영향을 받아 네트워크 중단이 발생할 수 있습니다.

클릭 **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

7단계. 정책 이름 지정

클릭 **Next** 까지 **Policy Overview** 이름을 지정합니다. 다른 값은 비워 둡니다. 클릭 **Save Policy**

Localized Policy > Add Policy

Create Groups of Interest Configure Forwarding Classes/QoS Configure Access Control Lists Configure Route Policy

Enter name and description for your localized master policy

Policy Name

Policy Description

Policy Settings

Netflow Netflow IPv6 Application Application IPv6 Cloud QoS Cloud QoS Service side Implicit ACL Logging

Log Frequency

FNF IPv4 Max Cache Entries

FNF IPv6 Max Cache Entries

[Back](#)

[Preview](#)

[Save Policy](#)

[Cancel](#)

정책이 올바른지 확인하려면 **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	<ul style="list-style-type: none"> View <li style="border: 1px solid red;">Preview Copy Edit Delete

정책의 순서 및 요소가 올바른지 확인합니다.

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

ACL 이름을 복사합니다. 추가 단계에서 필요합니다.

8단계. 현지화된 정책을 디바이스 템플릿과 연결합니다.

라우터에 연결된 디바이스 템플릿을 찾고 점 3개를 클릭한 다음 **Edit**.

Cisco vManage Select Resource Group Configuration · Templates

Device Feature

Search

Create Template

Template Type Non-Default

Total Rows: 1 of 9

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

선택 **Additional Templates** 현지화된 정책을 policy 필드에 추가하고 **Update > Next > Configure Devices** cEdge에 구성을 푸시합니다.

Additional Templates

AppQoS

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.
```

참고: 이때 vManage는 생성된 정책을 기반으로 ACL을 구축하고, 어떤 인터페이스와도 연결되지 않았지만 cEdge에 변경 사항을 푸시합니다. 따라서 트래픽 플로우에는 영향을 미치지 않습니다.

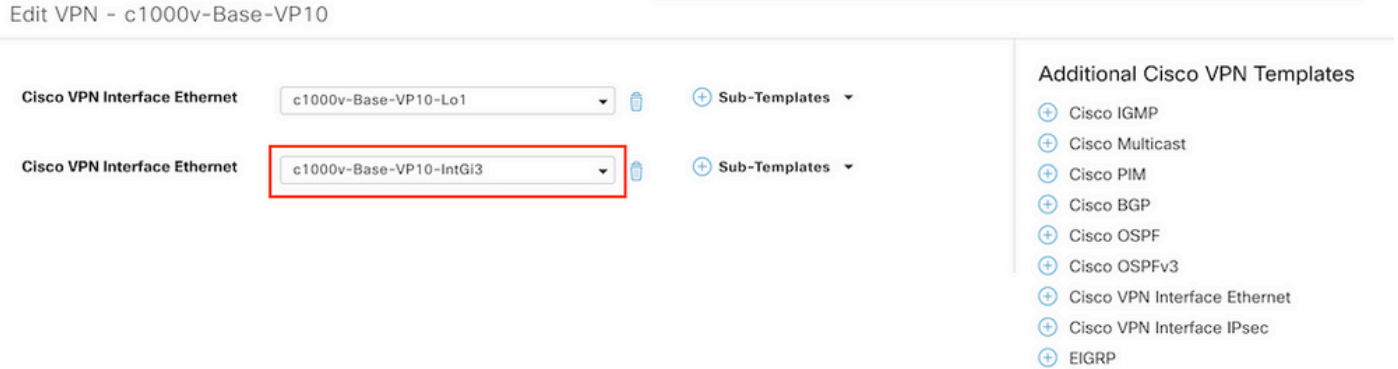
9단계. 디바이스 템플릿의 트래픽에 작업을 적용할 인터페이스의 기능 템플릿을 식별합니다.

트래픽을 차단해야 하는 기능 템플릿을 찾는 것이 중요합니다.

이 예에서 GigabitEthernet3 인터페이스는 Virtual Private Network 3(Virtual Forwarding Network 3)에 속합니다.

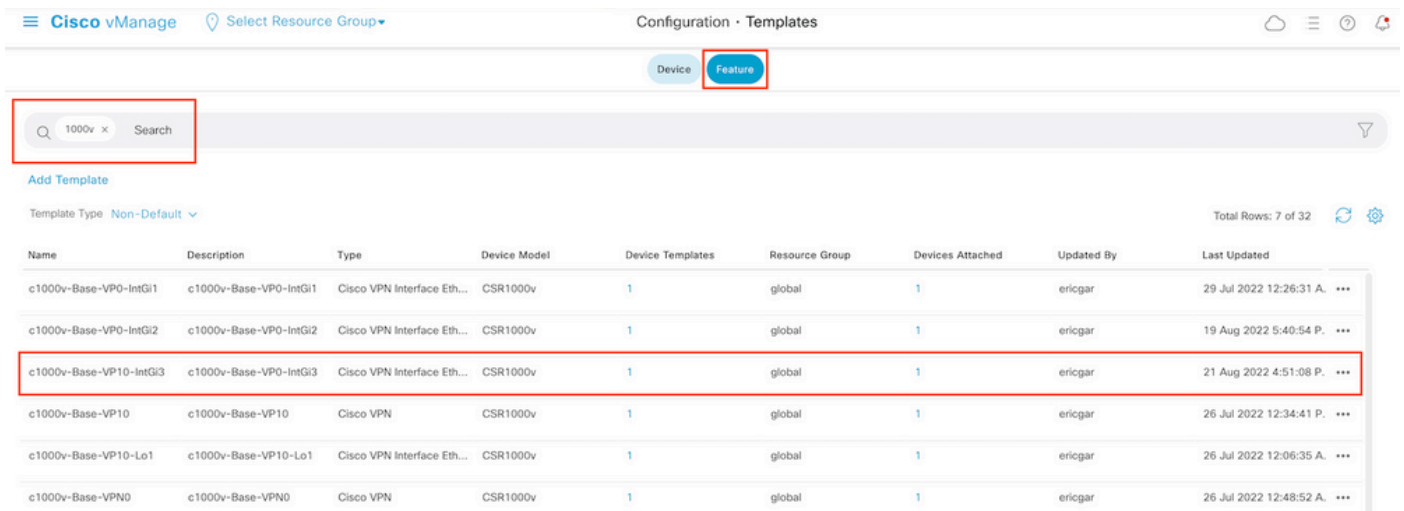
서비스 VPN 섹션으로 이동하고 Edit VPN 템플릿에 액세스합니다.

이 예에서 GigabitEthernet3 인터페이스에는 c1000v-Base-VP10-IntGi3 기능 템플릿이 연결되어 있습니다.



10단계. ACL 이름을 인터페이스와 연결합니다.

탐색 Configuration > Templates > Feature. 템플릿을 필터링하고 Edit



클릭 ACL/QoS 트래픽을 차단할 방향을 활성화합니다. 7단계에서 복사한 ACL 이름을 작성합니다. Update 변경 사항을 적용합니다.

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 checked="" type="checkbox"/> <input type="text"/>
QoS Map	<input checked="" type="checkbox"/> <input type="text"/>
VPN QoS Map	<input checked="" type="checkbox"/> <input type="text"/>
Rewrite Rule	<input checked="" type="checkbox"/> <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 checked="" type="checkbox"/> ICMP_Block
Ingress ACL - IPv6	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Egress ACL - IPv6	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off

Cancel

Update

참고: vManage 정책 구조가 두 아키텍처에서 동일하기 때문에 이 지역화된 정책 생성 프로세스도 vEdge에서 작동합니다. 다른 부분은 cEdge 또는 vEdge와 호환되는 컨피그레이션 구조를 구축하는 디바이스 템플릿에 의해 제공됩니다.

다음을 확인합니다.

1단계. 라우터에서 컨피그레이션이 올바른지 확인합니다

```
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

```

2단계. cEdge1의 서비스 네트워크에 있는 Host1에서 cEdge2의 서버로 ping 메시지 5개를 전송합니다

```

[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

```

참고: 이 예에서 host1은 Linux 시스템입니다. "-I"는 ping이 라우터를 떠나는 인터페이스를 나타내고 "-c"는 ping 메시지의 수를 나타냅니다.

3단계. cEdge2에서 ACL 카운터를 확인합니다

```

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

```

카운터는 정책에 정의된 대로 네트워크 192.168.60.0/24에서 보낸 5개의 패킷과 일치합니다.

4단계. cEdge3에서 서버 172.16.30.10에 4개의 ping 메시지를 보냅니다.

```

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

```

네트워크가 다르고(이 경우 1.1.1.1/32) 정책에서 일치하는 조건이 없기 때문에 라우터를 통해 서버로 전달된 패킷입니다.

5단계. cEdge2에서 ACL 카운터를 다시 확인합니다.

```

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

```

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

cEdge3에서 전송한 5개 패킷과 함께 증가하는 default_action_count의 카운터입니다.

카운터를 지우려면 `clear sdwan policy access-list` 명령을 실행합니다.

vEdge에서 확인할 명령

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

문제 해결

오류: 인터페이스의 ACL 이름에 대한 잘못된 참조입니다.

ACL을 포함하는 정책은 먼저 디바이스 템플릿에 연결해야 합니다. 그런 다음 인터페이스의 기능 디바이스 템플릿에 ACL 이름을 지정할 수 있습니다.

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

Total Task: 1 | Failure: 1

Q 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
```

관련 정보

- [Cisco SD-WAN 정책 컨피그레이션 가이드, Cisco IOS XE 릴리스 17.x](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.