

Konfigurieren der ACL zum Blockieren/Zuordnen von Datenverkehr an Edges mit vManage Policy

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Prozess zum Blockieren/Zuordnen in einem cEdge mit einer lokalisierten Richtlinie und einer Zugriffskontrollliste (ACL) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Cisco vManager
- cEdge-Befehlszeilenschnittstelle (CLI)

Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- c8000v Version 17.3.3
- vManage, Version 20.6.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrund

Es gibt verschiedene Szenarien, für die eine lokale Methode erforderlich ist, um Datenverkehr zu blockieren, zuzulassen oder abzugleichen. Jede Methode steuert den Zugriff auf den Router oder stellt sicher, dass die Pakete beim Gerät ankommen und verarbeitet werden.

cEdge-Router bieten die Möglichkeit, eine lokalisierte Richtlinie entweder über CLI oder vManage zu konfigurieren, um die Datenverkehrsbedingungen anzupassen und eine Aktion zu definieren.

Hier einige Beispiele für lokalisierte Richtlinienmerkmale:

Bedingungen für Übereinstimmung:

- Differentiated Services Code Point (DSCP)
- Paketlänge
- Protokolle
- Präfix für Quelldaten
- Quellport
- Präfix für Zieldaten
- Zielport

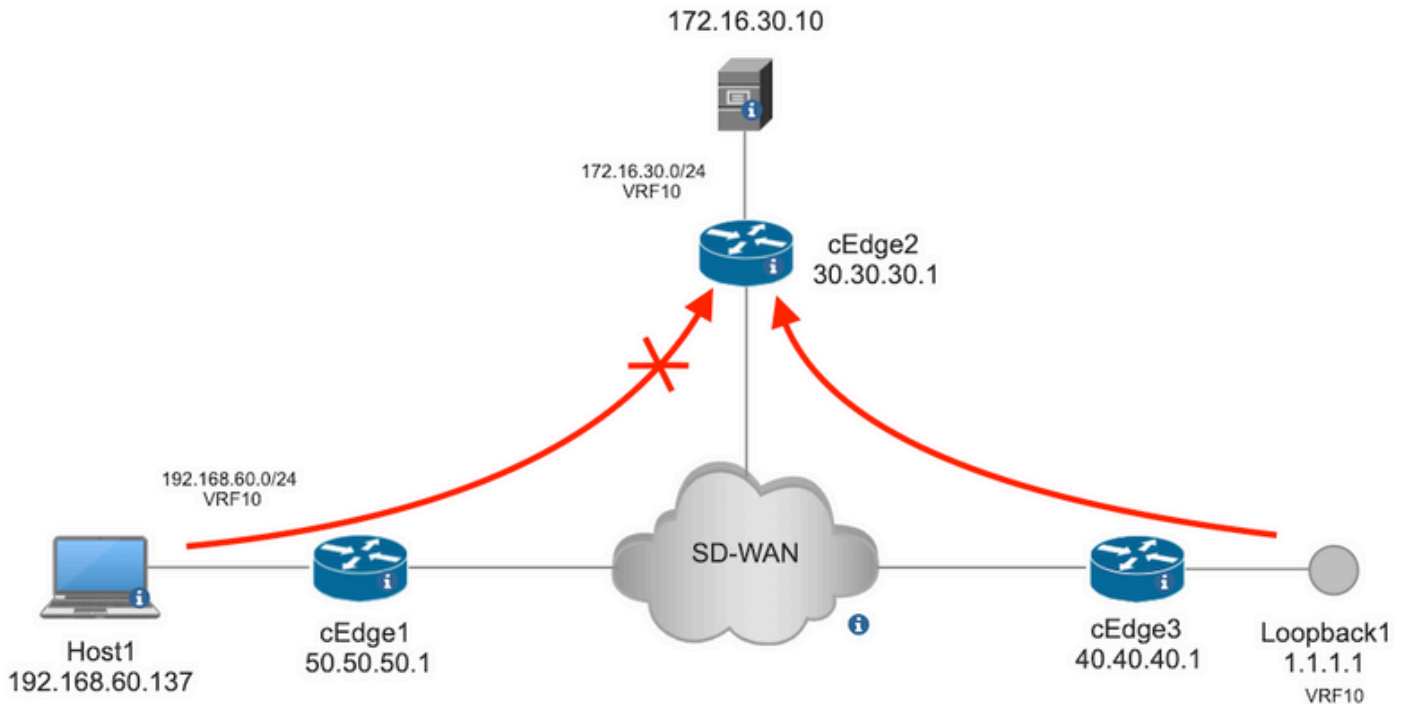
Aktionen:

- Akzeptieren Weitere: Zähler, DSCP, Protokolle, Next-Hop, Spiegelliste, Klasse, Richtlinie
- Löschen Zusätzlich: Zähler, Protokoll

Konfigurieren

Netzwerkdiagramm

In diesem Beispiel soll der Datenverkehr vom Netzwerk 192.168.20.0/24 am Ausgang in cEdge2 blockiert werden, und ICMP soll von der cEdge3-Loopback-Schnittstelle zugelassen werden.



Ping-Verifizierung von Host1 an 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
```

Ping-Überprüfung von cEdge3 an 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
```

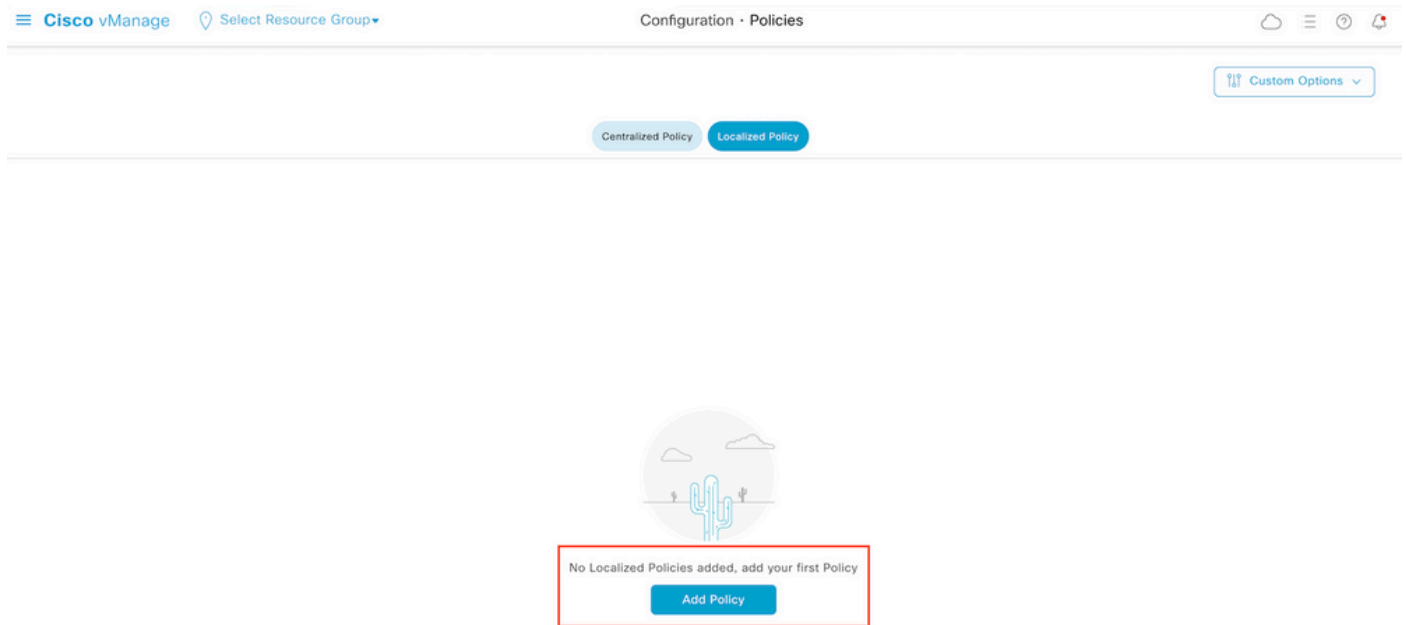
Voraussetzungen:

- cEdge2 muss eine Gerätevorlage angehängt haben.
- Alle Kanten müssen über aktive Steuerverbindungen verfügen.
- Für alle cEdges müssen BFD-Sitzungen (Bidirectional Forwarding Detection) aktiv sein.
- Alle Knoten müssen über OMP-Routen (Overlay Management Protocol) verfügen, um Service-VPN10-Netzwerke zu erreichen.

Konfigurationen

Schritt 1: Fügen Sie die lokalisierte Richtlinie hinzu.

Navigieren Sie in Cisco vManage zu **Configuration > Policies > Localized Policy**. Klicken Sie auf **Add Policy**

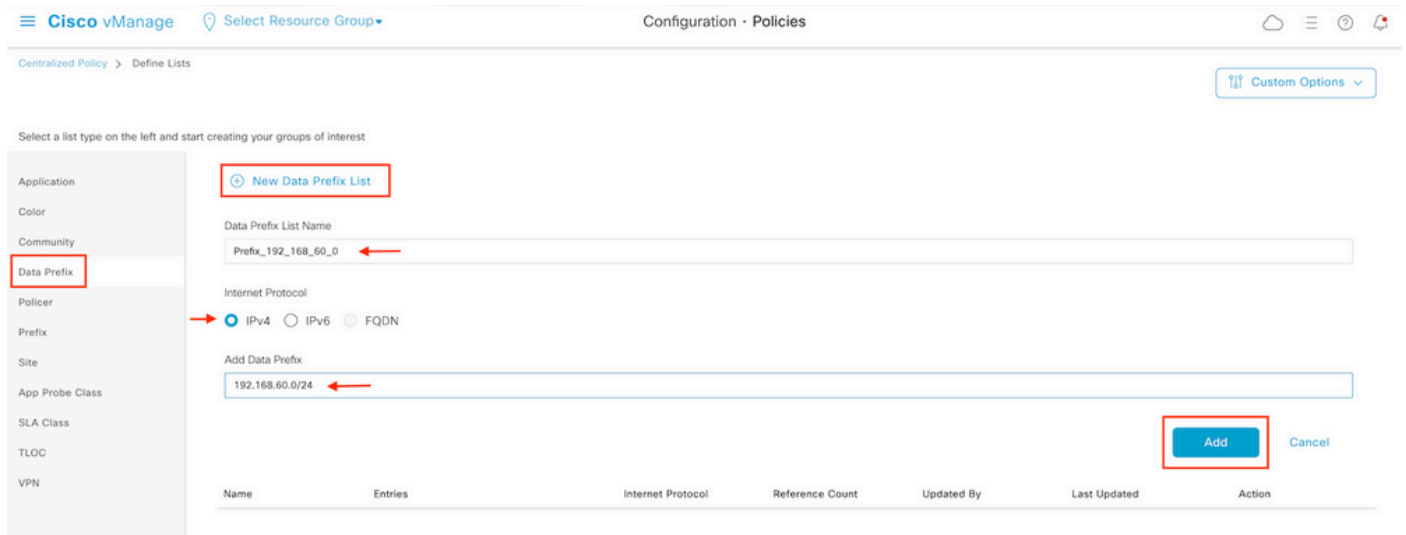


Schritt 2: Erstellen Sie Interessengruppen für die beabsichtigte Übereinstimmung.

Klicken Sie auf **Data Prefix** im linken Menü aus, und wählen Sie **New Data Prefix List**.

Geben Sie der Übereinstimmungsbedingung einen Namen, definieren Sie das Internetprotokoll, und fügen Sie ein Datenpräfix hinzu.

Klicken Sie auf **Add** und dann **Next** bis **Configure Access Control List** angezeigt.



Schritt 3: Erstellen Sie die Zugriffsliste, um die Übereinstimmungsbedingung anzuwenden.

Auswählen **Add IPv4 ACL Policy** von **Add Access Control List Policy** Dropdown-Menü.

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

Anmerkung: Dieses Dokument basiert auf einer Richtlinie für Zugriffskontrolllisten und darf nicht mit einer Richtlinie für den Gerätezugriff verwechselt werden. Die Richtlinie für den Gerätezugriff dient nur im Kontrollplan für lokale Dienste wie Simple Network Management Protocol (SNMP) und Secure Socket Shell (SSH), während die Richtlinie für die Zugriffskontrollliste flexibel ist und unterschiedliche Dienste und Übereinstimmungsbedingungen unterstützt.

Schritt 4: Definieren der ACL-Sequenz

Benennen Sie die ACL im Konfigurationsbildschirm der ACL, und geben Sie eine Beschreibung an. Klicken Sie auf **Add ACL Sequence** und dann **Sequence Rule**.

Wählen Sie im Menü "Bedingungen für Übereinstimmung" **Source Data Prefix** und wählen Sie dann in der **Source Data Prefix List** aus.

The screenshot shows the configuration page for an IPv4 ACL policy named 'ICMP_Block'. The 'Add ACL Sequence' button is highlighted in red. The 'Sequence Rule' section is also highlighted in red, showing the 'Match' tab with 'Source Data Prefix' selected. The 'Source Data Prefix List' dropdown is highlighted in red, showing 'Prefix_192_168_60_0' selected. The 'Actions' tab shows 'Accept' and 'Enabled'.

Schritt 5: Definieren Sie die Aktion für die Sequenz, und nennen Sie sie

Navigieren Sie zu **Action** auswählen **Drop**, und klicke auf **Save Match** und **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

Anmerkung: Diese Aktion ist ausschließlich der Sequenz selbst zugeordnet, nicht der vollständigen lokalisierten Richtlinie.

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

Schritt 6. Wählen Sie im Menü links **Default Action**, klicken Sie auf **Edit**, und wählen **Accept**.

Cisco vManage Configuration · Policies

Add IPv4 ACL Policy

Name: ICMP_Block
Description: ICMP block from cEdge 1

Default Action

Accept Enabled

Default Action

Anmerkung: Diese Standardaktion ist das Ende der lokalisierten Richtlinie. Verwenden Sie nicht **drop**, da sonst der gesamte Datenverkehr beeinträchtigt werden und ein Netzerkausfall verursachen kann.

Klicken Sie auf **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

Schritt 7: Benennen der Richtlinie

Klicken Sie auf **Next** bis **Policy Overview** und nennen Sie es. Lassen Sie die anderen Werte leer. Klicken Sie auf **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](#)

Um sicherzustellen, dass die Richtlinie korrekt ist, klicken Sie auf **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](#)

Überprüfen Sie die Reihenfolge und die Elemente in der Richtlinie.

Policy Configuration Preview

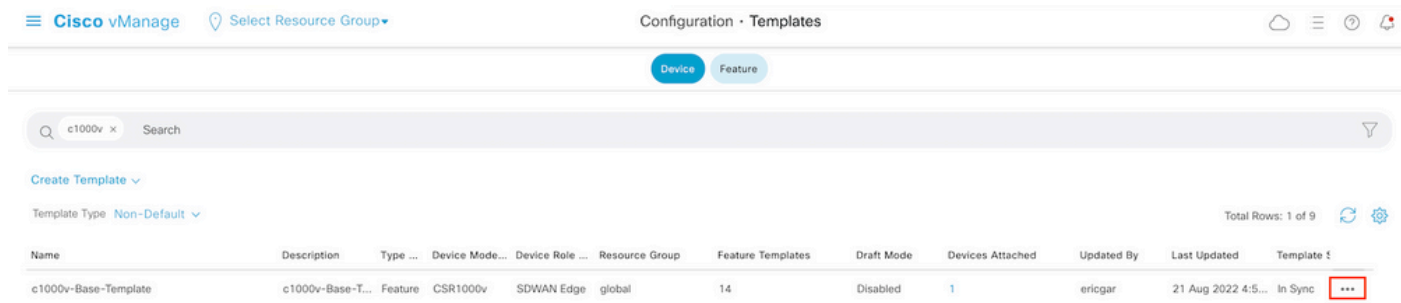
```
policy
access-list ICMP_Block
sequence 1
match
source-data-prefix-list Prefix_192_168_60_0 ←
!
action drop ←
count ICMP_block_counter ←
!
!
default-action accept ←
!
lists
data-prefix-list Prefix_192_168_60_0
ip-prefix 192.168.60.0/24 ←
!
!
!
```

OK

Kopieren Sie den ACL-Namen. Dies ist in einem weiteren Schritt erforderlich.

Schritt 8: Verknüpfen Sie die lokalisierte Richtlinie mit der Gerätevorlage.

Suchen Sie die Gerätevorlage, die mit dem Router verbunden ist, klicken Sie auf die drei Punkte, und klicken Sie auf **Edit**.



Auswählen **Additional Templates** und füge die lokalisierte Richtlinie dem Feld "Policy" hinzu. Klicken Sie dann auf **Update > Next > Configure Devices** um die Konfiguration an den cEdge zu übertragen.

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.
```

Anmerkung: Zu diesem Zeitpunkt erstellt vManage die ACL auf Basis der erstellten Richtlinie und überträgt die Änderungen an den cEdge, obwohl sie keiner Schnittstelle zugeordnet ist. Daher hat es keine Auswirkungen auf den Verkehrsfluss.

Schritt 9: Identifizieren Sie die Funktionsvorlage der Schnittstelle, auf der die Aktion auf den Datenverkehr in der Gerätevorlage angewendet werden soll.


Es ist wichtig, die Funktionsvorlage an der Stelle auszuwählen, an der der Datenverkehr blockiert werden muss.


In diesem Beispiel gehört die GigabitEthernet3-Schnittstelle zu Virtual Private Network 3 (Virtual Forwarding Network 3).

Navigieren Sie zum Service-VPN-Abschnitt, und klicken Sie auf **Edit** um auf die VPN-Vorlagen zuzugreifen.

In diesem Beispiel ist der GigabitEthernet3-Schnittstelle eine c1000v-Base-VP10-IntGi3-Funktionsvorlage angefügt.

Edit VPN - c1000v-Base-VP10

Cisco VPN Interface Ethernet  [+ Sub-Templates](#) ▾





Cisco VPN Interface Ethernet  [+ Sub-Templates](#) ▾

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](#)



Schritt 10: Verknüpfen Sie den Namen der ACL mit der Schnittstelle.

Navigieren Sie zu **Configuration > Templates > Feature**. Vorlagen filtern und auf **Edit**

Cisco vManage [Select Resource Group](#) Configuration · Templates    

[Device](#) [Feature](#)

[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-VP10-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. ...

Klicken Sie auf **ACLaaS** und die Richtung für die Blockierung des Datenverkehrs aktivieren. Schreiben Sie den in Schritt 7 kopierten ACL-Namen. Klicken Sie auf **update** und Änderungen vorantreiben.

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

Ingress ACL - IPv6

 On Off

Egress ACL - IPv6

 On Off

Cancel

Update

Hinweis: Dieser Prozess zur Erstellung lokalisierter Richtlinien funktioniert auch für vEdges, da die vManage-Richtlinienstruktur für beide Architekturen identisch ist. Der unterschiedliche Teil wird durch die Gerätevorlage bestimmt, die eine mit cEdge oder vEdge kompatible Konfigurationsstruktur erstellt.

Überprüfung

Schritt 1: Überprüfen der korrekten Konfiguration des Routers

```
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

```

Schritt 2: Senden Sie von Host 1, der sich im Servicenetzwerk von cEdge1 befindet, 5 Ping-Nachrichten an den 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

```

Anmerkung: In diesem Beispiel ist host1 eine Linux-Maschine. "-I" steht für die Schnittstellen, bei denen der Ping den Router verlässt, und "-c" steht für die Anzahl der Ping-Nachrichten.

Schritt 3: Überprüfen der ACL-Zähler am cEdge2

```

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

```

Der Zähler stimmte mit fünf (5) Paketen überein, die gemäß der Definition in der Richtlinie vom Netzwerk 192.168.60.0/24 stammten.

Schritt 4: Senden Sie von cEdge3 vier Ping-Nachrichten an 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

```

Die Pakete werden über den Router an den Server weitergeleitet, da das Netzwerk anders ist (in diesem Fall 1.1.1.1/32) und keine Übereinstimmungsbedingung für die Richtlinie vorliegt.

Schritt 5: Überprüfen Sie die ACL-Zähler in cEdge2 erneut.

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

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

Der Zähler von default_action_count wurde mit den 5 von cEdge3 gesendeten Paketen erhöht.

Führen Sie einen clear sdwan policy access-list aus.

Befehle zur Verifizierung in vEdge

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

Fehlerbehebung

Fehler: Ungültiger Verweis auf den ACL-Namen in der Schnittstelle

Die Richtlinie, die die ACL enthält, muss zuerst an die Gerätevorlage angefügt werden. Anschließend kann der ACL-Name in der Funktionsgerätevorlage der Schnittstelle angegeben werden.

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-A5FFEDC7B1F8)/vpn/vpn-instance(10)/interface(gigabitEthernet3)/access-list(out)/acl-name
```

Zugehörige Informationen

- [Konfigurationsleitfaden für Cisco SD-WAN-Richtlinien, Cisco IOS XE Version 17.x](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.